ÚMFT infovonal:
06 40 638 638
nfu@nfu.gov.hu • www.nfu.hu

TERMÉKEKRE VONATKOZÓ ÉRTÉKELÉSI MÓDSZERTAN

A dokumentum az Új Magyarország Fejlesztési Terv keretében, az Államreform Operatív Program támogatásával, az „Elektronikus közigazgatási keretrendszer” tárgyú kiemelt projekt megvalósításának részeként készült. A dokumentum elkészítésében részt vett:

Metaadat-táblázat

Megnevezés	**Leírás**
Cím (dc:Title)	Termékekre vonatkozó értékelési módszertan
Kulcsszó (dc:Subject)	IT biztonság; értékelés; módszertan
Leírás (dc:Description)	Az elkészült e-közigazgatási alkalmazást használatbavétel előtt meg kell vizsgálni, hogy megfelel-e a rá vonatkozó biztonsági követelményeknek. Jelen dokumentum a biztonság (termékekre irányuló) értékelési módszertanát határozza meg. A felállított/akkreditált gyártófüggetlen vizsgáló laboratóriumok az ebben a dokumentumban meghatározott értékelési módszertan alapján végezhetik a termék értékeléseket azokra a biztonsági szempontból kritikus termékekre, amelyek nem rendelkeznek CC (Common Criteria) tanúsítvánnyal.
Típus (dc:Type)	szöveg, táblázatok, ábrák
Forrás (dc:Source)	
Kapcsolat (dc:Relation)	e-Közigazgatási Keretrendszer egyéb dokumentumai
Terület (dc:Coverage)	KOP-ok során megvalósuló projektek, központi IT fejlesztési projektek
Létrehozó (dc:Creator)	e-Közigazgatási Keretrendszer Kialakítása projekt
Kiadó (dc:Publisher)	Miniszterelnöki Hivatal
Résztvevő (dc:Contributor)	Hunguard Kft.
Jogok (dc:Rights)	e-Közigazgatási Keretrendszer
Dátum (dc:Date)	2008.09.19.
Formátum (dc:Format)	.doc
Azonosító (dc:Identifier)	
Nyelv (dc:Language)	Magyar
Verzió (dc:Version)	V4
Státusz (State)	Végleges
Fájlnév (FileName)	EKK_ekozig_termek_ertekeles_080919_V4.doc
Méret (Size)	
Ár (Price)	
Felhasználási jogok	Korlátlan

Verziókövetési táblázat

A dokumentum neve	Termékekre vonatkozó értékelési módszertan
A dokumentum készítőjének neve	Hunguard Kft
A dokumentum jóváhagyójának neve	
A dokumentum készítésének dátuma	2008.09.19.
Verziószám	**V4**
Összes oldalszám	344
A projekt azonosítója	E-közigazgatási keretrendszer kialakítása

Változáskezelés

Verzió	Dátum	A változás leírása
V0.1	2008.05.10.	Első tartalomjegyzék
V1	2008.05.29.	Első átadott változat
V2	2008.06.20.	Módosítások
V3	2008.07.20	Módosítások
V4	2008.09.19.	Végleges változat

Szövegsablon

Megnevezés	**Leírás**
1. Előszó (Foreword)	1. fejezet
2. Bevezetés (Preamble)	2. fejezet
3. Alkalmazási terület (Scope)	
4. Rendelkező hivatkozások (References)	
5. Fogalom-meghatározások (Definitions)	
6. A szabvány egyedi tartalma (UniqueContent)	
7. Bibliográfia	nincs
8. Rövidítésgyűjtemény	9. fejezet
9. Fogalomtár	
10. Ábrák	szövegben
11. Képek	nincs
12. Fogalmak	5. fejezet
13. Verzió	V4
14. Mellékletek (Appendix)	nincs

Tartalomjegyzék

1. Előszó

A jelen dokumentumban megfogalmazott értékelési módszertan a közigazgatási fejlesztési operatív programok megvalósítására vonatkozó általános vizsgálati módszertan részét képezi.

Egy általános vizsgálati módszertan átfogja a szoftverminőség számos jellemzőjét, köztük az alábbiakat: funkcionalitás, megbízhatóság, használhatóság, hatékonyság, karbantarthatóság. A jelen dokumentumban megfogalmazott értékelési módszertan a funkcionalitáshoz kötődik.

A közigazgatási fejlesztési operatív programok megvalósítására vonatkozó általános vizsgálati módszertan a szoftverminőség funkcionalitás jellemzőjén belül elsősorban az együttműködés (interoperabilitás) és a biztonság segédjellemzőkre koncentrál. A jelen dokumentumban megfogalmazott értékelési módszertan a biztonságra (informatikai biztonságra) irányul.

Az általános vizsgálati módszertan az informatikai biztonságnak is két szempontjával foglalkozik:

- szervezeti szempontból, az informatikai rendszerek irányításáért, menedzseléséért felelős vezetőknek, illetve a szervezet egészére vonatkozó követelmények teljesülését értékelő szakembereknek szólóan,
- technológiai szempontból, az informatikai rendszerek kialakításáért és fejlesztéséért felelős szakemberek és vezetők, valamint az informatikai termékek és rendszerek biztonsági értékelését végző szakemberek számára.

A jelen dokumentumban megfogalmazott értékelési módszertan az informatikai biztonságot technológiai szempontból kezeli.

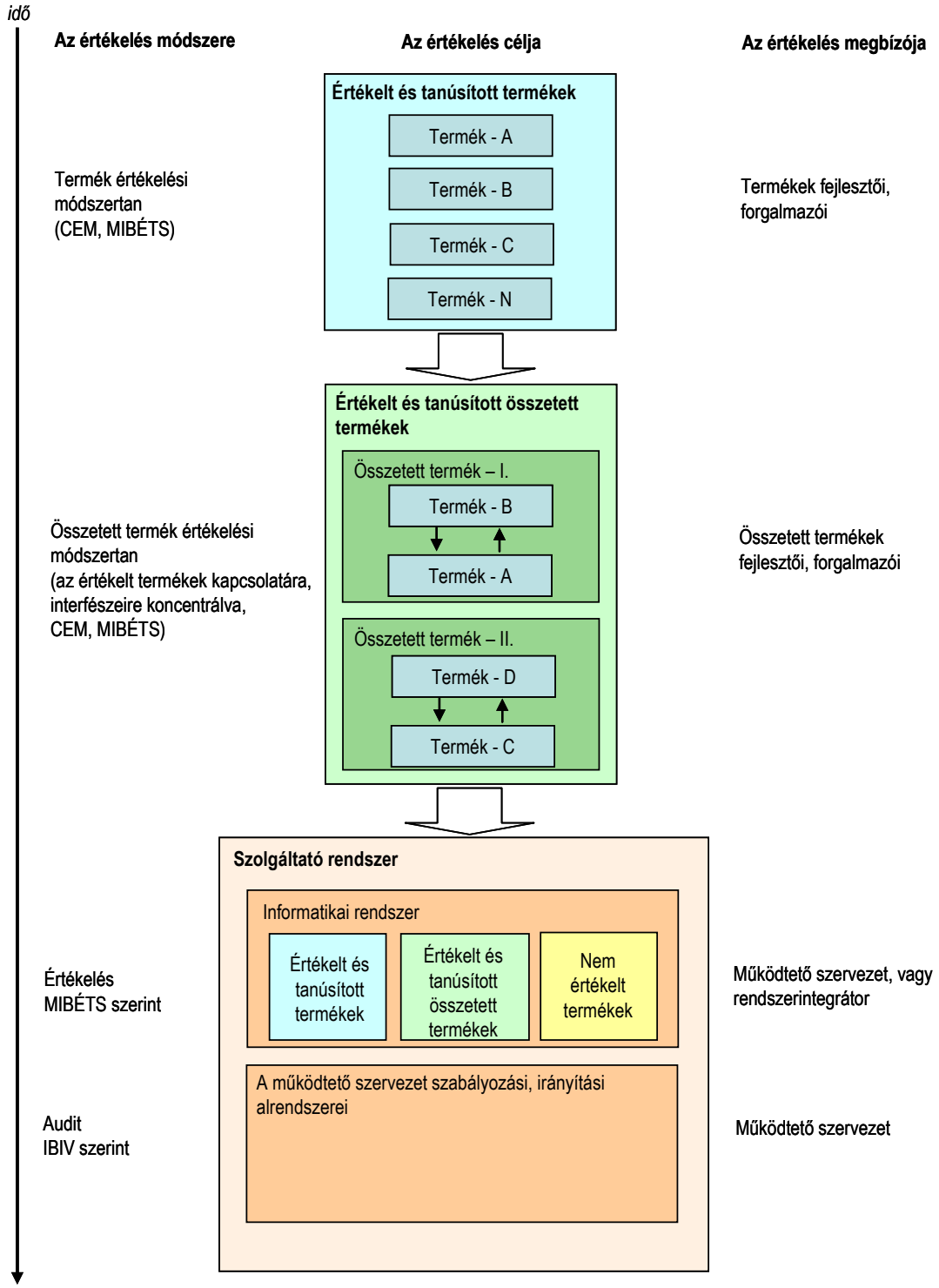
Az informatikai biztonságot technológiai szempontból kezelő értékelői módszertan az alábbi dokumentumokból áll:

- Termékekre vonatkozó értékelési módszertan (jelen dokumentum)
- Összetett termékekre vonatkozó értékelési módszertan [7],
- Szolgáltató (működő) rendszerre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozás alatt álló dokumentum),

A fenti három egymásra épülő módszertanban jelen dokumentum az alapot biztosítja:

- az összetett termékekre vonatkozó értékelési módszertan közvetlenül erre épül, mivel (lásd [7]) korábban már (termékként) értékelt komponensekből integrált entitások értékelését jelenti,
- egyúttal megalapozza a szolgáltató rendszerek értékelési módszertanát, mert a szolgáltató rendszerek (különböző biztonsági szabályzat hatálya alá eső) biztonsági tartományokra, majd ezeken belül összetett termékekre bonthatók, s ezek vizsgálata részben moduláris felépítésű.

A három értékelési módszertan kapcsolatát mutatja a következő ábra:



1. ábra – A három értékelési módszertan

2. Bevezetés

2.1. A dokumentum célja

Az informatikai biztonsági értékelésre vonatkozó közös szempontok (CC, [1]), és közös értékelési módszertan (CEM, [2]) alapján a világ számos országában végzik informatikai termékek technológiai szempontú értékelését és tanúsítását. A CC szerint kibocsátott tanúsítványok kölcsönös elismerési egyezménye [3] alapján az egyezményt aláíró nemzetek (köztünk hazánk is) az értékelési és tanúsítási eredményeket kölcsönösen elismerik.

Mivel Magyarország jelenleg még nem CC tanúsítványt kibocsátó ország, ezért mindazon termékekre, amelyekre nincsen CC értékelés és tanúsítás, de szükséges a biztonsági funkcionalitás megbízhatóságának garantálása, az informatika biztonság hazai séma-változata a MIBÉTS teremt lehetőséget a hazai értékelésekre. A legtöbb fejlett ország rendelkezik hasonló nemzeti sémával, melyet az adott országon belüli értékelő laboratóriumok értékelhetnek, és tanúsító szervezetek tanúsíthatnak. Ezek ugyan nemzetközi szinten nem érvényesek (a kölcsönös nemzetközi elfogadás csak a CC tanúsítványokra vonatkozik), de segítségükkel az adott országban működő szervezetek mégis garanciát szerezhetnek a termékek biztonságáról.

Jelen dokumentum a [6] által meghatározott termék értékelési módszertan olyan továbbfejlesztése, mely figyelembe veszi azt az [1] és [2] által megvalósított jelentős továbbfejlesztést és egyszerűsítést is, melyet a CC/CEM korábbi verzióinak több mint 10 éves tapasztalataiból szűrtek le, s a közelmúltban fogadták el a CC tanúsítványt kibocsátó országok.

A [6] által meghatározott termék értékelési módszertan a jelenleg érvényes nemzetközi szabványban [9] foglaltakat tükrözi, mely szerint az idén még értékeléseket végeztek, s mely a CC tanúsítványt kibocsátó országok garancia folytonosságot biztosító rendszereiben 2009. szeptemberéig még használható.

Jelen dokumentum a [2]-ben meghatározott legfrissebb értékelési módszertant tükrözi, melyet jövőre (minden valószínűség szerint lényegében változatlan formában) nemzetközi szabványként fogadnak el, s mely a CC tanúsítványt kibocsátó országokban 2008. márciusa óta a CC értékelésekhez kizárólagosan használható módszer.

2.2. A dokumentum felépítése

Az 1. fejezet elhelyezi a dokumentumot az e-Közigazgatási Keretrendszeren belül, tájékoztatást adva a célközönségről és a kapcsolódó dokumentumokról.

A 2. fejezet bevezető információkat tartalmaz, megadva a dokumentum célját és felépítését.

A 3. fejezet meghatározza az alkalmazás lehetséges területeit.

A 4. és 5. fejezet a hivatkozásokat, illetve a fogalom-meghatározásokat tartalmazza.

A 6. fejezet tartalmazza a dokumentum lényegi részét, 2 alfejezetben.

A 6.1 alfejezet a termékek fejlesztőinek ad útmutatást.

A 6.1.1 alfejezet megadja a dokumentum által az IT termékek biztonságára alkalmazott megközelítési módot.

A 6.1.2 alfejezet ismerteti az értékelési garanciaszint fogalmát, majd áttekinti a hierarchikus kapcsolatban álló 3 értékelési garanciaszintet (alap, fokozott és kiemelt).

A 6.1.3 alfejezet „ellenőrző lista”-ként használható módon azokat a fejlesztői feladatokat tekinti át (a később részletezettekre való hivatkozással), amelyeket egy termék biztonsági értékelésének előkészítése érdekében kell elvégezni (a különböző értékelési garanciaszintek szerint elkülönített csoportosításban).

A 6.1.4 alfejezet meghatározza az egyik fő értékelés előkészítő feladatot: a termékekre vonatkozó biztonsági előirányzat készítését. Ez egy mindhárom garanciaszinten egységes feladat.

A 6.1.5 – 6.1.9 alfejezetek részletezik a másik fő értékelés előkészítő feladatot: a termékekre vonatkozó értékelési bizonyítékok elkészítését. Ehhez az egyes alfejezetek részletesen tárgyalják a termék értékelésre vonatkozó 5 garanciaosztályt (Fejlesztés, Útmutató dokumentumok, Életciklus támogatás, Tesztelés, Sebezhetőség felmérés), az ezekhez tartozó garanciacsaládokat és garancia-összetevőket, meghatározva egyúttal a garancia-összetevők által elvárt tartalmi és formai követelményeket is.

A 6.2 alfejezet a termékek értékelőinek ad útmutatást.

A termékek értékelőinek természetesen valamennyi fejlesztőnek szükséges ismeret birtokában kell lenniük. Ez az alfejezet olvasóitól feltételezi ezt a tudást.

A 6.2.1 alfejezet az általános értékelői feladatokat tekinti át.

A 6.2.2 alfejezet a biztonsági előirányzat egységes, a 6.2.3 - 6.2.5 alfejezetek pedig a termék választott garanciaszintjétől függő egyre bővülő és szigorodó értékelési követelményeit és módszertani elemeit határozza meg.

A 7. fejezet mellékleteket tartalmaz.

A 7.1 melléklet azokat az általános fejlesztői útmutatásokat tartalmazza, melyeket különböző fejlesztői tevékenységek során egységesen kell alkalmazni (CC funkcionális követelmények szerkezete, CC műveletek, védelmi profil megfelelés).

A 7.2 melléklet azokat az általános értékelési útmutatásokat tartalmazza, melyeket különböző értékelési tevékenységek során egységesen kell alkalmazni (mintavételezés, függőségek kezelése, helyszíni szemlék).

A 7.3 melléklet az értékelési módszertan lényegi eleméhez, a sebezhetőség vizsgálatához nyújt egységes módszertani alapokat, többek között meghatározva a támadó képesség fogalmát, s meghatározva annak számítási módszerét.

Végül a 7.4 melléklet áttekinti a CC v2.3 és v3.1 verziói közötti fontosabb különbségeket. A CC v2.3 volt az alapja a MIBÉTS séma értékelési módszertanának [6], míg a CC v3.1 az alapja a jelen dokumentumban meghatározottaknak.

3. Alkalmazási terület

A jelen dokumentumban megfogalmazott irányelvek és követelmények elsődlegesen a közigazgatási fejlesztési operatív programok megvalósítására vonatkoznak, az ezekben felhasznált informatikai termékek biztonságos fejlesztését és vizsgálatát (biztonsági értékelését) alapozzák meg, s ezáltal a közigazgatási fejlesztési operatív programok végrehajtásával elkészülő rendszerek megfelelőségi vizsgálatának egy részét képezi.

Ezek az irányelvek és követelmények az elektronikus közigazgatáson kívül, a közszféra más területein, valamint a magánszférában is alkalmazhatók, minden olyan esetben, amikor biztonságosan működő informatikai termékek felhasználására, illetve ezek meghatározott biztonsági követelményeknek való megfelelésének független vizsgálatára (biztonsági értékelésére) van szükség.

4. Rendelkező hivatkozások

A jelen dokumentumban megfogalmazott irányelvek és követelmények az alábbi mértékadó dokumentumokon alapulnak:

[1]: Common Criteria for Information Technology Security Evaluation (September 2006 - version 3.1, revision 2) – Part 1: Introduction and general model – Part 2: Security functional components - Part 3: Security assurance components

[2]: Common Methodology for Information Technology Security Evaluation (September 2006 - version 3.1, revision 2)

[3]: Arrangement on the Recognition of Common Criteria Certificates – In the field of Information Technology Security – May 2000

[4]: Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma 3. számú segédlete: Útmutató a fejlesztők számára (v1.0, 2008)

[5]: Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma 4. számú segédlete: Útmutató az értékelők számára (v1.0, 2008)

[6]: Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma 5. számú segédlete: Értékelési módszertan (v1.0, 2008)

[7]: Összetett termékekre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v1, 2008.05.25)

[8]: Az értékeléssel megszerzett garancia folyamatosságának biztosítása (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v1.0, 2008.05.25)

[9]: ISO/IEC 18045:2005 Information technology – Security techniques – Methodology for IT security evaluation

Az 1. táblázat a rendelkező hivatkozások elérhetőségét adja meg.

1. táblázat - A rendelkező hivatkozások elérhetősége

Cím	**Külföldi elérhetőség**	**Magyar elérhetőség**
Common Criteria for Information Technology Security Evaluation (September 2006 -version 3.1, revision 2) - Part 1: Introduction and general model - Part 2: Security functional components - Part 3: Security assurance components	CCPart1v3.1R1 CCPart2v3.1R1 CCPart3v3.1R1	
Common Methodology for Information Technology Security Evaluation (September 2006 - version 3.1, revision 2)	CEMv3.1R2	
Arrangement on the Recognition of Common Criteria Certificates - In the field of Information Technology Security - May 2000	cc-recarrange.pdf	
Magyar Informatikai Biztonsági Ajánlások - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma 3. számú segédlete: Útmutató a fejlesztők számára (v1.0, 2008)		EEK KIB 25/2-3
Magyar Informatikai Biztonsági Ajánlások - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma 4. számú segédlete: Útmutató az értékelők számára (v1.0, 2008)		EEK KIB 25/2-4
Magyar Informatikai Biztonsági Ajánlások - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma 5. számú segédlete: Értékelési módszertan (v1.0, 2008)		EEK KIB 25/2-5
Összetett termékekre vonatkozó értékelési módszertan		e-Közigazgatási Keretrendszer dokumentumai
Az értékeléssel megszerzett garancia folyamatosságának biztosítása		e-Közigazgatási Keretrendszer dokumentumai
ISO/IEC 18045:2005 Information technology – Security techniques – Methodology for IT security evaluation	ISO/IEC 18045:2005	

5. Fogalom-meghatározások

Jelen dokumentum a [6] által meghatározott termék értékelési módszertan továbbfejlesztése, figyelembe véve azt az [1] és [2] által megvalósított jelentős továbbfejlesztést és egyszerűsítést, melyet a CC/CEM korábbi verzióinak több mint 10 éves tapasztalataiból szűrtek le.

Jelen dokumentum az alábbi kiegészítő fogalmakra épül, s ezeket az alábbi értelemben használja:

Alrendszer: A tervlebontás egyik szintje (lásd még modul). Az alrendszer a TOE terv leírása; ez elősegíti annak magas szintű leírását, hogy a TOE egyes részei mit és hogyan végeznek. Egy alrendszert tovább lehet bontani alacsonyabb szintű alrendszerekre vagy modulokra.

Általános határozat: „Megfelelt" vagy „nem felelt meg" nyilatkozat, amelyet egy értékelő bocsát ki egy értékelés eredményét illetően.

Átvizsgálói határozat: Nyilatkozat, amelyet egy tanúsító szervezet által megbízott tanúsító készít, egy általános határozat megerősítésére vagy elutasítására egy értékelést átvizsgáló tevékenység eredményének alapján.

Biztonsági cél: Szándéknyilatkozat azonosított fenyegetések elleni fellépésről és/vagy meghatározott szervezeti biztonsági szabályzatoknak és feltételezésnek való megfelelésről.

Biztonsági előirányzat: Biztonsági követelmények és előírások olyan összessége, amelyet egy értékelés tárgyára, az értékelés alapjaként használnak.

Biztonsági funkcionalitás: Az értékelés tárgyának mindazon részei, amelyekre az értékelés tárgya biztonsági szabályzatának helyes érvényre juttatásához támaszkodni kell, illetve lehet.

Biztonsági követelmények: Az informatikai biztonsági célok lebontása biztonsági funkcionalitásra (SFR) és garanciára (SAR) vonatkozó szakmai követelmények egy összességére, melyek az értékelés tárgyára és annak üzemeltetési környezetére vonatkoznak.

Biztonsági tulajdonság: Szubjektumokkal, felhasználókkal és/vagy objektumokkal társított olyan információ, amelyet az értékelés tárgyára vonatkozó biztonsági szabályzat érvényre juttatására használnak.

Család: Összetevők egy olyan csoportja, melyek azonos biztonsági célokkal kapcsolatosak.

Csomag: Összetevők egy közbenső kombinációja. Egy csomag olyan összetartozó követelményeket tartalmaz, amelyek biztonsági célok egy adott részhalmazának felelnek meg.

Elem: Oszthatatlan biztonsági követelmény.

Ellenőrizni: (igehasználat követelményen belül): Értékelői határozat előállítása egy egyszerű összehasonlítás segítségével. Értékelői szaktudást nem igényel. Az ezt az igét használó megállapítás a megfeleléseket írja le.

Értelmezés: Séma követelmény tisztázása vagy megerősítése.

Értékadás: Az egyik megengedett művelet összetevőkön.

Értékelés: Védelmi profil, biztonsági előirányzat, vagy az értékelés tárgya felmérése meghatározott szempontok (pl. a CC vagy a MIBÉTS módszertana) alapján.

Értékelési átadandó: Bármely forrás, amelyet az értékelő vagy a tanúsító szervezet kér be a megbízótól vagy fejlesztőtől abból a célból, hogy egy vagy több értékelési vagy értékelést átvizsgáló tevékenységet hajtson végre.

(Értékelési) bizonyíték: Kézzelfogható értékelési átadandó.

Értékelési garanciaszint: A CC. 3 részének olyan garancia-összetevőiből álló csomag, amelyek egy-egy pontot képviselnek a CC előre meghatározott garanciális skáláján.

Értékelési jelentés: Jelentés, amely dokumentálja az általános határozatot és annak indoklását, és amelyet az értékelő állít elő és ad át a tanúsító szervezetnek.

Értékelési séma: Olyan igazgatási és szabályozási keret, amely szerint az értékelő szervezet egy adott közösségben alkalmazza a CC alapelveit.

Értékelés tárgya: Az az informatikai termék, valamint a hozzá kapcsolódó útmutatók, amelyre az értékelés irányul.

Értékelői akció: A CC 3. részben megadott értékelői tevékenység elem. Ezek az akciók vagy közvetlenül értékelői akcióként vannak megadva, vagy pedig közvetett módon, a fejlesztői akciókból vannak származtatva (származtatott értékelői akciók) a CC 3. rész garancia-összetevőin belül.

Értékelői altevékenység: Az egyik garancia-összetevő alkalmazása. Az értékelési módszertan nem közvetlenül garanciacsaládokra irányul, mivel az értékeléseket egy garanciacsaládból származó valamelyik garancia-összetevőre hajtják végre.

Értékelői tevékenység: Az egyik garanciaosztály (ADV, AGD, ALC, ASE, ATE, AVA) alkalmazása.

Észrevételezési jelentés: Jelentés, amelyet az értékelő abból a célból készít, hogy az értékelés során felmerülő kérdések tisztázását kérje, vagy azonosítson egy problémát.

Felhasználó: Az értékelés tárgyán kívüli bármely olyan entitás (humán felhasználó vagy egy külső informatikai entitás), amely kölcsönhatásban áll az értékelés tárgyával.

Feljegyezni (igehasználat követelményen belül): Eljárások, események, megfigyelések, észrevételek és eredmények ismertetésének írott formában, megfelelő részletességgel történő megőrzése abból a célból, hogy lehetővé váljon az értékelés során végrehajtott munka rekonstruálása egy későbbi időpontban.

Formális: Korlátozott szintaktikus nyelven és meghatározott jelentés-tannal kifejezett, jól kidolgozott matematikai fogalmakon alapuló.

Függőség: Két összetevő között függőség lép fel, ha az egyik összetevő önmagában nem elegendő, és egy másik összetevő fennállására támaszkodik.

Garancia: Biztosíték arra nézve, hogy egy egyed megfelel a rá vonatkozó biztonsági céloknak.

Hamisítás: Olyan általános támadási módszer, mely azon alapul, hogy egy támadó megpróbálja a TSF működését befolyásolni (azaz módosítani vagy hatástalanítani).

Határozat: „Megfelelt" , „nem felelt meg" vagy „nem bizonyított" nyilatkozat, amelyet egy értékelő bocsát ki egy értékelői akcióelemet, garancia-összetevőt vagy garanciaosztályt illetően. (Lásd még általános határozat.)

Informális: Természetes nyelven kifejezett.

Ismétlés: Az egyik megengedett művelet összetevőkön.

Jelenteni, jelentésbe foglalni (igehasználat követelményen belül): Az értékelési eredmények és az ezeket alátámasztó anyagok belefoglalása egy értékelési jelentésbe vagy egy észrevételezési jelentésbe.

Kiterjesztés: A biztonsági előirányzat vagy a védelmi profil kiegészítése olyan funkcionális és/vagy biztonsági követelményekkel, amelyek nem szerepelnek a CC 2. illetve 3. részében.

Kiválasztás: Az egyik megengedett művelet összetevőkön.

Konfiguráció kezelés (CM) dokumentáció: CM felhasználói dokumentáció és a CM output dokumentáció együtt.

Konfiguráció kezelés (CM) felhasználói dokumentáció: A CM rendszer részét képező dokumentáció, ami azt írja le, hogy a CM rendszert hogyan határozzák meg és használják.

Konfiguráció kezelés (CM) kimenet: CM-el kapcsolatos eredmények, melyeket a CM rendszer állít elő vagy juttat érvényre (lehetnek dokumentumok, tevékenységek).

Konfiguráció elem: A CM rendszer által kezelt objektum, amit a CM rendszer közvetlenül vagy hivatkozás által rögzít, tárol, a verziószámmal együtt.

Konfiguráció kezelés (CM) eszközök: Azon eszközök, amelyek a CM rendszer kialakítását segítik vagy támogatják.

Konfiguráció kezelés (CM) hozzáférés ellenőrzés: Azon mechanizmusok és eljárások összessége, amelyek azt garantálják, hogy a konfiguráció elemekhez kizárólag az arra jogosultak férhessenek hozzá.

Konfiguráció lista: CM kimeneti dokumentáció, ami felsorolja egy adott termék összes konfiguráció elemét, a kész termék adott verziója szempontjából lényeges elemek pontos verzióazonosítóit. CC kontextusban: ez az értékelt verzió lesz, és a termék értékelt és egyéb verziói közötti megkülönböztetést segíti. A végső CM lista egy adott termék egy adott verziójának elemeit leíró dokumentum.

Konfiguráció kezelés (CM) rendszer: Általános kifejezés egy fejlesztő által használt összes eljárásra és eszközre (ideértve a dokumentációkat), amelyek a termék konfigurációjának fenntartását szolgálják a teljes életciklusban.

Konfiguráció kezelés (CM) rendszer iratok: Azon kimeneti dokumentumok, amelyek a fontos tevékenységeket dokumentáló CM tevékenység során jöttek létre.

Konfiguráció kezelés (CM) terv: A CM dokumentáció része, ami azt írja le, hogyan alkalmazzák a CM rendszert egy adott projekt vagy termék esetén. (A teljes CM rendszer szempontjából ez egy output dokumentum, amit a CM rendszer alkalmazása során készíthetnek el, míg egy konkrét projekt esetén egy felhasználói dokumentum, melyet a projekt tagjai használnak.)

Közvetlen támadás: Olyan általános támadási módszer, mely a permutáción vagy valószínűségen alapuló mechanizmusok feltörésére irányul (pl. az összes lehetséges eset kipróbálásának elvét alkalmazva).

Megkerülés: Olyan általános támadási módszer, mely révén egy támadó megkerülheti a biztonság érvényre juttatását.

Megvizsgálni (igehasználat követelményen belül): Határozat előállítása egy értékelői szaktudást alkalmazó vizsgálat segítségével. Az ezt az igét használó megállapítás meghatározza, hogy mi, és milyen tulajdonságokra vonatkozóan lett vizsgálva.

Modul: A tervlebontás egyik szintje (lásd még alrendszer). A modul a funkcionalitás legspecifikusabb leírása: ez a megvalósítás leírása. A modul segítségével egy fejlesztő további tervezési döntés nélkül képes a TOE leírt részét megvalósítani.

Módszertan: Elvek, eljárások és folyamatok rendszere, amelyet informatikai biztonságértékelésre használnak.

Munkaegység: Az értékelői munka legjobban részletezett szintje. Minden (CEM) értékelői akció egy vagy több munkaegységet foglal magában, amelyek a (CEM) értékelői akción belül csoportosítva vannak a CC tartalom- és bizonyítékbemutatás vagy fejlesztői akcióelem szerint. A CEM-ben és a jelen dokumentumban a munkaegységek ugyanolyan sorrendben vannak bemutatva, mint azok a CC elemek, amelyekből származnak. A munkaegységeket a bal margón elhelyezett szimbólum azonosítja, mint pl. ALC_TAT.1-2. Ebben a szimbólumban az ALC betűcsoport jelöli a CC garanciaosztályt (vagyis az értékelői tevékenységet), az ALC_TAT.1 betűcsoport jelöli a CC garancia-összetevőt (vagyis az értékelői altevékenységet), az utolsó számjegy (2) pedig azt jelöli, hogy ez a második munkaegység az ALC_TAT.1 altevékenységen belül.

Művelet: Az összetevőket pontosan a CC-ben megadottaknak megfelelően lehet használni, de megengedett műveletek alkalmazásával testre is szabhatóak egy meghatározott biztonsági szabályzat kielégítése, illetve egy meghatározott fenyegetés kivédése érdekében. Minden összetevő meghatározza a megengedett műveleteket, azokat a körülményeket, amelyek mellett ezek alkalmazhatók és az alkalmazás végeredményeit. A megengedett műveletek: ismétlés, értékadás, kiválasztás és pontosítás.

Objektum: Az értékelés tárgyának ellenőrzési körén belül található olyan entitás, amely információt tartalmaz vagy fogad, és amelyen szubjektumok műveleteket hajtanak végre.

Osztály: Családok egy olyan csoportja, melyek közös feladatokhoz kapcsolódnak. A CC funkcionális osztályai az alábbi közös célokhoz kapcsolódnak: Biztonsági naplózás (FAU), Kommunikáció (FCO), Kriptográfiai támogatás (FCS), A felhasználói adatok védelme (FDP), Azonosítás és hitelesítés (FIA), Biztonsági menedzsment (FMT), A magántitok védelme (FPR), ATOE biztonsági funkcionalitás védelme (FPT), Erőforrás gazdálkodás (FRU), TOE hozzáférés (FTA), Megbízható útvonal/csatornák (FTP). A CC garanciaosztályai az alábbi közös célokhoz kapcsolódnak: Fejlesztés (ADV), Útmutató dokumentumok (AGD), Életciklus támogatás (ALC), Védelmi profil értékelés (APE), Biztonsági előirányzat értékelés (ASE), Tesztelés (ATE), Sebezhetőség felmérés (AVA), Komponens-összeállítás (ACO). A jelen dokumentum által leírt módszertan az alábbi garanciaosztályokra épül: ASE, ADV, AGD, ALC, ATE és AVA.

Összerendelés: Egyszerű irányított reláció két entitás halmaz között, amely megmutatja, hogy az első halmaz melyik entitása a másik halmaz melyik entitásának felel meg.

Összetevő: Valamely csomag vagy biztonsági előirányzat számára választható elemek legkisebb összessége.

Pontosítás: Az egyik megengedett művelet összetevőkön.

SFR-t érvényre juttató (interfész/alrendszer/modul): A TOE olyan részei (interfész/alrendszer/modul), melyek közvetlen szerepet játszanak valamely SFR megvalósításában a TOE-n.

SFR-t támogató (interfész/alrendszer/modul): A TOE olyan részei (interfész/alrendszer/modul), melyek nem juttatják érvényre az SFR-ket, de ebben alátámasztó szerepet játszanak.

SFR-be nem beavatkozó (interfész/alrendszer/modul): A TOE olyan részei (interfész/alrendszer/modul), melyeknek nincs szerepük az SFR-ek megvalósításában, és valószínűleg a környezetük miatt részei a TSF-nek.

Séma: Szabályok összessége, amely meghatározza az értékelés környezetét, beleértve az informatikai biztonsági értékelések végrehajtásához szükséges szempontokat és módszertant.

Szervezeti biztonsági szabályzat: Egy vagy több biztonsági szabály, eljárás, gyakorlat vagy útmutató, amelyet egy szervezet működéséhez állít fel.

Szolgáltató (működő) rendszer: Egy konkrét informatikai elrendezés meghatározott céllal és üzemeltetési környezettel.

Szubjektum: Az értékelés tárgyának ellenőrzési körén belül található olyan entitás, amely a műveletek végzését kiváltja.

Támadó képesség: Támadás esetén annak érzékelt lehetősége, hogy a támadás sikeres lesz, a támadó szaktudásával, erőforrásaival és motivációjával kifejezve (Lehetséges szintjei: alap, megemelt-alap, közepes, magas, A jelen dokumentumban leírt értékelési módszertan lehetséges szintjei: alap, megemelt-alap).

Termék: Informatikai szoftver, förmver és/ vagy hardver által alkotott csomag, amelyek adott használatra vagy különböző rendszerekbe való beépítésre tervezett funkciókészletet biztosítanak.

Védelmi profil: Olyan megvalósítástól független biztonsági követelményrendszer az értékelés tárgyai egy kategóriájára, amely adott fogyasztói igényeket elégít ki.

Visszaélés (helytelen használat): Olyan általános támadási módszer, mely az alábbiakat igyekszik kihasználni a biztonság érvényre juttatásának megakadályozására: hiányos útmutató dokumentáció, ésszerűtlen útmutatók, a TOE véletlenül rossz konfigurálása, a TSF kikényszerített kivételes viselkedése.

6. Termékekre vonatkozó biztonság értékelési módszertan

6.1. A megbízó és a fejlesztő feladatai egy termék biztonsági értékelésének előkészítésében

6.1.1. Igény biztonságos IT termékekre

Az IT termékek biztonságába vetett bizalomra igen gyakran szükség van.

Jelen dokumentum az IT termékek biztonsága tekintetében az alábbi ([1]-ben lefektetett) megközelítési módot alkalmazza: az IT biztonságba vetett bizalom a fejlesztés, értékelés és üzemeltetés során végrehajtható tevékenységeken keresztül nyerhető el.

Annak érdekében, hogy egy termék informatikai biztonságára vonatkozó követelményeket szabványos, egységes terminológia felhasználásával lehessen megadni, a CC két katalógust határoz meg: a funkcionális biztonsági követelményeket ([1] 2. rész) és a garanciális biztonsági követelményeket ([1] 3. rész), mely utóbbiakat jelen anyag is részletesen ismertet.

A CC funkcionális követelmények a megkívánt biztonsági működésmódot határozzák meg. A garanciális követelmények pedig azt a meggyőződést alapozzák meg, hogy a kinyilvánított biztonsági intézkedések valóban hatékonyak, egyúttal helyesen is lettek megvalósítva.

A CC hasznosításában egyaránt érdekeltek az informatikai termékek felhasználói, fejlesztői és értékelői.

6.1.2. Értékelési garanciaszintek

Egy termék biztonsági értékelését különböző mélységben és szigorúsággal lehet elvégezni, melyet az értékelési garanciaszintek fejeznek ki.

Jelen dokumentum olyan meghatározott garanciaszintek együttesét tartalmazza, amelyeket az [1] által meghatározott garanciaosztályok összetevőinek felhasználásával alakítottak ki. Ezek a garanciaszintek belsőleg konzisztens, általános célú garanciacsomagokat nyújtanak.

Az értékelési garanciaszintek mértéket határoznak meg a biztonsági előirányzatok értékelési követelményeinek méréséhez. Az értékelési garanciaszintek az alábbiakban részletezett garancia-összetevőkből épülnek fel. Minden garancia-összetevő hozzájárul annak garantálásához, hogy az értékelés tárgya valóban kielégíti biztonsági követelményeit.

Az értékelési garanciaszintek egy egyenletesen növekedő skálát alkotnak, melyek az elérhető garanciával, illetve az ezen garanciaszint elérésének lehetőségével és költségével arányosak. A jelen dokumentum által meghatározott értékelési módszertan három hierarchikusan rendezett garanciaszintet határoz meg: alap (A), fokozott (F) és kiemelt (K). A garancia növekedését a szinteken keresztül azzal érik el, hogy ugyanazon garanciaosztály hierarchikusan magasabb (szigorúbb) garancia-összetevőit helyettesítik be, illetve más garanciacsaládokból kiegészítő garancia-összetevőket csatolnak.

6.1.2.1. Az értékelési garanciaszintek áttekintése

A 2. táblázat a három garanciaszintet összegzi. Az oszlopok a garanciaszintek hierarchikusan rendezett halmazát mutatják, míg a sorok a garanciacsaládokat. A mátrixban látható számok egy adott garancia-összetevőt jelentenek, ahol ez értelmezhető.

2. táblázat - Az értékelési garanciaszintek összegzése

Garanciaosztály	**Garanciacsalád**	**Garancia-összetevők az egyes garanciaszinteken**		
		Alap	**Fokozott**	**Kiemelt**
Biztonsági előirányzat értékelés (ASE)	ASE_CCL	1	1	1
	ASE_ECD	1	1	1
	ASE_INT	1	1	1
	ASE_OBJ	2	2	2
	ASE_REQ	2	2	2
	ASE_SPD	1	1	1
	ASE_TSS	1	1	1
Fejlesztés(ADV)	ADV_ARC	1	1	1
	ADV_FSP	2	3	4
	ADV_TDS	1	2	3
	ADV_IMP	-	-	1
Útmutató dokumentumok (AGD)	AGD_PRE	1	1	1
	AGD_OPE	1	1	1

Garanciaosztály	Garanciacsalád	Garancia-összetevők az egyes garanciaszinteken		
		Alap	Fokozott	Kiemelt
Életciklus támogatás (ALC)	ALC_CMC	2	3	4
	ALC_CMS	2	3	4
	ALC_DEL	1	1	1
	ALC_DVS	-	1	1
	ALC_LCD	-	1	1
	ALC_TAT	-	-	1
Tesztelés (ATE)	ATE_FUN	1	1	1
	ATE_COV	1	2	2
	ATE_DPT	-	1	2
	ATE_IND	2	2	2
Sebezhetőség felmérés (AVA)	AVA_VAN	2	2	3

A 2. táblázatból látható, hogy a biztonsági előirányzatra mindhárom garanciaszinten egységes elvárások vonatkoznak. Ezért a következő három alfejezet csak az értékelés tárgyára vonatkozó többi garancia-összetevőt tekinti át. A különbségek szemléltetése érdekében az F és K garanciaszinten vastagított betűtípus jelöli az előző szinthez képest kiegészítő elvárásokat.

6.1.2.2. Alap garanciaszint (A)

Az alap értékelési garanciaszint a fejlesztők részéről csak minimális többletfeladat elvégzését igényli.

Olyan körülmények között használható, amikor a függetlenül garantált biztonság alacsonyabb szintjére van csak szükség, esetleg nem áll rendelkezésre a teljes fejlesztői dokumentum sem. Az alap garanciaszint megegyezik a CC [1] EAL2 garanciaszintjével.

3. táblázat - Az alap garanciaszint garancia-összetevői

Fejlesztés (ALC)	ADV_ARC.1: Biztonsági szerkezet leírás
	ADV_FSP.2: Biztonságot érvényre juttató funkcionális specifikáció
	ADV_TDS.1: Alap terv
	ADV_IMP: -
Útmutató dokumentumok (AGD)	AGD_OPE.1: Üzemeltetési felhasználói útmutató
	AGD_PRE.1: Előkészítő eljárások
Életciklus támogatás (ALC)	ALC_CMC.2: CM rendszer használata
	ALC_CMS.2: A TOE részeinek CM lefedettsége
	ALC_DEL.1: Szállítási eljárások
	ALC_DVS:-
	ALC_LCD:-
	ALC_TAT:-
Tesztelés (ATE)	ATE_FUN.1: Funkcionális tesztelés
	ATE_COV.1: A lefedettség bizonyítéka
	ATE_DPT: -
	ATE_IND.2: Független tesztelés - minta
Sebezhetőség felmérés (AVA)	AVA_VAN.2: Sebezhetőség vizsgálat

6.1.2.3. Fokozott garanciaszint (F)

A fokozott értékelési garanciaszint a fejlesztőktől biztonsági tervezést követel meg. A biztonsági szempontok tervezésben való érvényesítése - a hazai fejlesztői gyakorlatot figyelembe véve - elérhető a kialakult fejlesztői gyakorlat alapvető megváltoztatása nélkül, de jelentős odafigyelést igényel, egyúttal nagyobb garanciát nyújt a helyes és biztonságos megvalósításra.

Olyan körülmények között használható, amikor a függetlenül garantált biztonság fokozott szintjére van szükség, a termék és a fejlesztői környezet mélyreható vizsgálatával. Ezen a garanciaszinten az értékelési feladatok még nem járnak lényeges újratervezési költséggel.

A fokozott garanciaszint megegyezik a CC [1] EAL3 garanciaszintjével.

4. táblázat: A fokozott garanciaszint garancia-összetevői

Fejlesztés(ALC)	ADV_ARC.1: Biztonsági szerkezet leírás
	ADV_FSP.**3: Funkcionális specifikáció teljes összegzéssel**
	ADV_TDS.**2: Szerkezeti terv**
	ADV_IMP: -
Útmutató dokumentumok (AGD)	AGD_OPE.1: Üzemeltetési felhasználói útmutató
	AGD_PRE.1: Előkészítő eljárások
Életciklus támogatás(ALC)	ALC_CMC.**3: Engedélyezéssel kapcsolatos intézkedések**
	ALC_CMS.**3: A megvalósítási reprezentáció CM lefedettsége**
	ALC_DEL.1: Szállítási eljárások
	ALC_DVS.1: A biztonsági intézkedések azonosítása
	ALC_LCD.1: A fejlesztő által meghatározott életciklus modell
	ALC_TAT:-
Tesztelés(ATE)	ATE_FUN.1: Funkcionális tesztelés
	ATE_COV.**2: A lefedettség vizsgálata**
	ATE_DPT.1: Az alap terv tesztelése
	ATE_IND.2: Független tesztelés - minta
Sebezhetőség felmérés (AVA)	AVA_VAN.2: Sebezhetőség vizsgálat

6.1.2.4. Kiemelt garanciaszint (K)

A kiemelt értékelési garanciaszint igen szigorú (de azért a hazai fejlesztési gyakorlatokban már létező) biztonsági technikák alkalmazását várja el a fejlesztőktől.

Olyan körülmények között alkalmazható, ahol a függetlenül garantált biztonság magas szintjére van szükség, s ennek érdekében vállalják a pótlólagos biztonsági technikai munkákat és költségeket.

A kiemelt garanciaszint megegyezik a CC [1] EAL4 garanciaszintjével.

5. táblázat - A kiemelt garanciaszint garancia-összetevői

Fejlesztés (ALC)	ADV_ARC.1: Biztonsági szerkezet leírás
	ADV_FSP. **4: Teljes funkcionális specifikáció**
	ADV_TDS.**3: Alap moduláris terv**
	ADV_IMP: A TSF megvalósítási reprezentációja

Útmutató dokumentumok (AGD)	AGD_OPE.1: Üzemeltetési felhasználói útmutató
	AGD_PRE.1: Előkészítő eljárások
Életciklus támogatás (ALC)	ALC_CMC.**4: A TOE előállítás támogatása, átvételi eljárások és automatizálás**
	ALC_CMS.**4: A probléma követés CM lefedettsége**
	ALC_DEL.1: Szállítási eljárások
	ALC_DVS.1: A biztonsági intézkedések azonosítása
	ALC_LCD.1: A fejlesztő által meghatározott életciklus modell
	ALC_TAT.1: Jól meghatározott fejlesztő eszközök
Tesztelés (ATE)	ATE_FUN.1: Funkcionális tesztelés
	ATE_COV.2: A lefedettség vizsgálata
	ATE_DPT.**2: A biztonságot érvényre juttató modulok tesztelése**
	ATE_IND.2: Független tesztelés - minta
Sebezhetőség felmérés (AVA)	AVA_VAN.**3: Célirányos sebezhetőség vizsgálat**

6.1.3. A fejlesztői feladatok áttekintése

Ez az alfejezet előzetesen összefoglalja azokat a feladatokat, melyeket egy informatikai termék biztonsági értékelése esetén a termék fejlesztőjének, illetve részben az értékelés megbízójának kell elvégeznie. A feladatok részletezése a további alfejezetekben található.

Az első feladat a termék biztonsági értékelés feltételeinek áttekintésével eldönteni az alábbi kérdéseket:

- Milyen garanciaszintű (alap, fokozott, kiemelt) értékelésnek biztosítottak a feltételei?
- Milyen garanciaszintű (A,F,K) értékelésre van igény?

Ezt a feladatot a 6.1.2.1 pont részletezi.

A második feladat a termék biztonsági előirányzatának elkészítése. A biztonsági előirányzat a termék informatikai biztonsági követelményeit tartalmazza, illetve előírja azokat a funkcionális és garanciális biztonsági intézkedéseket, amelyeket a termék (mint a biztonsági értékelés tárgya) ajánl fel a kinyilvánított követelmények kielégítése érdekében. A biztonsági előirányzat alkotja a fejlesztők, az értékelők és a megbízó között létrejött, az értékelés tárgya biztonsági tulajdonságait és az értékelés hatókörét rögzítő megállapodás alapját.

Ezt a feladatot a 6.1.2.2 pont részletezi.

A harmadik feladat a termék biztonsági értékeléséhez szükséges értékelési bizonyítékok elkészítése. Ez a feladat a választott garanciaszinttől (A,F,K) függően különböző (egyre bővülő és szigorodó) elvárásoknak való megfelelést igényel.

A megoldandó feladat részletezése a választott garanciaszinttől függően a 6.1.2.3 – 6.1.2.5 pontokban található meg.

6.1.3.1. Garanciaszint választás (A / F / K)

Az alap (A) garanciaszint akkor alkalmazható, ha:

- a függetlenül garantált biztonság alacsonyabb szintjére van csak szükség.

A fokozott (F) garanciaszint akkor alkalmazható, ha:
- a függetlenül garantált biztonság fokozott szintjére van szükség, a termék és a fejlesztői környezet mélyreható vizsgálatával, és
- a fejlesztők vállalják a biztonsági tervezést (a biztonsági szempontok tervezésben való érvényesítését).

A kiemelt (K) garanciaszint akkor alkalmazható, ha:
- a függetlenül garantált biztonság magas szintjére van szükség,
- a fejlesztők vállalják a pótlólagos biztonsági technikai munkákat és költségeket.

6.1.3.2. Biztonsági előirányzat készítése

Az elkészítendő biztonsági előirányzatra vonatkozó egységes elvárásokat a 6.1.4 alfejezet tekinti át.

6.1.3.3. Értékelési bizonyítékok alap garanciaszint választása esetén (A)

6.1.3.3.1. Biztonsági szerkezet leírás (ADV_ARC.1)

A fejlesztőnek úgy kell megterveznie és megvalósítania a TOE-t, hogy a TSF biztonsági tulajdonságait ne lehessen megkerülni, és hogy az képes legyen megvédeni magát a nem-megbízható aktív egyedek hamisításaitól.

A fejlesztőnek biztosítania kell egy leírást a TSF biztonsági szerkezetéről.

A biztonsági szerkezet leírás tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.2.1 pontban található.

6.1.3.3.2. Biztonságot érvényre juttató funkcionális specifikáció (ADV_FSP.2)

A fejlesztőnek biztosítania kell egy funkcionális specifikációt és ennek visszavezetését az SFR-ekre.

A funkcionális specifikáció és a visszavezetés tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.3.4 pontban található.

6.1.3.3.3. Alap terv (ADV_TDS.1)

A fejlesztőnek biztosítania kell a TOE tervét, valamint egy leképezést a funkcionális specifikáció TSFI-je és a TOE terv rendelkezésre álló legalacsonyabb szintű felbontása között.

A TOE terv és a leképezés tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.4.1 pontban található.

6.1.3.3.4. Előkészítő eljárások (AGD_PRE.1)

A fejlesztőnek biztosítania kell a TOE-t, s benne az előkészítő eljárásokat.

Az előkészítő eljárások tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.2.1 pontban található.

6.1.3.3.5. Üzemeltetési felhasználói útmutató (AGD_OPE.1)

A fejlesztőnek üzemeltetési felhasználói útmutatót kell biztosítania.

Az üzemeltetési felhasználói útmutató tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.6.3.1 pontban található.

6.1.3.3.6. CM rendszer használata (ALC_CMC.2)

A fejlesztőnek meg kell adnia a TOE-t és a TOE egy hivatkozását.

A fejlesztőnek biztosítania kell a konfiguráció kezelés dokumentációt.

A fejlesztőnek egy konfiguráció kezelés rendszert kell használnia.

A fenti bizonyítékok tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.7.2.2 pontban található.

6.1.3.3.7. A TOE részeinek CM lefedettsége (ALC_CMS.2)

A fejlesztőnek meg kell adnia egy TOE-ra vonatkozó konfiguráció listát.
A konfiguráció lista tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.7.3.2 pontban található.

6.1.3.3.8. Szállítási eljárások (ALC_DEL.1)

A fejlesztőnek dokumentálnia kell a TOE vagy annak részei felhasználóhoz való szállításának eljárásait.

A fejlesztőnek használnia kell a szállítási eljárásokat.

A szállítási dokumentáció tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.7.4.1 pontban található.

6.1.3.3.9. Funkcionális tesztelés (ATE_FUN.1)

A fejlesztőnek tesztelnie kell a TSF-t, és ennek eredményeit dokumentálnia kell.

A fejlesztőnek teszt dokumentációt kell biztosítania.

A teszt dokumentáció tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.8.3.1 pontban található.

6.1.3.3.10. A lefedettség bizonyítéka (ATE_COV.1)

A fejlesztőnek biztosítania kell a teszt lefedettség bizonyítékát.

A teszt lefedettség bizonyíték tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.8.3.1 pontban található.

6.1.3.4. Értékelési bizonyítékok fokozott garanciaszint választása esetén (F)

6.1.3.4.1. Biztonsági szerkezet leírás (ADV_ARC.1)

A fejlesztőnek úgy kell megterveznie és megvalósítania a TOE-t, hogy a TSF biztonsági tulajdonságait ne lehessen megkerülni, és hogy az képes legyen megvédeni magát a nem-megbízható aktív egyedek hamisításaitól.

A fejlesztőnek biztosítania kell egy leírást a TSF biztonsági szerkezetéről.

A biztonsági szerkezet leírás tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.2.1 pontban található.

6.1.3.4.2. Funkcionális specifikáció teljes összegzéssel (ADV_FSP.3)

A fejlesztőnek biztosítania kell egy funkcionális specifikációt és ennek visszavezetését az SFR-ekre.

A funkcionális specifikáció és a visszavezetés tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.3.5 pontban található.

6.1.3.4.3. Szerkezeti terv (ADV_TDS.2)

A fejlesztőnek biztosítania kell a TOE tervét, valamint egy leképezést a funkcionális specifikáció TSFI-je és a TOE terv rendelkezésre álló legalacsonyabb szintű felbontása között.

A TOE terv és a leképezés tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.4.2 pontban található.

6.1.3.4.4. Előkészítő eljárások (AGD_PRE.1)

A fejlesztőnek biztosítania kell a TOE-t, s benne az előkészítő eljárásokat.

Az előkészítő eljárások tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.6.2.1 pontban található.

6.1.3.4.5. Üzemeltetési felhasználói útmutató (AGD_OPE.1)

A fejlesztőnek üzemeltetési felhasználói útmutatót kell biztosítania.

Az üzemeltetési felhasználói útmutató tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.6.3.1 pontban található.

6.1.3.4.6. Engedélyezéssel kapcsolatos intézkedések (ALC_CMC.3)

A fejlesztőnek meg kell adnia a TOE-t és a TOE egy hivatkozását.

A fejlesztőnek biztosítania kell a konfiguráció kezelés dokumentációt.

A fejlesztőnek egy konfiguráció kezelés rendszert kell használnia.

A fenti bizonyítékok tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.7.2.3 pontban található.

6.1.3.4.7. A megvalósítási reprezentáció CM lefedettsége (ALC_CMS.3)

A fejlesztőnek meg kell adnia egy TOE-ra vonatkozó konfiguráció listát.

A konfiguráció lista tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.7.3.3 pontban található.

6.1.3.4.8. Szállítási eljárások (ALC_DEL.1)

A fejlesztőnek dokumentálnia kell a TOE vagy annak részei felhasználóhoz való szállításának eljárásait.

A fejlesztőnek használnia kell a szállítási eljárásokat.

A szállítási dokumentáció tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.7.4.1 pontban található.

6.1.3.4.9. A biztonsági intézkedések azonosítása (ALC_DVS.1)

A fejlesztőnek fejlesztés biztonsági dokumentációt kell biztosítania.

A fejlesztés biztonsági dokumentáció tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.7.5.1 pontban található.

6.1.3.4.10. A fejlesztő által meghatározott életciklus modell (ALC_LCD.1)

A fejlesztőnek egy életciklus modellt kell felállítania a TOE fejlesztésére és karbantartására vonatkozóan.

A fejlesztőnek dokumentálnia kell az életciklus modellt.

Az életciklus modell dokumentációjának tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.7.6.1 pontban található.

6.1.3.4.11. Funkcionális tesztelés (ATE_FUN.1)

A fejlesztőnek tesztelnie kell a TSF-t, és ennek eredményeit dokumentálnia kell.

A fejlesztőnek teszt dokumentációt kell biztosítania.

A teszt dokumentáció tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.8.3.1 pontban található.

6.1.3.4.12. A lefedettség vizsgálata (ATE_COV.2)

A fejlesztőnek biztosítania kell a teszt lefedettség elemzését.

A teszt lefedettség elemzés tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.8.3.2 pontban található.

6.1.3.4.13. Az alap terv tesztelése (ATE_DPT.1)

A fejlesztőnek teszt mélység elemzést kell biztosítania.

A teszt mélység elemzés tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.8.4.1 pontban található.

6.1.3.5. Értékelési bizonyítékok kiemelt garanciaszint választása esetén (K)

6.1.3.5.1. Biztonsági szerkezet leírás (ADV_ARC.1)

A fejlesztőnek úgy kell megterveznie és megvalósítania a TOE-t, hogy a TSF biztonsági tulajdonságait ne lehessen megkerülni, és hogy az képes legyen megvédeni magát a nem-megbízható aktív egyedek hamisításaitól.

A fejlesztőnek biztosítania kell egy leírást a TSF biztonsági szerkezetéről.

A biztonsági szerkezet leírás tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.2.1 pontban található.

6.1.3.5.2. Teljes funkcionális specifikáció (ADV_FSP.4)

A fejlesztőnek biztosítania kell egy funkcionális specifikációt és ennek visszavezetését az SFR-ekre.

A funkcionális specifikáció és a visszavezetés tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.3.6 pontban található.

6.1.3.5.3. Alap moduláris terv (ADV_TDS.3)

A fejlesztőnek biztosítania kell a TOE tervét, valamint egy leképezést a funkcionális specifikáció TSFI-je és a TOE terv rendelkezésre álló legalacsonyabb szintű felbontása között.

A TOE terv és a leképezés tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.4.3 pontban található.

6.1.3.5.4. A TSF megvalósítási reprezentációja (ADV_IMP.1)

A fejlesztőnek az egész TSF-re elérhetővé kell tennie a megvalósítási reprezentációt (szoftver estén forráskódot).

A fejlesztőnek egy leképezést kell biztosítania a TOE terv és a megvalósítási reprezentáció egy mintája között.

A megvalósítási reprezentáció és a leképezés tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.5.1 pontban található.

6.1.3.5.5. Előkészítő eljárások (AGD_PRE.1)

A fejlesztőnek biztosítania kell a TOE-t, s benne az előkészítő eljárásokat.

Az előkészítő eljárások tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.6.2.1 pontban található.

6.1.3.5.6. Üzemeltetési felhasználói útmutató (AGD_OPE.1)

A fejlesztőnek üzemeltetési felhasználói útmutatót kell biztosítania.

Az üzemeltetési felhasználói útmutató tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.6.3.1 pontban található.

6.1.3.5.7. A TOE előállítás támogatása, átvételi eljárások és automatizálás (ALC_CMC.4)

A fejlesztőnek meg kell adnia a TOE-t és a TOE egy hivatkozását.

A fejlesztőnek biztosítania kell a konfiguráció kezelés dokumentációt.

A fejlesztőnek egy konfiguráció kezelés rendszert kell használnia.

A fenti bizonyítékok tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.7.2.4 pontban található.

6.1.3.5.8. A probléma követés CM lefedettsége (ALC_CMS.4)

A fejlesztőnek meg kell adnia egy TOE-ra vonatkozó konfiguráció listát.

A konfiguráció lista tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.7.3.4 pontban található.

6.1.3.5.9. Szállítási eljárások (ALC_DEL.1)

A fejlesztőnek dokumentálnia kell a TOE vagy annak részei felhasználóhoz való szállításának eljárásait.

A fejlesztőnek használnia kell a szállítási eljárásokat.

A szállítási dokumentáció tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.7.4.1 pontban található.

6.1.3.5.10. A biztonsági intézkedések azonosítása (ALC_DVS.1)

A fejlesztőnek fejlesztés biztonsági dokumentációt kell biztosítania.

A fejlesztés biztonsági dokumentáció tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.7.5.1 pontban található.

6.1.3.5.11. A fejlesztő által meghatározott életciklus modell (ALC_LCD.1)

A fejlesztőnek egy életciklus modellt kell felállítania a TOE fejlesztésére és karbantartására vonatkozóan.

A fejlesztőnek dokumentálnia kell az életciklus modellt.

Az életciklus modell dokumentációjának tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.7.6.1 pontban található.

6.1.3.5.12. Jól meghatározott fejlesztő eszközök (ALC_TAT.1)

A fejlesztőnek azonosítania kell a TOE-hez használt minden fejlesztő eszközt.

A fejlesztőnek minden fejlesztő eszközre dokumentálnia kell a kiválasztott megvalósítás-függő opciókat.

A fejlesztő eszközök dokumentációjának tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.7.7.2 pontban található.

6.1.3.5.13. Funkcionális tesztelés (ATE_FUN.1)

A fejlesztőnek tesztelnie kell a TSF-t, és ennek eredményeit dokumentálnia kell.

A fejlesztőnek teszt dokumentációt kell biztosítania.

A teszt dokumentáció tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.8.3.1 pontban található.

6.1.3.5.14. A lefedettség vizsgálata (ATE_COV.2)

A fejlesztőnek biztosítania kell a teszt lefedettség elemzését.

A teszt lefedettség elemzés tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.8.3.2 pontban található.

6.1.3.5.15. A biztonságot érvényre juttató modulok tesztelése (ATE_DPT.2)

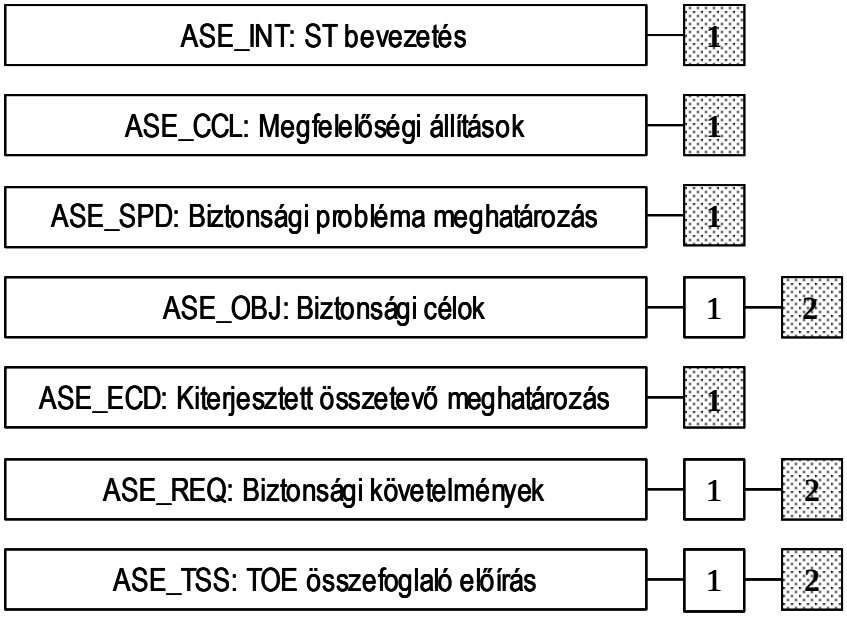
A fejlesztőnek teszt mélység elemzést kell biztosítania.

A teszt mélység elemzés tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.8.4.1 pontban található.

6.1.4. Biztonsági előirányzat (ASE)

6.1.4.1. A biztonsági előirányzat áttekintése

A 2. ábra a biztonsági előirányzat CC garanciaosztály családjait, valamint a családokon belül az összetevők hierarchiáját mutatja. A jelen dokumentum által meghatározott értékelési módszertannak csak az ábrán külön megjelölt garancia-összetevők képezik részét.



2. ábra - A biztonsági előirányzat garanciaosztály felépítése

A biztonsági előirányzat az alábbi részekből áll:

1. ST bevezetés (INT)
- a) ST hivatkozás
- b) TOE hivatkozás
- c) TOE áttekintés
- d) TOE leírás

2. Megfelelőségi nyilatkozatok (CCL)
- a) CC megfelelőség
  - aa) CC verzió (melyhez az ST és TOE megfelelőséget állít)
  - ab) ST megfelelőség a CC 2. részéhez képest (megfelel vagy kiterjeszti)
  - ac) ST megfelelőség a CC 3. részéhez képest (megfelel vagy kiterjeszti)
- b) PP megfelelőség
- c) Biztonsági követelmény csomag megfelelőség (megfelel vagy szigorítja)
- d) A megfelelőségi nyilatkozatok indoklása

3. Biztonsági probléma meghatározás (SPD)
- a) fenyegetések
- b) szervezeti biztonsági szabályzatok
- c) üzemeltetési környezetre vonatkozó feltételezések

4. Biztonsági célok (OBJ)
- a) TOE-ra vonatkozó biztonsági célok
- b) üzemeltetési környezetre vonatkozó biztonsági célok
- c) A biztonsági célok indoklása

5. Kiterjesztett biztonsági követelmények (ECD)

a) kiterjesztett funkcionális biztonsági követelmények
b) kiterjesztett garanciális biztonsági követelmények

6. Biztonsági követelmények (REQ)

a) funkcionális biztonsági követelmények (SFR-ek)
b) garanciális biztonsági követelmények (SAR-ok)
c) indoklás (az SFR-ek teljesítik a TOE összes biztonsági célját)
d) indoklás (miért az adott SAR-t választották.)

7. TOE összefoglaló előírás (TSS)

a) leírás (a TOE hogyan teljesíti az egyes SFR-eket)
b) leírás (a TOE hogyan védi meg magát a fizikai és logikai hamisítás ellen)
c) leírás (a TOE hogyan védi meg magát a megkerülés ellen)

Az alábbi pontok részletezik a biztonsági előirányzat készítésével kapcsolatos fejlesztői feladatokat, illetve a tartalomra és a bemutatás módjára vonatkozó követelményeket.

6.1.4.2. ST bevezetés (INT.1)

Függések: Nincsenek függések

Fejlesztői akcióelemek:

ASE_INT.1.1D A fejlesztőnek biztosítania kell egy ST bevezetést.

A bizonyíték elemek tartalma és bemutatása:

ASE_INT.1.1C Az ST bevezetésnek tartalmaznia kell egy ST hivatkozást, egy TOE hivatkozást, egy TOE áttekintést és egy TOE leírást.

ASE_INT.1.2C Az ST hivatkozásnak egyértelműen azonosítania kell az ST-t.

ASE_INT.1.3C A TOE hivatkozásnak egyértelműen azonosítania kell a TOE-t.

ASE_INT.1.4C A TOE áttekintésnek össze kell foglalnia a TOE használatát és fő biztonsági tulajdonságait.

ASE_INT.1.5C A TOE áttekintésnek azonosítania kell a TOE típusát.

ASE_INT.1.6C A TOE áttekintésnek azonosítania kell a TOE által megkövetelt valamennyi nem TOE hardvert/szoftvert/förmvert.

ASE_INT.1.7C A TOE leírásnak le kell írnia a TOE fizikai hatókörét.

ASE_INT.1.8C A TOE leírásnak le kell írnia a TOE logikai hatókörét.

Értékelői akcióelemek:

ASE_INT.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASE_INT.1.2E Az értékelőnek meg kell erősítenie, hogy a TOE hivatkozás, a TOE áttekintés és a TOE leírás összhangban áll egymással.

6.1.4.3. Megfelelőségi állítások (CCL.1)

Függések: ASE_INT.1, ASE_ECD.1, ASE_REQ.1

Fejlesztői akcióelemek:

ASE_CCL.1.1D A fejlesztőnek biztosítania kell egy megfelelőségi nyilatkozatot.

ASE_CCL.1.2D A fejlesztőnek biztosítania kell egy megfelelőségi nyilatkozat indoklást.
A bizonyíték elemek tartalma és bemutatása:

ASE_CCL.1.1C A megfelelőségi nyilatkozatnak tartalmaznia kell egy CC megfelelőségi nyilatkozatot, ami azonosítja azt a CC verziót, melyhez az ST és a TOE megfelelőséget állít.

ASE_CCL.1.2C A CC megfelelőségi nyilatkozatnak le kell írnia az ST megfelelőségét a CC 2. részéhez képest, hogy az megfelel-e a CC 2. részének vagy kiterjeszti azt.

ASE_CCL.1.3C A CC megfelelőségi nyilatkozatnak le kell írnia az ST megfelelőségét a CC 3. részéhez képest, hogy az megfelel-e a CC 3. részének vagy kiterjeszti azt.

Jelen értékelési módszertan az alap, fokozott és kiemelt garanciaszinteken kívül nem engedi más garanciacsomagok használatát. Mindhárom garanciaszint megfelel a CC 3. résznek, ezért egy biztonsági előirányzatban kizárólag CC 3. rész megfelelést lehet állítani (kiterjesztett CC 3. rész megfelelést nem).

ASE_CCL.1.4C A CC megfelelőségi nyilatkozatnak összhangban kell lennie a kiterjesztett összetevők definíciójával.

ASE_CCL.1.5C A megfelelőségi nyilatkozatnak azonosítania kell minden PP-t és biztonsági követelmény csomagot, melyhez az ST megfelelőséget vállal.

ASE_CCL.1.6C A megfelelőségi nyilatkozatnak le kell írnia az ST minden csomagra vonatkozó megfelelésére, hogy megfelel-e a csomagnak, vagy szigorítja azt.

ASE_CCL.1.7C A megfelelőségi nyilatkozat indoklásának meg kell mutatnia, hogy a TOE típus összhangban van azon PP-k TOE típusával, melyekhez megfelelést állít.

ASE_CCL.1.8C A megfelelőségi nyilatkozat indoklásának meg kell mutatnia, hogy a biztonsági probléma meghatározás állításai összhangban vannak azon PP-k biztonsági probléma meghatározásával, melyekhez az ST megfelelést állít.

ASE_CCL.1.9C A megfelelőségi nyilatkozat indoklásának meg kell mutatnia, hogy a biztonsági célok állításai összhangban vannak azon PP-k biztonsági céljaival, melyekhez az ST megfelelést állít.

ASE_CCL.1.10C A megfelelőségi nyilatkozat indoklásának meg kell mutatnia, hogy a biztonsági követelmények összhangban vannak azon PP-k biztonsági követelményeivel, melyekhez az ST megfelelést állít.

Értékelői akcióelemek:

ASE_CCL.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.4.4. Biztonsági probléma meghatározás (SPD.1)

Függések: Nincsenek függések

Fejlesztői akcióelemek:

ASE_SPD.1.1D A fejlesztőnek biztosítania kell egy biztonsági probléma meghatározást.

A bizonyíték elemek tartalma és bemutatása:

ASE_SPD.1.1C A biztonsági probléma meghatározásnak le kell írnia a fenyegetéseket.

ASE_SPD.1.2C Minden fenyegetést le kell írni a támadó, a támadás tárgyát képező vagyon és a támadó tevékenység szerint.

ASE_SPD.1.3C A biztonsági probléma meghatározásnak le kell írnia a szervezeti biztonsági szabályokat.

ASE_SPD.1.4C A biztonsági probléma meghatározásnak le kell írnia a TOE üzemeltetési környezetére vonatkozó feltételezéseket.

Értékelői akcióelemek:

ASE_SPD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.4.5. Biztonsági célok (OBJ.2)

Függések: Nincsenek függések

Fejlesztői akcióelemek:

ASE_OBJ.2.1D A fejlesztőnek biztosítania kell egy biztonsági célokról szóló nyilatkozatot.

ASE_OBJ.2.2D A fejlesztőnek biztosítania kell egy biztonsági célok indoklást.
A bizonyíték elemek tartalma és bemutatása:

ASE_OBJ.2.1C A biztonsági célokról szóló nyilatkozatnak le kell írnia a TOE-ra vonatkozó biztonsági célokat, valamint az üzemeltetési környezetre vonatkozó biztonsági célokat.

ASE_OBJ.2.2C A biztonsági célok indoklásának minden TOE-ra vonatkozó biztonsági célt vissza kell vezetnie az adott biztonsági cél által kivédett fenyegetésekre, valamint az adott biztonsági cél által érvényre juttatott szervezeti biztonsági szabályzatokra.

ASE_OBJ.2.3C A biztonsági célok indoklásának minden üzemeltetési környezetre vonatkozó biztonsági célt vissza kell vezetnie az adott biztonsági cél által kivédett fenyegetésekre, az adott biztonsági cél által érvényre juttatott szervezeti biztonsági szabályzatokra, valamint az adott biztonsági cél által támasztott feltételezésekre.

ASE_OBJ.2.4C A biztonsági célok indokolásának szemléltetnie kell, hogy a biztonsági célok lefednek minden fenyegetést.

ASE_OBJ.2.5C A biztonsági célok indokolásának szemléltetnie kell, hogy a biztonsági célok érvényre juttatják az összes szervezeti biztonsági szabályzatot.

ASE_OBJ.2.6C A biztonsági célok indokolásának szemléltetnie kell, hogy az üzemeltetési környezetre vonatkozó biztonsági célok az összes feltételezést igénylik.
Értékelői akcióelemek:

ASE_OBJ.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.4.6. Kiterjesztett biztonsági követelmények (ECD.1)

Függések: Nincsenek függések

Fejlesztői akcióelemek:

ASE_ECD.1.1D A fejlesztőnek biztosítania kell egy biztonsági követelményekről szóló nyilatkozatot.

ASE_ECD.1.2D A fejlesztőnek biztosítania kell egy kiterjesztett összetevők meghatározást.

A bizonyíték elemek tartalma és bemutatása:

ASE_ECD.1.1C A biztonsági követelményekről szóló nyilatkozatnak azonosítania kell minden kiterjesztett biztonsági követelményt.

ASE_ECD.1.2C A kiterjesztett összetevők meghatározásának minden kiterjesztett biztonsági követelményre meg kell határoznia egy kiterjesztett összetevőt.

ASE_ECD.1.3C A kiterjesztett összetevők meghatározásának le kell írnia, hogy az egyes kiterjesztett összetevők hogyan kapcsolódnak a meglévő CC összetevőkhöz, családokhoz és osztályokhoz.

ASE_ECD.1.4C A kiterjesztett összetevők meghatározásának a meglévő CC összetevőket, családokat, osztályokat és módszertant kell használnia megjelenítési modellként.

ASE_ECD.1.5C A kiterjesztett összetevőknek mérhető és objektív elemekből kell állniuk, hogy megfelelőségük vagy nem megfelelőségük kimutatható legyen.

Jelen értékelési módszertan az alap, fokozott és kiemelt garanciaszinteken kívül nem engedi más garanciacsomagok használatát. Mindhárom garanciaszint megfelel a CC 3. résznek, ezért egy biztonsági előirányzatban kizárólag a CC 2. részében meghatározott funkcionális biztonsági követelményeket lehet kiterjeszteni (a CC 3. részében meghatározott garanciális biztonsági követelményeket nem).

Értékelői akcióelemek:

ASE_ECD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASE_ECD.1.2E Az értékelőnek meg kell erősítenie, hogy nincs olyan kiterjesztett összetevő, amely egyértelműen kifejezhető lenne a meglévő összetevők segítségével.

6.1.4.7. Biztonsági követelmények (REQ.2)

Függések: ASE_OBJ.2, ASE_ECD.1

Fejlesztői akcióelemek:

ASE_REQ.2.1D A fejlesztőnek biztosítania kell egy biztonsági követelményekről szóló nyilatkozatot.

ASE_REQ.2.2D A fejlesztőnek biztosítania kell egy biztonsági követelmények indoklást.

A bizonyíték elemek tartalma és bemutatása:

ASE_REQ.2.1C A biztonsági követelményekről szóló nyilatkozatnak le kell írnia az SFR-ket és az SAR-eket.

ASE_REQ.2.2C Az SFR-ekben és SAR-ekben használt minden szubjektumot, objektumot, műveletet, biztonsági tulajdonságot, külső egyedet és egyéb terminológiai egységet definiálni kell.

ASE_REQ.2.3C A biztonsági követelményekről szóló nyilatkozatnak azonosítania kell a biztonsági követelményekben szereplő összes műveletet.

ASE_REQ.2.4C Minden műveletet helyesen kell végrehajtani.

ASE_REQ.2.5C A biztonsági követelmények minden függési viszonyát vagy teljesíteni kell, vagy a biztonsági követelmények indoklásának igazolnia kell a függés nem teljesítését.

ASE_REQ.2.6C A biztonság követelmények indoklásában vissza kell vezetni minden SFR-t a TOE biztonsági céljaira.

ASE_REQ.2.7C A biztonsági követelmények indoklásának meg kell mutatnia, hogy az SFR-ek teljesítik a TOE összes biztonsági célját.

ASE_REQ.2.8C A biztonsági követelmények indoklásának meg kell magyaráznia, hogy miért az adott SAR-t választották.

ASE_REQ.2.9C A biztonsági követelményekről szóló nyilatkozatnak belső ellentmondásoktól mentesnek kell lennie.

Értékelői akcióelemek:

ASE_REQ.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.4.8. TOE összefoglaló előírás (TSS.2)

Függések: ASE_INT.1, ASE_REQ.1

Fejlesztői akcióelemek:

ASE_TSS.2.1D A fejlesztőnek biztosítania kell egy TOE összefoglaló előírást.

A bizonyíték elemek tartalma és bemutatása:

ASE_TSS.2.1C A TOE összefoglaló előírásnak le kell írnia, hogy a TOE hogyan teljesíti az egyes SFR-eket.

ASE_TSS.2.2C A TOE összefoglaló előírásnak le kell írnia, hogy a TOE hogyan védi meg magát a fizikai és a logikai hamisítás ellen.

ASE_TSS.2.3C A TOE összefoglaló előírásnak le kell írnia, hogy a TOE hogyan védi meg magát a megkerülés ellen.

Értékelői akcióelemek:

ASE_TSS.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASE_TSS.2.2E Az értékelőnek meg kell erősítenie, hogy a TOE összefoglaló előírás összhangban van a TOE áttekintéssel és a TOE leírással, nem mond ellent azoknak.

6.1.5. Fejlesztés garanciaosztály (ADV)

6.1.5.1. A Fejlesztés garanciaosztály áttekintése

A Fejlesztés garanciaosztály követelményei információkat nyújtanak a TOE-ról. Az ezen információk segítségével nyert ismeretek szolgáltatnak alapot a TOE-n végrehajtott sebezhetőség vizsgálatnak és tesztelésnek, az AVA és ATE osztályban leírtak szerint.

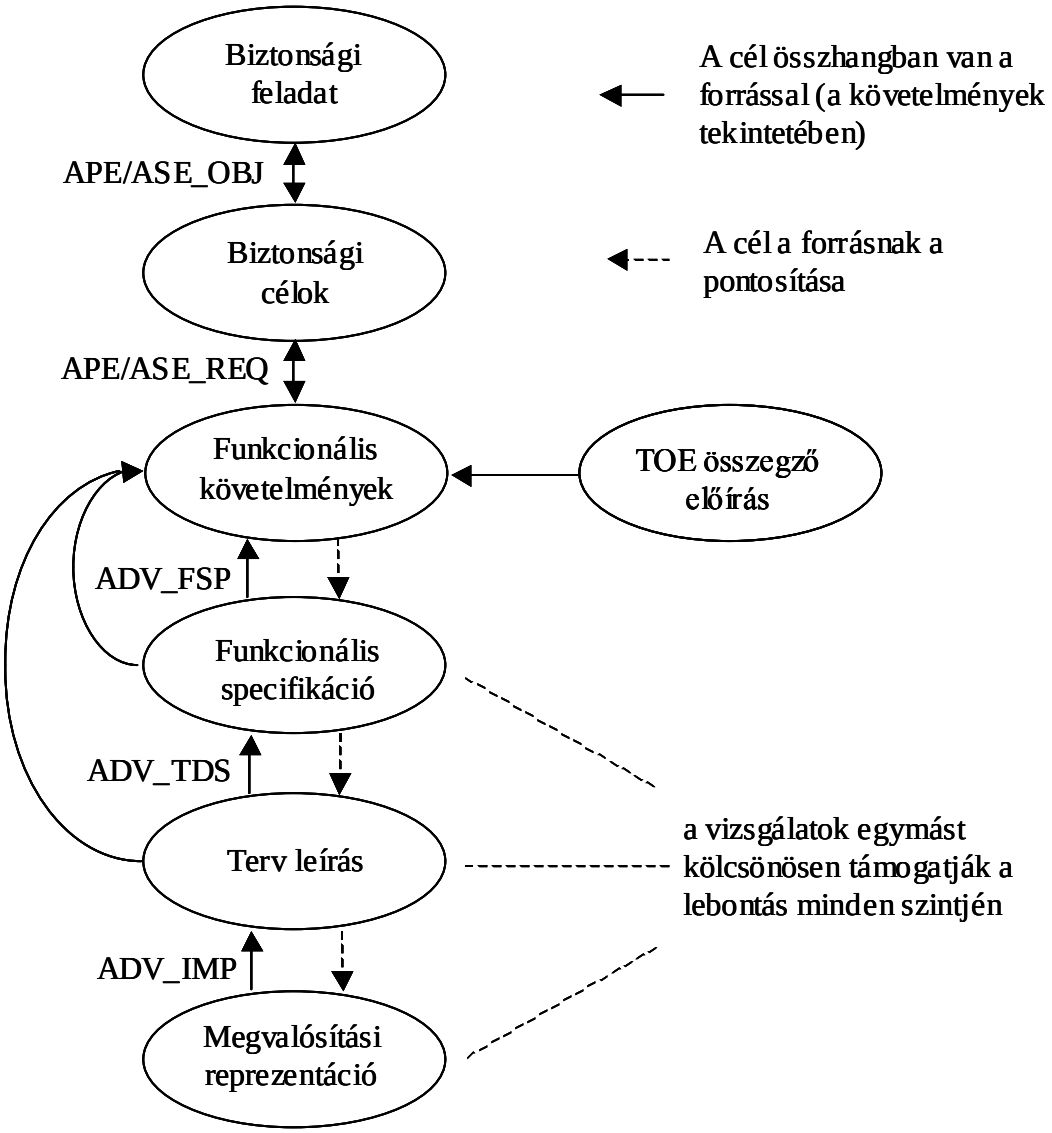
A Fejlesztés osztály 4 követelmény családot ölel fel a TSF felépítésére és megjelenítésére, az absztrakció különböző szintjei és különböző formái mellett. Ezek a családok a következőket foglalják magukban:

- követelmények az SFR-ek tervezésére és megvalósítására vonatkozó leírásokra, a különböző absztrakciós szintek mellett (ADV_FSP, ADV_TDS, ADV_IMP);
- követelmények a biztonsági funkcionalitás szerkezet-orientált tulajdonságainak a leírására, a tartomány szétválasztásra, a TSF önvédelmére és nem-megkerülhetőségére (ADV_ARC).

Egy TOE biztonsági funkcionalitásának a dokumentálásakor két tulajdonságot kell bizonyítani. Az első tulajdonság az, hogy a biztonsági funkcionalitás helyesen működik; vagyis a specifikáltaknak megfelelően teljesít. A második, vitathatatlanul nehezebben bizonyítható tulajdonság, hogy a TOE-t nem lehet olyan módon használni, ami a biztonsági funkcionalitást lerontja, vagy megkerüli. E két tulajdonság némileg eltérő megközelítési módot kíván meg a vizsgálatoknál, emiatt az ADV családjait e különböző megközelítési módok támogatására strukturálták. A „Funkcionális specifikáció” (ADV_FSP), a „TOE terv” (ADV_TDS) és a „Megvalósítási reprezentáció” (ADV_IMP) családok az első tulajdonsággal foglalkoznak, vagyis a biztonsági funkcionalitás specifikálásával. A „Biztonsági szerkezet” (ADV_ARC) család pedig a második tulajdonsággal foglalkozik, azaz a TOE terv olyan specifikálásával, ami bizonyítja, hogy a biztonsági funkcionalitást nem lehet lerontani vagy megkerülni. Meg kell jegyezni, hogy mindkét tulajdonságot át kell látni: minél jobban meggyőződik valaki a tulajdonságok teljesüléséről, annál megbízhatóbb a TOE. A család összetevőit úgy tervezték, hogy az összetevők hierarchikus növekedésével egyre nagyobb garancia nyerhető.

Az első tulajdonságot megcélzó családokra vonatkozó alapelv a tervezés szintekre bontása. Legmagasabb szinten a TSF funkcionális specifikációja áll, a csatlakozási felületek (interfészek) szempontjából (leírja, hogy a TSF hogyan viselkedik a TSF-hez érkező szolgáltatás kérelmek és az ezekre történő válaszok szempontjából), amely a TSF-et (a megkívánt garanciától és a TOE bonyolultságától függően) kisebb egységekre bontja le, ismerteti, hogy a TSF hogyan teljesíti a funkcióit (a garanciaszintnek megfelelő részletességgel), valamint bemutatja a TSF megvalósítását. A részletezett szinteket a többi

szint teljességének és helyességének a megállapítására használják, amely garantálja, hogy a szintek kölcsönösen támogatják egymást. A különböző TSF reprezentációkra (megjelenési formákra) vonatkozó követelményeket különböző családokba sorolták, ami lehetővé teszi az ST szerzője számára, hogy specifikálja, hogy mely TSF reprezentációk szükségesek. A megválasztott szint szabja meg a megkívánt/megszerzett garanciát.



3. ábra - Az ADV családok egymás közötti és más osztályokkal való kapcsolódásai

A 3. ábra vázolja az ADV osztály különböző TSF reprezentációi közötti összefüggéseket, valamint ezek összefüggéseit a többi osztállyal. Az ábrán látható módon az ASE osztály az SFR-ek és a TOE biztonsági céljai közötti megfelelésekre vonatkozó követelményeket határozza meg. Az ASE osztály a biztonsági célok és SFR-ek közötti összefüggések mellett követelményeket határoz meg a TOE összefoglaló előírásra is, amely kifejti, hogy a TOE hogyan felel meg az SFR-eknek. Minden garanciacsalád, amely egy meghatározott TSF reprezentációra vonatkozik (vagyis a „Funkcionális specifikáció” (ADV_FSP), a „TOE terv” (ADV_TDS) és a „Megvalósítási reprezentáció” (ADV_IMP)), az adott TSF reprezentáció és

az SFR-ek közötti kapcsolatra vonatkozó követelményeket definiálja. Minden lebontásnak pontosan vissza kell tükröznie minden más lebontást (vagyis ezeknek kölcsönösen alá kell támasztaniuk egymást); a fejlesztőnek meg kell adnia a nyomkövetéseket az összetevők utolsó .C elemeinél. Az erre a tényezőre vonatkozó garanciát annak a vizsgálatnak a során kell megszerezni, amely az egyes, további lebontási szintekre (rekurzív módon) hivatkozó lebontási szintekre vonatkozik, és amelyet egy meghatározott lebontási szint vizsgálatának a folyamán végeznek el; az értékelőnek ellenőriznie kell a megfeleltetést a második .E elem részeként. A szóbanforgó lebontási szintekből nyert megértés képezi az alapját a funkcionális és áthatolás tesztelésnek.

Az ADV_ARC család sincs feltüntetve az ábrán, mivel ez a TSF szerkezeti helyességére vonatkozik, nem pedig annak megjelenési formájára. Az ADV_ARC annak a tulajdonságnak a vizsgálatára vonatkozik, hogy a TOE-nak nem lehet megkerülni vagy lerontatni a biztonsági funkcionalitását.

A TOE biztonsági funkcionalitása (TSF) mindazokból a TOE részekből áll, amelyekre az SFR-ek érvényre juttatásánál támaszkodni kell. A TSF magában foglalja azt a funkcionalitást, amely az SFR-eket közvetlenül érvényre juttatja, és azt a funkcionalitást is, amely, bár nem juttatja közvetlenül érvényre az SFR-eket, közvetett módon hozzájárul azok érvényre juttatásához, beleértve az olyan funkcionalitást is, amelyek képesek az SFR-ek megsértésére. Ez magában foglalja a TOE azon részeit, melyeket indításkor hívnak meg, és amelyek felelősek azért, hogy a TOE-t a kezdeti biztonságos állapotba hozzák.

Az ADV családok összetevőinek kialakításánál számos fontos elgondolást használtak fel. Az alábbiak röviden bevezetik ezeket, bővebb magyarázatuk a családokra vonatkozó alkalmazási megjegyzésekben található.

Az egyik legalapvetőbb elgondolás az, hogy egyre több információ igénybe vehetőségével egyre nagyobb garancia nyerhető arról, hogy a biztonsági funkcionalitás 1) helyesen lett megvalósítva; 2) nem lehet lerontani; és 3) nem lehet megkerülni. Ez elérhető annak ellenőrzésén keresztül, hogy a dokumentáció helyes és összhangban áll a többi dokumentációval, illetve olyan információk szolgáltatásán keresztül, amelyek felhasználhatók a (funkcionális és áthatolás) tesztelési tevékenységek átfogóságának a biztosítására. Mindez tükröződik a család összetevőinek a szintezésében. Általában az összetevőket a megadandó (és következésképpen vizsgálandó) információ mennyiségén alapulva szintezik.

Általában a TSF eléggé bonyolult ahhoz, hogy olyan részei is vannak, amelyek a többinél elmélyültebb vizsgálatokat igényelnek. A szóbanforgó részek meghatározása sajnos meglehetősen szubjektív, ennélfogva a terminológiát és az összetevőket úgy határozták meg, hogy a garanciaszint növekedésével annak meghatározásának a felelőssége, hogy a TSF mely részeit kell részletesen vizsgálni, a fejlesztőről áttolódik az értékelőre. Ezen elgondolás kifejezésének az elősegítésére az alábbi terminológia került bevezetésre. Meg kell jegyezni, hogy az osztály családjaiban ezt a terminológiát akkor használják, amikor a TOE SFR-rel kapcsolatos részeit juttatják kifejezésre (vagyis a „Funkcionális specifikáció” (ADV_FSP), a „TOE terv” (ADV_TDS) és a „Megvalósítási reprezentáció” (ADV_IMP) családokhoz tartozó elemeknél és munkaegységeknél). Bár az általános elképzelés (hogy a TOE bizonyos részei érdekesebbek, mint a többiek) más családokra is érvényes, az elvárt garancia megszerzésére irányuló kritériumokat eltérő módon fejezik ki.

A TSF minden része fontos biztonsági szempontból, ami azt jelenti, hogy ezeknek kell megőrizniük a TOE biztonságát, ahogyan ez a SFR-ekben, illetve a tartomány szétválasztásra és nem-megkerülhetőségre vonatkozó követelményekben kifejeződik. A biztonsági fontosság egyik oldala az a mérték, amilyen fokig a TSF egy része érvényre juttat egy biztonsági követelményt. Minthogy a TOE különböző részei különböző szerepeket játszanak a biztonsági követelmények érvényre juttatásában (vagy egyáltalán nincs szerepük ebben), ez egy SFR fontossági sorrendet alakít ki: ennek a sorrendnek az egyik végén a TOE azon részei állnak, amelyeket ***SFR-t érvényre juttató***knak neveznek. Az ilyen részek közvetlen szerepet játszanak valamely SFR megvalósításában a TOE-n. Az ilyen SFR-ek olyan funkcionalitásra utalnak, amelyet az ST-ben leírt SFR-ek egyike nyújt. Meg kell jegyezni, hogy annak a definícióját, hogy szerepet játszik az SFR-t érvényre juttató funkcionalitásban, lehetetlen kvantitatív módon kifejezni. Például egy belátáson alapuló hozzáférés ellenőrzési (DAC, Discretionary Access Control) mechanizmus megvalósításánál az SFR-t érvényre juttatásnak egy nagyon szűk nézete lehet a kódnak az a néhány sora, amely ténylegesen végrehajtja egy szubjektum jellemzőinek az ellenőrzését az objektum jellemzőivel összehasonlítva. Egy tágabb nézet magában foglalhatja a szoftver entitást (például C függvényt), amely a néhány kód-sort tartalmazza. A tágabb nézet magában foglalhatja a C függvénynek a meghívóit is, minthogy ezek lehetnek felelősek a jellemző-ellenőrzés által visszaadott döntés érvényre juttatásáért. Egy még tágabb nézet magában foglalhat bármely kódot a szóbanforgó C függvény meghívásainak fájában (vagy ennek programozási megfelelőjében a használt megvalósítási nyelvnél), például egy rendezési funkciót, amely a hozzáférés ellenőrzési lista bejegyzéseit sorba rendezi egy első-egyezés algoritmus megvalósításnál. Egy bizonyos ponton a komponens nem is annyira érvényre juttatja a biztonsági szabályt, hanem inkább alátámasztó szerepet játszik; az ilyen komponenseket ***SFR-t támogató***nak nevezik.

Az SFR-t támogató funkcionalitás egyik jellemzőjeként megbíznak abban, hogy hiba mentes működésével megőrzi az SFR megvalósítás helyességét. Az ilyen funkcionalitás függhet az SFR-t érvényre juttató funkcionalitástól, de a függőség általában funkcionális szintű; például memória kezelés, buffer kezelés, stb. A biztonsági fontossági sorrendben tovább lefelé haladva következik az a funkcionalitás, amelyet az ***SFR-be nem beavatkozó*** funkcionalitásnak neveznek. Az ilyen funkcionalitásnak nincs szerepe az SFR-ek megvalósításában, és valószínűleg a környezete miatt része a TSF-nek; például valamilyen kód, amely privilegizált hardver módban fut egy operációs rendszeren. Szükséges, hogy ezt a TOE részének tekintsék, mert ha meghamisítják (vagy rosszindulatú kóddal helyettesítik), akkor leronthatja egy SFR helyes működését annak következtében, hogy privilegizált hardver módban fut. Példa lehet egy SFR-be nem beavatkozó funkcionalitásra egy matematikai lebegőpontos művelet készlet, amelyet gyorsasági megfontolásokból kernel módban valósítottak meg.

A „Biztonsági szerkezet” (ADV_ARC) család azokról a követelményekről és a TOE olyan vizsgálatáról gondoskodik, amelyek a tartomány szétválasztás, a önvédelem és a nem-megkerülhetőség tulajdonságokon alapulnak. Ezek a tulajdonságok annyiban kapcsolódnak az SFR-ekhez, hogy ha ezek a tulajdonságok nincsenek meg, akkor ez valószínűleg az SFR-eket megvalósító mechanizmusok hibájához fog vezetni. Az ezekhez a tulajdonságokhoz kapcsolódó funkcionalitást és tervezést nem tekintik a fent ismertetett sorrend részének, hanem elkülönítetten kezelik az alapvetően eltérő természetük és vizsgálati követelményeik miatt.

Az SFR-ek megvalósításának (SFR-t érvényre juttató és SFR-t támogató funkcionalitás), illetve a TOE bizonyos értelemben alapvető biztonsági tulajdonságai megvalósításának (köztük az inicializálás, az önvédelem és a nem-megkerülhetőség kérdései) a vizsgálatában az a különbség, hogy az SFR-hez kapcsolódó funkcionalitás többé-kevésbé közvetlenül látható és viszonylag könnyen tesztelhető, míg a inicializálási, önvédelmi és nem-megkerülhetőségi tulajdonságok különböző mértékű vizsgálatokat igényelnek egy jóval szélesebb körű funkcionalitást érintően. Ugyanakkor az adott tulajdonságok vizsgálatának mélysége is változni fog a TOE tervétől függően. Az ADV családokat úgy alakították ki, hogy ezt egy külön család („Biztonsági szerkezet, ADV_ARC) veszi figyelembe, amelyet az inicializálás, az önvédelem és a nem-megkerülhetőség követelményeinek szenteltek, míg a többi család az SFR-eket érvényre juttató és támogató funkcionalitás vizsgálatával foglalkozik.

Nem feltétlenül szükséges, hogy minden TSF reprezentáció különálló dokumentumban legyen, még azokban az esetekben sem, amikor az absztrakció több szintjéhez külön leírás szükséges. Egyetlen dokumentum egynél több TSF reprezentáció dokumentációs követelményeit is kielégítheti, mivel az adott TSF reprezentációkról az információt követelik meg, s nem a keletkező dokumentum struktúrát. Azokban az esetekben, amikor több TSF reprezentáció van összefogva egyetlen dokumentumban, a fejlesztőnek meg kell jelölnie, hogy a dokumentum mely részei mely követelményeket elégítik ki.

Ez az osztály háromféle specifikálási stílust teszt kötelezővé: az informális, a félformális és a formális stílust. A funkcionális specifikációnak és a TOE terv dokumentációnak mindig vagy informális, vagy félformális stílusúnak kell lennie. Egy félformális stílus csökkenti a félreérthetőségeket ezekben a dokumentumokban egy informális bemutatással szemben. Formális specifikáció ugyancsak megkövetelhető a félformális bemutatás kiegészítéseként; ennek az a jelentősége, hogy a TSF-nek egynél többféle leírása fokozott garanciát nyújt arra, hogy a TSF-et teljesen és pontosan specifikálták.

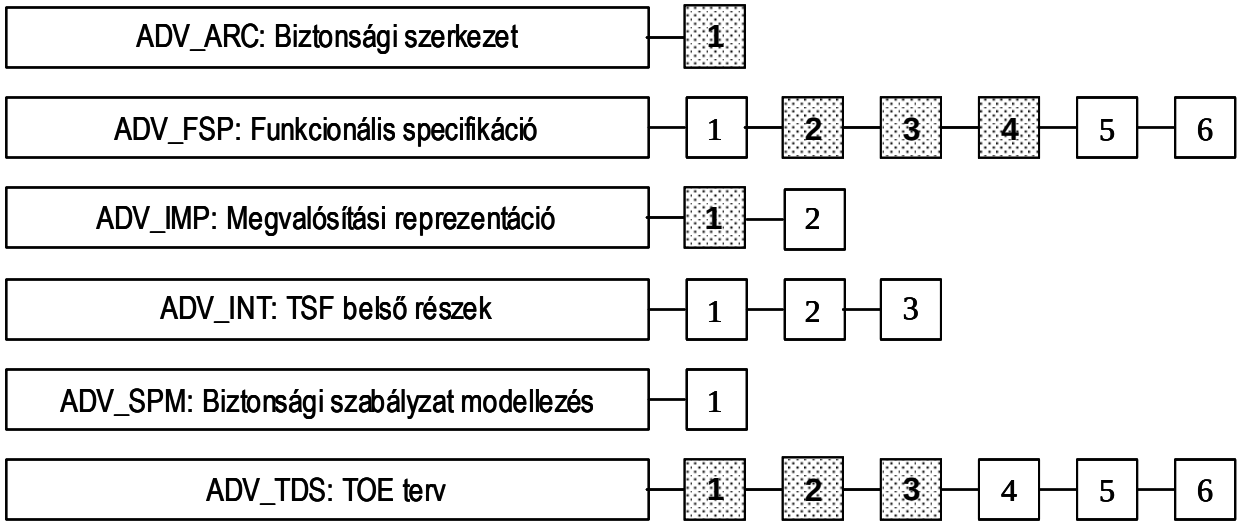
Egy informális specifikáció természetes nyelven elbeszélő formában van megírva. A természetes nyelvet itt úgy kell használni, ahogyan az a kommunikációt kifejezi bármely általánosan használt nyelven (pl. magyar, német, angol). Egy informális specifikációra nem vonatkozik semmilyen jelölésbeli vagy speciális kikötés a szóbanforgó nyelvre megkövetelt szokásos konvenciókon túl (pl. nyelvtan és szintaxis). Bár nincsenek jelölésbeli megkötések, azt elvárják, hogy az informális specifikáció adja meg azoknak a kifejezéseknek a jól meghatározott értelmezését, amelyeket a szokásos használattól eltérő szövegösszefüggésben használnak.

A félformális és informális dokumentumok közötti különbség csak a megformázás vagy megjelenítés kérdése: egy félformális jelölésrendszer magában foglal olyan dolgokat, mint pl. közvetlen fogalom-meghatározások, szabványos bemutatás formátum stb. Egy szabványos bemutatás sablont félformális specifikáció ír le. A bemutatásnak a fogalmakat következetesen kell használnia, ha természetes nyelven íródott. A bemutatás használhat jobban strukturált nyelveket/diagramokat (pl. adatáramlási, állapot-átmeneti, entitás-összefüggési, adatstruktúra és eljárás- vagy programstruktúra diagramokat). Akár diagramokon, akár természetes nyelven alapszik egy bemutatás, számos konvenciót be kell tartani. A fogalom meghatározás rész közvetlenül meghatározza a pontosan és következetesen használandó szavakat. Hasonlóképpen, a szabványosított formátum arra utal, hogy különös figyelmet fordítottak a

dokumentum tervszerű előkészítésére az érthetőséget maximalizáló módon. A TSF alapvetően eltérő részeihez tartozhatnak eltérő félformális jelölési konvenciók és bemutatási stílusok (amennyiben az eltérő „félformális jelölések” száma kicsi); ez még megfelel a félformális bemutatás fogalmának.

Egy formális specifikációt olyan jelölésrendszerben írtak meg, amely jól megalapozott matematikai fogalmakon nyugszik, és általában alátámasztó magyarázó (informális) szövegek kísérik. A szóbanforgó matematikai fogalmakat használják arra, hogy a jelölésrendszer szintaxisát és szemantikáját definiálják, és meghatározzák azokat a bizonyítási szabályokat, amelyek alátámasztják a logikai érvelést. A formális jelölésrendszert alátámasztó szintaktikai és szemantikai szabályok határozzák meg, hogy hogyan kell a szerkezeti elemeket egyértelműen felismerni, és azok jelentését meghatározni. Bizonyítékra van szükség az ellentmondás mentesség kimutathatóságára, és a jelölésrendszert alátámasztó minden szabályt definiálni kell, vagy meg kell hivatkozni.

A 4. ábra az ADV CC garanciaosztályon belüli családokat, s a családokon belül az összetevők hierarchiáját mutatja. A jelen dokumentum által meghatározott értékelési módszertannak csak az ábrán külön megjelölt garancia-összetevők képezik részét.



4. ábra - A fejlesztés garanciaosztály felépítése

6.1.5.2. Biztonsági szerkezet (ADV_ARC)

Ennek a garanciacsaládnak az a célja, hogy a fejlesztő leírást biztosítson a TSF biztonsági szerkezetéről. Ez lehetővé teszi olyan információk vizsgálatát, melyek a TSF-hez benyújtott további bizonyítékokhoz társulva megerősíti, hogy a TSF megvalósítja a kívánt tulajdonságokat. A biztonsági szerkezet leírása alátámasztja azt a közvetett állítást, hogy a TOE biztonsági vizsgálata megvalósítható a TSF vizsgálatával; egy megbízható architektúra nélkül a teljes TOE funkcionalitást vizsgálni kellene.

Ez a család csak egy összetevőt tartalmaz.

Az önvédelem, a tartomány szétválasztás és a nem-megkerülhetőség tulajdonságokat elkülönítették a CC 2. részbeli SFR-ek által kifejezett biztonsági funkcionalitástól, minthogy ezek nagyrészt nem rendelkeznek közvetlenül megfigyelhető TSF interfésszel. Ezek inkább olyan tulajdonságai a TSF-nek, amelyeket a TOE és TSF tervezésén keresztül valósítanak meg, és amelyeket a szóbanforgó terv helyes megvalósításával juttatnak érvényre.

Az e családban alkalmazott megközelítési mód szerint a fejlesztőnek a fent említett tulajdonságokkal bíró TSF-et kell terveznie és szolgáltatnia, valamint a TSF adott tulajdonságait megmagyarázó bizonyítékokat kell nyújtania (dokumentáció formájában). A magyarázatot ugyanolyan szinten kell részletezni, mint a TOE SFR-t érvényre juttató elemeit a TOE terv dokumentumban. Az értékelő felelőssége a bizonyíték áttekintése, valamint a TOE-hez és TSF-hez átadott egyéb bizonyítékokkal társítva annak megállapítsa, hogy a tulajdonságok megvalósulnak-e.

Az SFR-eket megvalósító biztonsági funkcionalitás specifikáció (a „Funkcionális specifikáció”-ban (ADV_FSP) és a „TOE terv”-ben (ADV_TDS)) nem ismertetni szükségszerűen az önvédelem és a nem-megkerülhetőség megvalósítására alkalmazott mechanizmusokat (pl. memória-kezelési mechanizmusok). Ennélfogva ahhoz az anyaghoz, amelynek garanciát kell nyújtania a szóbanforgó követelmények megvalósulására, jobban megfelel egy olyan bemutatás, amely elkülönül a TSF terv ADV_FSP-ben és ADV_TDS-ben kifejezésre juttatott lebontásától. Ebből nem következik, hogy az ezen összetevő által megkívánt biztonsági szerkezet leírás nem hivatkozhat a terv lebontás anyagaira, vagy nem hasznosíthatja azokat; de a lebontási dokumentációban lévő részletek nagy része valószínűleg nem lesz fontos a biztonsági szerkezetet leíró dokumentumhoz nyújtandó indokláshoz.

A szerkezeti megbízhatóság leírását egy fejlesztői sebezhetőség vizsgálatnak lehet képzelni, amelyben a fejlesztő indokolást nyújt arra, hogy a TSF mi miatt megbízható, és mi miatt juttatja érvényre az SFR-eket. Ha a megbízhatóságot speciális biztonsági mechanizmusokkal érik el, akkor ezeket a „Mélység” (ATE_DPT) követelményei részeként fogják tesztelni; ha a megbízhatóságot pusztán a szerkezeten keresztül valósítják meg, akkor a viselkedést a „Sebezhetőség felmérés” (AVA) követelmények részeként fogják tesztelni (áthatolás teszteléssel).

Ez a család a biztonsági szerkezet leírására vonatkozó követelményekből áll, amely ismerteti a önvédelem, a tartomány szétválasztás és a nem-megkerülhetőség elveit, beleértve annak leírását, hogy ezeket az elveket hogyan támogatják a TOE azon részei, amelyeket a TSF inicializálásához használnak.

6.1.5.2.1. ADV_ARC.1 Biztonsági szerkezet leírás

Függések: ADV_FSP.1, ADV_TDS.1

Fejlesztői akcióelemek:

ADV_ARC.1.1D A fejlesztőnek úgy kell megterveznie és megvalósítania a TOE-t, hogy a TSF biztonsági tulajdonságait ne lehessen megkerülni.

ADV_ARC.1.2D A fejlesztőnek úgy kell megterveznie és megvalósítania a TSF-t, hogy az képes legyen megvédeni magát a nem-megbízható aktív egyedek hamisításaitól.

ADV_ARC.1.3D A fejlesztőnek biztosítania kell egy leírást a TSF biztonsági szerkezetéről.

A bizonyíték elemek tartalma és bemutatása:

ADV_ARC.1.1C A biztonsági szerkezet leírást olyan szinten kell részletezni, amely összemérhető a TOE terv dokumentációban ismertetett, SFR-et érvényre juttató absztrakciók leírásával.

ADV_ARC.1.2C A biztonsági szerkezet leírásnak ismertetnie kell a TSF által kezelt biztonsági tartományokat, összhangban az SFR-ekkel.

ADV_ARC.1.3C A biztonsági szerkezet leírásnak ismertetnie kell, hogy a TSF inicializálási eljárása milyen mértékben biztonságos.

ADV_ARC.1.4C A biztonsági szerkezet leírásnak szemléltetnie kell, hogy a TSF megvédi magát a hamisítással szemben.

ADV_ARC.1.5C A biztonsági szerkezet leírásnak szemléltetnie kell, hogy a TSF meggátolja az SFR-et érvényre juttató funkcionalitás megkerülését.

Értékelői akcióelemek:

ADV_ARC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.5.3. Funkcionális specifikáció (ADV_FSP)

Ez a család a TSF interfészeket (TSFI) leíró funkcionális specifikációra határoz meg követelményeket. A TSFI azokból az eszközökből áll, amelyek a felhasználók számára lehetővé teszik, hogy szolgáltatást hívjanak meg a TSF-ből (a TSF által feldolgozandó adatok megadásával), valamint a szolgáltatás meghívásokra adott megfelelő válaszokból. Nem írja le azt, hogy a TSF hogyan dolgozza fel a szolgáltatás meghívásokat, és nem írja le azt a kommunikációt sem, amelynek során a TSF szolgáltatásokat hív meg üzemeltetési környezetéből; ezeket az információkat „TOE terv” (ADV_TDS) család tárgyalja.

Ez a család közvetlenül garanciát nyújt, lehetővé téve az értékelő számára annak átlátását, hogy a TSF hogyan felel meg a megkívánt SFR-eknek. Közvetetten is nyújt garanciát más garanciacsaládok és garanciaosztályok bemeneteként:

- ADV_ARC, ahol a TSFI-k leírása annak jobb megértésére használható, hogy a TSF-t hogyan védik meg a lerontás (vagyis a önvédelem vagy tartomány szétválasztás aláaknázása) és/vagy megkerülés ellen;
- ATE, ahol a TSFI-k leírása fontos bemenet a fejlesztői és az értékelői teszteléshez;
- AVA, ahol a TSFI-k leírását felhasználják a sebezhetőségek keresésénél.

A család összetevőinek a szintjei aszerint különböznek, hogy a TSFI-k leírása milyen részletességet és milyen fokú formalizmust kíván meg.

6.1.5.3.1. Alkalmazási megjegyzések

A TSFI-k meghatározását követően le kell írni azokat. Az alacsonyabb szintű összetevőknél a fejlesztők a dokumentációjukat (az értékelők pedig a vizsgálataikat) a TOE biztonsági szempontból legfontosabb vonatkozásaira összpontosítják. A TSFI-k három kategóriáját határozták meg, az ezeken keresztül elérhető szolgáltatások SFR-ekhez való viszonyán alapulva:

- Ha egy interfészen keresztül elérhető szolgáltatás visszavezethető egy TSF-től elvárt SFR-hez, akkor az adott interfészt ***SFR-t érvényre juttató***nak nevezik. Lehetséges, hogy egy interfészhez több szolgáltatás és eredmény tartozhat, melyek közül egyesek SFR-t érvényre juttatók, mások pedig nem.
- Azokat az interfészeket (vagy az interfészen keresztül elérhető szolgáltatásokat), amelyek olyan szolgáltatásokhoz csatlakoznak, amelyektől SFR-t érvényre juttató funkcionalitás függ, de amelyektől csak a helyes működést várják el a TOE biztonsági szabályzatok megőrzése érdekében, ***SFR-et támogató***knak nevezik.
- Az olyan szolgáltatásokhoz csatlakozó interfészeket, amelyektől SFR-t érvényre juttató funkcionalitás nem függ, ***SFR-be nem beavatkozó***nak nevezik.

Meg kell jegyezni, hogy ahhoz, hogy egy interfész SFR-t támogató vagy SFR-be nem beavatkozó legyen, feltétlenül szükséges, hogy ne rendelkezzen SFR-t érvényre juttató szolgáltatással vagy eredménnyel. Ezzel szemben egy SFR-t érvényre juttató interfész rendelkezhet SFR-t támogató szolgáltatásokkal (például a rendszeróra beállításának képessége lehet egy interfész SFR-t érvényre juttató szolgáltatása, de ha ugyanazt az interfészt arra használják, hogy a rendszerdátumot kijelezze, akkor a szóbanforgó szolgáltatás lehet csak SFR-t támogató).

Minél több információ áll rendelkezésre a TSFI-kről, annál nagyobb garancia nyerhető arra, hogy az interfészeket helyesen kategorizálták/vizsgálták. A követelményeket úgy strukturálták, hogy a legalacsonyabb szinten az SFR-be nem beavatkozó interfészekre megkövetelt információ a minimálisan szükséges információ ahhoz, hogy az értékelő ezt a megállapítást hatékonyan megtehesse. Magasabb szinteken több információ áll rendelkezésre, hogy az értékelőnek nagyobb legyen a bizalma a megállapításban.

A kategóriák (SFR-t érvényre juttató, SFR-t támogató, és SFR-be nem beavatkozó) meghatározásának és ezektől különböző követelmények elvárásának (az alacsonyabb garancia-összetevőknél) az a célja, hogy egy első közelítést nyújtson arra, hogy a vizsgálatokat mire kell összpontosítani, illetve melyek azok a bizonyítékok, amelyeken a vizsgálatokat el kell végezni. Ha a TSF interfészek fejlesztői dokumentációja az interfészek mindegyikét az SFR-t érvényre juttató interfészekre meghatározott követelményeknek megfelelően írja le (vagyis ha a dokumentáció meghaladja a követelményeket), akkor a fejlesztőnek nem kell új bizonyítékokat létrehoznia a követelmények kielégítésére. Hasonlóan, minthogy a kategóriák csupán eszközök az interfész típusok követelmények szerinti megkülönböztetésére, nem szükséges, hogy a fejlesztő frissítse a bizonyítékokat pusztán azért, hogy az interfészeket kategorizálja SFR-t érvényre juttató, SFR-t támogató és SFR-be nem beavatkozóként. Ennek a kategorizálásának az elsődleges célja annak lehetővé

tétele, hogy a fejlesztőknek csak a szükséges bizonyítékokat kelljen szolgáltatniuk, egy kevésbé részletesen kidolgozott fejlesztési módszertan (és pl. az ehhez kapcsolódó interfész- és terv dokumentáció) mellett, indokolatlan költségek nélkül.

A család összetevőinek utolsó C eleme közvetlen megfeleltetést biztosít az SFR-ek és a funkcionális specifikáció között; vagyis egy arra vonatkozó jelzést, hogy mely interfész szolgál az egyes megkívánt SFR-ek meghívására. Azokban az esetekben, amikor az ST tartalmaz olyan funkcionális követelményeket (mint például „Maradék információ védelem” (FDP_RIP)), amelynek funkcionalitása nem feltétlenül nyilvánul meg a TSFI-ken keresztül, a funkcionális specifikációnak és/vagy a nyomkövetésnek azonosítania kell ezeket az SFR-eket; ezeknek a funkcionális specifikációhoz való csatolása segít annak biztosításában, hogy nem vesztik el ezeket a lebontás alacsonyabb szintjein, ahol ezek fontosak lesznek.

Az interfész elvárt részletessége

A követelmények a TSFI-ről megadandó részleteket határozzák meg. A követelményekben az interfészeket az alábbi szempontok szerint határozzák meg (különböző részletesség mellett): rendeltetés, használati mód, paraméterek, paraméter leírások, tevékenységek és hibaüzenetek.

Egy interfész ***rendeltetés***e az interfész általános céljának magas szintű ismertetése (pl. GUI parancsok feldolgozása, hálózati csomagok fogadása, printer output létrehozása, stb.).

Az interfész ***használati mód***ja ismerteti az interfész használatára vonatkozó feltételezéseket. Ennek az ismertetése épüljön az adott interfészen elérhető különböző kölcsönhatások köré. Például, ha az interfész egy Unix parancs shell, akkor kölcsönhatás az interfészen például az Is, mv és cp. A használati mód minden egyes kölcsönhatásra ismertesse, hogy a kölcsönhatás mit végez el az interfészen látható működésmód tekintetében (pl. a programozó meghívja az API-t, a Windows felhasználók megváltoztatnak egy beállítást a nyilvántartásban, stb.), és az egyéb interfészeken kiváltott működésmód tekintetében is (pl. egy napló bejegyzés előállítása).

A ***paraméterek*** olyan közvetlen bemenetek és kimenetek egy interfész felé, illetve felől, amelyek vezérlik az adott interfész működésmódját. Paraméterek például azok az argumentumok, amelyeket egy API-nak adnak át; egy csomagnak a különböző mezői egy megadott hálózati protokoll esetén; a Windows Registry-ben lévő egyedi kulcs-értékek; egy chip érintkezői közötti jelek; azok a jelzőbitek, amelyeket egy Is számára be lehet állítani, stb. A paraméterek „meghatározása” a paraméterek egyszerű felsorolásával történik.

Egy ***paraméter leírás*** valamilyen érthető módon közli, hogy mi a paraméter. Például elfogadható paraméter leírás a foo(i) interfészre a következő: „az i paraméter egy egész szám, amely a rendszerbe jelenleg bejelentkezett felhasználók számát jelöli”. Egy olyan leírás, mint például: „az i paraméter egy egész szám”, nem elfogadható.

Egy interfészre a ***tevékenységek leírása*** ismerteti, hogy az interfész mit végez el. Ez annyiban részletesebb, mint a rendeltetés, hogy míg a „rendeltetés” azt mutatja ki, hogy miért akarja valaki ezt használni, a „tevékenységek” kimutatnak mindent, amit elvégez. Ezek a tevékenységek vagy kapcsolódnak az SFR-ekhez, vagy nem. Azokban az esetekben, amikor az interfész tevékenységek nincsenek kapcsolatban az SFR-ekkel, akkor a leírás legyen

kimondottan összegző, ami azt jelenti, hogy a leírás pusztán azt tegye világossá, hogy valóban nem kapcsolódik SFR-hez.

A ***hibaüzenet leírás*** meghatározza az üzenetet generáló feltételeket, magát az üzenetét, valamint az egyes hiba kódok jelentését. A TSF annak jelzésére generál hibaüzenetet, hogy hiba vagy bizonyos fokú rendellenesség merült fel. Az ehhez a családhoz tartozó követelmények különböző fajtájú hibaüzenetekre vonatkoznak:

- A „közvetlen” hibaüzenet egy meghatározott TSFI meghíváshoz köthető biztonság-vonzatú válasz.
- Egy „közvetett” hiba nem köthető egy meghatározott TSFI meghívásához, mivel rendszer-terjedelmű körülményekből keletkezik (pl. erőforrás kimerülés, kapcsolat megszakadások, stb.). A nem biztonság-vonzatú hibaüzeneteket szintén „közvetett”-nek tekintik.
- „Maradék” hiba minden egyéb hiba, mint például azok, amelyeket egy program kódon belül lehet előidézni. Például, egy feltétel-ellenőrzési kód használata, amely olyan feltételeket ellenőriz, amely logikusan nem léphet fel (pl. egy záró „else” előfordulása „case” utasítások sorozata után), kiválthat egy catch-all hibaüzenetet; egy működő TOE esetében ilyen hibaüzenetek sosem láthatók.

6.1.5.3.2. A családon belüli összetevők

A fejlesztőtől elvárt dokumentáció tükrözi az interfész specifikáció növekvő teljességén és pontosságán keresztül elérhető növekvő garanciát, ezt a család különböző hierarchikus összetevője részletezi.

Az ADV_FSP.1 „Alap funkcionális specifikáció” csak a TSFI egészének jellemzését, valamint az SFR-t érvényre juttató és az SFR-t támogató TSFI magas szintű leírását várja el. Az arra vonatkozó garancia érdekében, hogy a fejlesztő helyesen jellemezte a TSF „fontos” szempontjait, a fejlesztőnek az SFR-t érvényre juttató és az SFR-t támogató TSFI-re meg kell adnia azok rendeltetését, használati módját, paramétereit és paraméter leírásait.

Az ADV_FSP.2 „Biztonságot érvényre juttató funkcionális specifikáció” elvárja a fejlesztőtől, hogy az egész TSFI-re megadja az interfészek rendeltetését, használati módját, paramétereit és paraméter leírásait. Ezen kívül az SFR-t érvényre juttató TSFI-re a fejlesztőnek le kell írnia az SFR-t érvényre juttató tevékenységeket és a közvetlen hibaüzeneteket is.

Az ADV_FSP.3 „Funkcionális specifikáció teljes összegzéssel” esetén a fejlesztőnek az ADV_FSP.2 által elvártakon túl, elegendő információt kell biztosítania az SFR-t támogató és SFR-be nem beavatkozó tevékenységekről és hibaüzenetekről, annak kimutatása érdekében, hogy ezek nem SFR-t érvényre juttatóak. A fejlesztőnek dokumentálnia kell továbbá az SFR-t érvényre juttató TSFI meghívásából származó valamennyi közvetlen hibaüzenetet is.

Az ADV_FSP.4 „Teljes funkcionális specifikáció” esetén valamennyi TSFI-t (tehát az SFR-t érvényre juttató, az SFR-t támogató és az SFR-be nem beavatkozó interfészeket egyaránt) ugyanolyan szinten kell leírni, beleértve valamennyi közvetlen hibaüzenetet is.

Az ADV_FSP.5 „Teljes félformális funkcionális specifikáció kiegészítő hibaüzenetekkel” esetén a TSFI leírásoknak a közvetett hibaüzeneteket is tartalmazniuk kell.

Az ADV_FSP.6 „Teljes félformális funkcionális specifikáció kiegészítő formális specifikációval” esetén az ADV_FSP.5 által elvártakon túl a maradék hibaüzeneteket is tartalmazniuk kell. A fejlesztőnek a TSFI egy formális leírását is biztosítania kell. Ez a TSFI egy alternatív nézetét nyújtja, mely rámutathat a belső ellentmondásokra vagy a specifikáció teljességének hiányára.

A jelen dokumentumban meghatározott értékelési módszertan az FSP.2, FSP.3 és FSP4 összetevőket alkalmazza.

6.1.5.3.3. ADV_FSP.1 Alap funkcionális specifikáció

Függések: Nincsenek függések

Fejlesztői akcióelemek:

ADV_FSP.1.1D A fejlesztőnek biztosítania kell egy funkcionális specifikációt.

ADV_FSP.1.2D A fejlesztőnek biztosítania kell a funkcionális specifikáció visszavezetését az SFR-ekre.

A bizonyíték elemek tartalma és bemutatása:

ADV_FSP.1.1C A funkcionális specifikációnak le kell írnia minden TSFI rendeltetését és használati módját.

ADV_FSP.1.2C A funkcionális specifikációnak azonosítania kell minden TSFI-hez kapcsolódó összes paramétert.

ADV_FSP.1.3C A funkcionális specifikációnak meg kell magyaráznia a közvetve SFR-be nem beavatkozóként kategorizált interfészeket.

ADV_FSP.1.4C A visszavezetésnek szemléltetnie kell az SFR-ek visszavezetését a funkcionális specifikáció TSFI-eire.

Értékelői akcióelemek:

ADV_FSP.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ADV_FSP.1.2E Az értékelőnek meg kell erősítenie, hogy a funkcionális specifikáció az SFR-ek pontos és teljes megjelenítése.

6.1.5.3.4. ADV_FSP.2 Biztonságot érvényre juttató funkcionális specifikáció

Függések: ADV_TDS.1

Fejlesztői akcióelemek:

ADV_FSP.2.1D A fejlesztőnek biztosítania kell egy funkcionális specifikációt.

ADV_FSP.2.2D A fejlesztőnek biztosítania kell a funkcionális specifikáció visszavezetését az SFR-ekre.

A bizonyíték elemek tartalma és bemutatása:

ADV_FSP.2.1C **A funkcionális specifikációnak teljes mértékben be kell mutatnia a TSF-et.**

ADV_FSP.2.2C A funkcionális specifikációnak le kell írnia **minden** TSFI rendeltetését és használati módját.

ADV_FSP.2.3C A funkcionális specifikációnak azonosítania kell és **le kell írnia** minden TSFI-hez kapcsolódó összes paramétert.

ADV_FSP.2.4C **A funkcionális specifikációnak az SFR-t érvényre juttató TSFI-kre le kell írnia az egyes TSFI-khez kapcsolódó, SFR-t érvényre juttató tevékenységeket.**

ADV_FSP.2.5C **A funkcionális specifikációnak az SFR-t érvényre juttató TSFI-kre le kell írnia az SFR-t érvényre juttató tevékenységek feldolgozásából származó közvetlen hibaüzeneteket.**

ADV_FSP.2.6C A visszavezetésnek szemléltetnie kell az SFR-ek visszavezetését a funkcionális specifikáció TSFI-eire.

Értékelői akcióelemek:

ADV_FSP.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ADV_FSP.1.2E Az értékelőnek meg kell erősítenie, hogy a funkcionális specifikáció az SFR-ek pontos és teljes megjelenítése.

6.1.5.3.5. ADV_FSP.3 Funkcionális specifikáció teljes összegzéssel

Függések: ADV_TDS.1

Fejlesztői akcióelemek:

ADV_FSP.3.1D A fejlesztőnek biztosítania kell egy funkcionális specifikációt.

ADV_FSP.3.2D A fejlesztőnek biztosítania kell a funkcionális specifikáció visszavezetését az SFR-ekre.

A bizonyíték elemek tartalma és bemutatása:

ADV_FSP.3.1C A funkcionális specifikációnak teljes mértékben be kell mutatnia a TSF-et.

ADV_FSP.3.2C A funkcionális specifikációnak le kell írnia minden TSFI rendeltetését és használati módját.

ADV_FSP.3.3C A funkcionális specifikációnak azonosítania kell és le kell írnia minden TSFI-hez kapcsolódó összes paramétert.

ADV_FSP.3.4C A funkcionális specifikációnak az SFR-t érvényre juttató TSFI-kre le kell írnia az egyes TSFI-khez kapcsolódó, SFR-t érvényre juttató tevékenységeket.

ADV_FSP.3.5C A funkcionális specifikációnak az SFR-t érvényre juttató TSFI-kre le kell írnia a biztonságot érvényre juttató hatásokból származó közvetlen hibaüzeneteket, valamint a TSFI meghívásához kapcsolódó kivételeket.

ADV_FSP.3.6C A funkcionális specifikációnak minden TSFI-re összegeznie kell az SFR-t támogató és az SFR-be nem beavatkozó tevékenységeket.

ADV_FSP.3.7C A visszavezetésnek szemléltetnie kell az SFR-ek visszavezetését a funkcionális specifikáció TSFI-eire.

Értékelői akcióelemek:

ADV_FSP.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ADV_FSP.3.2E Az értékelőnek meg kell erősítenie, hogy a funkcionális specifikáció az SFR-ek pontos és teljes megjelenítése.

6.1.5.3.6. ADV_FSP.4 Teljes funkcionális specifikáció

Függések: ADV_TDS.1

Fejlesztői akcióelemek:

ADV_FSP.4.1D A fejlesztőnek biztosítania kell egy funkcionális specifikációt.

ADV_FSP.4.2D A fejlesztőnek biztosítania kell a funkcionális specifikáció visszavezetését az SFR-ekre.

A bizonyíték elemek tartalma és bemutatása:

ADV_FSP.4.1C A funkcionális specifikációnak teljes mértékben be kell mutatnia a TSF-et.

ADV_FSP.4.2C A funkcionális specifikációnak le kell írnia minden TSFI használatának célját és módját.

ADV_FSP.4.3C A funkcionális specifikációnak azonosítania kell és le kell írnia minden TSFI-hez kapcsolódó összes paramétert.

ADV_FSP.4.4C A funkcionális specifikációnak le kell írnia **minden egyes** TSFI-hez kapcsolódó **összes** tevékenységet.

ADV_FSP.4.5C **A funkcionális specifikációnak le kell írnia minden közvetlen hibaüzenetet, melyet bármelyik TSFI meghívása eredményezhet.**

ADV_FSP.4.6C A visszavezetésnek szemléltetnie kell az SFR-ek visszavezetését a funkcionális specifikáció TSFI-eire.

Értékelői akcióelemek:

ADV_FSP.4.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ADV_FSP.4.2E Az értékelőnek meg kell erősítenie, hogy a funkcionális specifikáció az SFR-ek pontos és teljes megjelenítése.

6.1.5.4. TOE terv (ADV_TDS)

A „TOE terv” a TSF leírására vonatkozó összefüggéseket és a TSF-nek egy részletes ismertetését adja meg. A garancia igények növekedésével a leírásban nyújtott részletezettség szintje is növekszik. A TSF méretének és bonyolultságának a növekedésével a lebontásnak egyre több szintje a megfelelő. A terv követelmények azt a célt szolgálják, hogy (az adott garanciaszinttel összemérhető) információt biztosítsanak annak meghatározásához, hogy a funkcionális biztonsági követelmények (SFR-ek) megvalósulnak-e.

A család összetevőinek szintjei aszerint különböznek, hogy mennyi információ szükséges a TSF bemutatására, és milyen fokú formalizmust kíván meg a terv leírása.

Alkalmazási megjegyzések

A terv dokumentáció célja, hogy megfelelő információt biztosítson a TSF határainak a meghatározásához, és hogy ismertesse, hogy a TSF hogyan valósítja meg a funkcionális biztonsági követelményeket (SFR-eket). A terv dokumentáció mennyisége és struktúrája a TOE bonyolultságától és az SRF-ek számától függ; általában egy nagyon bonyolult, nagyszámú SFR-rel rendelkező TOE több terv dokumentációt igényel, mint egy egyszerű TOE, amely csak néhány SFR-et valósít meg. A nagyon bonyolult TOE-k számára (a nyújtott garancia szempontjából) előnyös lesz, ha a terv leírásban különböző lebontási szinteket

készítenek, míg a nagyon egyszerű TOE-k megvalósításukra nem igénylik a magas és alacsony szintű leírások mindegyikét.

Ez a család a lebontás két szintjét alkalmazza: az alrendszerek és a modulok szintjét. A modul a funkcionalitás legspecifikusabb leírása: ez a megvalósítás leírása. A modul segítségével egy fejlesztő további tervezési döntés nélkül képes a TOE leírt részét megvalósítani. Az alrendszer a TOE terv leírása; ez elősegíti annak magas szintű leírását, hogy a TOE egyes részei mit és hogyan végeznek. Egy alrendszert tovább lehet bontani alacsonyabb szintű alrendszerekre vagy modulokra. A nagyon bonyolult TOE-k esetén szükség lehet alrendszerek több szintjére abból a célból, hogy megfelelő módon hordozzanak hasznos információt a TOE működéséről. Ezzel ellentétben a nagyon egyszerű TOE-k nem feltétlenül igényelnek egy alrendszer szintű leírást; lehetséges, hogy modul-szinten világosan leírható, hogy a TOE hogyan működik.

A terv dokumentációra általánosan elfogadott megközelítési mód, hogy a garanciaszint növekedésével a leírás hangsúlya áttolódik az általánosról (alrendszer-szint) a részletesebbre (modul-szint). Azokban az esetekben, amikor egy modul-szintű absztrakció megfelelő, mert a TOE elég egyszerű ahhoz, hogy modul-szinten legyen leírva, de a garanciaszint alrendszer-szintű leírást kíván meg, a modul-szintű leírás önmagában is elegendő lesz. A bonyolult TOE-k esetében azonban nem ez az eset: egy hatalmas mennyiségű (modul-szintű) részlet áttekinthetetlen lenne egy kísérő, alrendszer-szintű leírás nélkül.

Ez a megközelítési mód követi azt az általános alapelvet, hogy további részletek nyújtása a TSF megvalósításról nagyobb garanciát eredményez az SFR-ek helyes megvalósítására, valamint olyan információt biztosít, amely felhasználható ennek bizonyítására a tesztelések (ATE: Tesztek) során.

Az ezen családra vonatkozó követelményekben az interfész kifejezés (két alrendszer vagy modul közötti) jelentése: kommunikáció. Azt írja le, hogy a kommunikációt hogyan idézik elő; ez hasonló a TSFI részleteihez (lásd „Funkcionális specifikáció” (ADV_FSP)). A kölcsönhatás kifejezés a kommunikáció céljának meghatározására szolgál; meghatározza, hogy két alrendszer vagy modul miért kommunikál.

Az alrendszerek és a modulok elvárt részletessége

A követelmények az alrendszerekről és modulokról megadandó alábbi részleteket határozzák meg:

- Az alrendszerek és modulok *meghatározása* egyszerű felsorolásukkal történik.
- Az alrendszerek és modulok (közvetlenül vagy közvetett módon) *kategorizálható*k, mint "SFR-et érvényre juttató"-k, "SFR-et támogató"-k, vagy "SFR-be nem beavatkozó”-k; ezek a kifejezések ugyanolyan módon értendők, mint ahogyan a „Funkcionális specifikáció” (ADV_FSP) használja ezeket.
- Egy alrendszer *működésmód*ja azt jelenti, hogy mit végez el. A működésmód szintén kategorizálható, mint "SFR-t érvényre juttató"-k, "SFR-t támogató"-k, vagy "SFR-be nem beavatkozó”-k. Az alrendszer működésmódja sohasem kategorizálható magasabb SFR-fontosságúnak, mint maga az alrendszer. Például egy SFR-t érvényre juttató alrendszer rendelkezhet SFR-t érvényre juttató működésmóddal, és SFR-t támogató vagy SFR-be nem beavatkozó működésmóddal is.

- Egy alrendszer *működésmód összegzése* az általa végrehajtott tevékenységek áttekintése (pl. „A TCP alrendszer az IP datagrammokat megbízható byte folyamokká állítja össze”).
- Egy alrendszer *működésmód leírása* magyarázata mindannak, amit elvégez. Ez a leírás legyen olyan részletes, hogy könnyen meg lehessen állapítani, hogy a működésmódnak van-e valamilyen vonzata az SFR-ek érvényre juttatásában.
- Az alrendszerek közötti *kölcsönhatások leírása* meghatározza azt az okot, ami miatt az alrendszerek kommunikálnak, valamint jellemzi az átadott információt. Az információt nem szükséges ugyanolyan részletesen meghatározni, mint egy interfész specifikációt. Például elegendő lehet annyit mondani, hogy „az X alrendszer egy-blokknyi memóriát kér a memóriakezelőtől, amely az allokált memória elhelyezkedését adja meg válaszul”.
- Egy modul *rendeltetése* elegendő részletet biztosít ahhoz, hogy további tervezési döntésre ne legyen szükség. A modult megvalósító forráskód és a modul rendeltetése közötti megfeleltetés legyen azonnal nyilvánvaló.
- Egy modul *leírás*a azokat a szempontokat érinti, melyeket a követelmény elem meghatároz.

6.1.5.4.1. ADV_TDS.1 Alap terv

Függések: ADV_FSP.2

Fejlesztői akcióelemek:

ADV_TDS.1.1D A fejlesztőnek biztosítania kell a TOE tervét.

ADV_TDS.1.2D A fejlesztőnek egy leképezést kell biztosítania a funkcionális specifikáció TSFI-je és a TOE terv rendelkezésre álló legalacsonyabb szintű felbontása között.

A bizonyíték elemek tartalma és bemutatása:

ADV_TDS.1.1C A tervnek le kell írnia a TOE szerkezetét alrendszerek szerint.

ADV_TDS.1.2C A tervnek azonosítania kell a TSF minden alrendszerét.

ADV_TDS.1.3C A tervnek le kell írnia a TSF minden SFR-t támogató és SFR-be nem beavatkozó alrendszerének működésmódját, kellő részletességgel annak megállapításához, hogy az nem SFR-t érvényre juttató.

ADV_TDS.1.4C A tervnek összegeznie kell az SFR-t érvényre juttató alrendszerek SFR-t érvényre juttató működésmódját.

ADV_TDS.1.5C A tervnek leírást kell nyújtania a TSF-t érvényre juttató alrendszerek közötti, valamint a TSF-t érvényre juttató és egyéb alrendszerek közötti kölcsönhatásokról.

ADV_TDS.1.6C A leképezésnek szemléltetnie kell, hogy a TOE tervben ismertetett minden működésmódot megfeleltették az ezt aktivizáló TSFI-nek.

Értékelői akcióelemek:

ADV_TDS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ADV_TDS.1.2E Az értékelőnek meg kell erősítenie, hogy a terv az összes funkcionális biztonsági követelmény (SFR) pontos és teljes megjelenítése.

6.1.5.4.2. ADV_TDS.2 Szerkezeti terv

Függések: ADV_FSP.3

Fejlesztői akcióelemek:

ADV_TDS.2.1D A fejlesztőnek biztosítania kell a TOE tervét.

ADV_TDS.2.2D A fejlesztőnek egy leképezést kell biztosítania a funkcionális specifikáció TSFI-je és a TOE terv rendelkezésre álló legalacsonyabb szintű felbontása között.

A bizonyíték elemek tartalma és bemutatása:

ADV_TDS.2.1C A tervnek le kell írnia a TOE szerkezetét alrendszerek szerint.

ADV_TDS.2.2C A tervnek azonosítania kell a TSF minden alrendszerét.

ADV_TDS.2.3C **A tervnek le kell írnia a TSF minden SFR-be be nem avatkozó alrendszerének működésmódját, kellő részletességgel annak megállapításához, hogy az SFR-be be nem avatkozó.**

ADV_TDS.2.4C A tervnek **le kell írnia** az SFR-t érvényre juttató alrendszerek SFR-t érvényre juttató működésmódját.

ADV_TDS.2.5C A tervnek összegeznie kell az SFR-t érvényre juttató alrendszerek S**FR-be nem beavatkozó** működésmódját.

ADV_TDS.2.6C A tervnek összegeznie kell az **SFR-t támogató** alrendszerek működésmódját.

ADV_TDS.2.7C **A tervnek le kell írnia a TSF összes alrendszere közötti kölcsönhatásokat**.

ADV_TDS.2.8C A leképezésnek szemléltetnie kell, hogy a TOE tervben ismertetett minden működésmódot megfeleltették az ezt aktivizáló TSFI-nek.

Értékelői akcióelemek:

ADV_TDS.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ADV_TDS.2.2E Az értékelőnek meg kell erősítenie, hogy a terv az összes funkcionális biztonsági követelmény (SFR) pontos és teljes megjelenítése.

6.1.5.4.3. ADV_TDS.3 Alap moduláris terv

Függések: ADV_FSP.4

Fejlesztői akcióelemek:

ADV_TDS.3.1D A fejlesztőnek biztosítania kell a TOE tervét.

ADV_TDS.3.2D A fejlesztőnek egy leképezést kell biztosítania a funkcionális specifikáció TSFI-je és a TOE terv rendelkezésre álló legalacsonyabb szintű felbontása között.

A bizonyíték elemek tartalma és bemutatása:

ADV_TDS.3.1C A tervnek le kell írnia a TOE szerkezetét alrendszerek szerint.

ADV_TDS.3.2C **A tervnek le kell írnia a TSF-et modulok szerint**.

ADV_TDS.3.3C A tervnek azonosítania kell a TSF minden alrendszerét.

ADV_TDS.3.4C A tervnek leírást kell biztosítania a TSF minden alrendszeréről.

ADV_TDS.3.5C A tervnek le kell írnia a TSF összes alrendszere közötti kapcsolatokat.

ADV_TDS.3.6C **A tervnek egy leképezést kell biztosítania a TSF alrendszerei és a TSF moduljai között.**

ADV_TDS.3.7C **A tervnek le kell írnia az összes SFR-t érvényre juttató modult, megadva céljukat és a többi modullal való kapcsolatukat.**

ADV_TDS.3.8C **A tervnek le kell írnia az összes SFR-t érvényre juttató modult, megadva SFR vonatkozású interfészeiket, ezen interfészek visszatérési értékeit, valamint a többi modullal való kapcsolatukat és meghívott interfészeket.**

ADV_TDS.3.9C **A tervnek le kell írnia az összes SFR-t támogató, illetve az SFR-hez nem kapcsolódó modult, megadva céljukat és a többi modullal való kapcsolatukat.**

ADV_TDS.3.10C A leképezésnek szemléltetnie kell, hogy a TOE tervben leírt minden működést leképezi az ezeket meghívó TSFI-kre.

Értékelői akcióelemek:

ADV_TDS.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ADV_TDS.3.2E Az értékelőnek meg kell erősítenie, hogy a terv az összes funkcionális biztonsági követelmény (SFR) pontos és teljes megjelenítése.

6.1.5.5. Megvalósítási reprezentáció (ADV_IMP)

A „Megvalósítási reprezentáció” (ADV_IMP) családnak az a feladata, hogy a fejlesztő tegye hozzáférhetővé a TOE megvalósítási reprezentációját (és magasabb szinteken magát a megvalósítást) olyan formában, amelyet az értékelő vizsgálni tud. A megvalósítási reprezentációt a többi család vizsgálati tevékenységei során is felhasználják (például a TOE terv vizsgálatakor) annak bizonyítására, hogy a TOE megfelel a tervnek, illetve arra, hogy alapját képezze az értékelés egyéb területein végzett vizsgálatoknak (pl. sebezhetőségek keresése). Elvárás, hogy a megvalósítási reprezentáció olyan formájú legyen, amely átfogja a TSF részletes belső működését. A megvalósítási reprezentáció lehet szoftver forráskód, förmver forráskód, hardver diagram és/vagy hardver-tervezési nyelven írott kód vagy tervrajz adat.

A család összetevőinek szintjei aszerint különböznek, hogy a megvalósítás mekkora részét feleltetik meg a TOE tervnek.

Alkalmazási megjegyzések

A szoftver forráskód, förmver forráskód, hardver diagram és/vagy a tényleges hardver felépítéséhez használt, hardver-tervezési nyelven írott kód vagy tervrajz adat, példák megvalósítási reprezentáció részekre. Fontos megjegyezni, hogy míg a megvalósítási reprezentációt feltétlenül rendelkezésre kell bocsátani az értékelő számára, ez nem vonja maga után, hogy az értékelőnek birtokolnia is kell a szóbanforgó reprezentációt. A fejlesztő megkövetelheti például, hogy az értékelő olyan helyszínen vizsgálja át a megvalósítási reprezentációt, amelyet a fejlesztő választ meg.

A teljes megvalósítási reprezentáció álljon rendelkezésre nehogy információ hiányban szenvedjen a vizsgálati tevékenység. Ebből azonban nem következik, hogy a teljes reprezentációt át kell vizsgálni a vizsgálati tevékenység során. Ez valószínűleg majdnem minden esetben kivihetetlen, azon felül, hogy minden valószínűség szerint nem eredményezne nagyobb garanciájú TOE-t, a megvalósítási reprezentáció célirányos mintavételezésével szemben. A megvalósítási reprezentáció rendelkezésre állása azt a célt szolgálja, hogy lehetővé váljon a többi TOE terv lebontás (pl. funkcionális specifikáció, TOE terv) vizsgálata, és hogy bizonyosságot lehessen szerezni arról, hogy tervezés magasabb szintjén leírt biztonsági funkcionalitás ténylegesen megvalósítottnak bizonyul a TOE-ban.

A megvalósítási reprezentáció bizonyos formáiban alkalmazott konvenciók nehézzé vagy lehetetlenné tehetik, hogy csak magából a megvalósítási reprezentációból meg lehessen határozni, hogy mi lesz a tényleges eredménye a fordításnak vagy futás-idejű parancsértelmezésnek. Például a C nyelvű fordítóprogramoknak szóló szerkesztési utasítások azt eredményezik, hogy a fordítóprogram teljes kód-részeket kihagy vagy hozzácsatol. Emiatt

fontos, hogy az ilyen „extra” információkat vagy a kapcsolódó eszközöket (scriptek, fordítóprogramok stb.) is megadják, hogy a megvalósítási reprezentációt pontosan lehessen meghatározni.

A megvalósítási reprezentáció és a TOE terv közötti megfeleltetés célja, hogy elősegítse az értékelői vizsgálatot. A TOE belső működését jobban meg lehet érteni, ha a TOE tervet a megvalósítási reprezentáció megfelelő részeivel együtt vizsgálják. A megfeleltetés tárgymutatóként szolgál a megvalósítási reprezentációhoz.

A megvalósítási reprezentációt a fejlesztőnek olyan formára kell alakítania, amely alkalmas arra, hogy a tényleges megvalósításra átalakítsák. Például a fejlesztő dolgozhat forráskódokat tartalmazó fájlokkal, amelyeket végül lefordítanak, hogy a TSF részeivé váljanak. A fejlesztőnek a megvalósítási reprezentációt olyan formában kell rendelkezésre bocsátania, ahogyan azt a fejlesztő használja, hogy az értékelő automatizált technikákat használhasson a vizsgálatoknál. Ez szintén növeli a bizonyosságát annak, hogy a vizsgált megvalósítási reprezentáció tényleg az, mint amit a TSF előállítására használnak (szemben azzal az esettel, amikor a reprezentáció egy változó bemutatási formátumban van megadva, például egy szövegszerkesztővel előállított dokumentumban). Meg kell jegyezni, hogy a megvalósítási reprezentációnak más formáit is használhatja a fejlesztő; ezeket a formákat ugyancsak rendelkezésre kell bocsátani. Az általános cél az, hogy az értékelő számára biztosítani kell azokat az információkat, amelyek fokozzák az értékelői vizsgálatok hatékonyságát.

A megvalósítási reprezentáció bizonyos formái kiegészítő információkat igényelhetnek, mert jelentősen megnehezítik a megértést és a vizsgálatokat. A példák magukban foglalják a „leplezett” forráskódot vagy az olyan forráskódot, amelyet más módon homályosítottak el úgy, hogy ez gátolja a megértést és/vagy a vizsgálatokat. A megvalósítási reprezentációnak ezek a formái általában úgy keletkeznek, hogy a TOE fejlesztője a megvalósítási reprezentáció egy verziójára ráereszt egy leplező vagy elhomályosító programot. Bár a leplezett reprezentáció az, amit lefordítottak, és lehet, hogy ez közelebb áll a megvalósításhoz (a szerkezet szempontjából), mint az eredeti, nem-leplezett reprezentáció, egy ilyen homályossá tett kódnak a rendelkezésre bocsátása azt okozhatja, hogy jelentősen több időt kell fordítani a reprezentációt érintő vizsgálati feladatokra. Amikor ilyen formájú reprezentációt alakítanak ki, az összetevők megkövetelik a használt leplező eszközökre/algoritmusokra vonatkozó részleteket, hogy rendelkezésre lehessen bocsátani a nem-leplezett reprezentációt, és a kiegészítő információk használhatók arra, hogy bizonyosságot szerezzenek arról, hogy a leplező eljárás nem ront le egyetlen biztonsági funkcionalitást sem.

6.1.5.5.1. ADV_IMP.1 A TSP megvalósítási reprezentációja

Függések: ADV_TDS.3, ALC_TAT.1

Fejlesztői akcióelemek:

ADV_IMP.1.1D A fejlesztőnek az egész TSF-re elérhetővé kell tennie a megvalósítási reprezentációt.

ADV_IMP.1.2D A fejlesztőnek egy leképezést kell biztosítania a TOE terv és a megvalósítási reprezentáció egy mintája között.

A bizonyíték elemek tartalma és bemutatása:

ADV_IMP.1.1C A megvalósítási reprezentációnak olyan részletességgel kell meghatároznia a TSF-et, hogy ebből a TSF már minden további tervezési döntés nélkül előállítható legyen.

ADV_IMP.1.2C A megvalósítási reprezentációnak a fejlesztő személyzet által használt formában kell lennie.

ADV_IMP.1.3C A TOE terv és a megvalósítási reprezentáció mintája közötti leképezésnek szemléltetnie kell a megfelelést.

Értékelői akcióelemek:

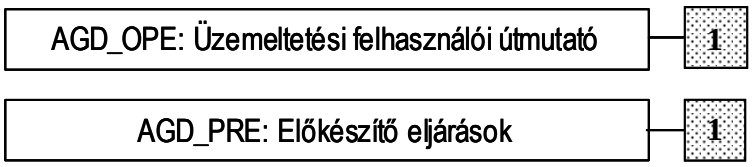
ADV_IMP.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.6. Útmutató dokumentumok garanciaosztály (AGD)

6.1.6.1. Az Útmutató dokumentumok garanciaosztály áttekintése

Az AGD garanciaosztály a fejlesztő által a felhasználó számára készítendő, előkészítő feladatokkal és üzemeltetéssel kapcsolatos dokumentációk érthetőségével, lefedettségével és teljességével foglalkozik. A felhasználón a TOE-val kapcsolatos, SFR-nek megfelelő műveleteket jogosultan végrehajtó személyt értjük. A minden felhasználói szerepkör számára szóló dokumentáció a TOE biztonságos előkészítésének és üzemeltetésének fontos eleme.
Az AGD garanciaosztályt két családra osztották. Ezek közül az első az előkészítési eljárásokkal foglakozik (mit kell tenni, hogy a leszállított TOE-t üzemeltetési környezetében, az ST-ben meghatározott értékelt konfigurációra alakítsák), a másik pedig az üzemeltetési felhasználói útmutató (mit kell tenni, hogy a TOE-t az értékelt konfigurációjában működtessék).

Az 5. ábra az AGD CC garanciaosztályon belüli családokat, s a családokon belül az összetevők hierarchiáját mutatja. A jelen dokumentum által meghatározott értékelési módszertannak az ábrán megjelölt garancia-összetevők képezik részét.



5. ábra - Az útmutató dokumentumok garanciaosztály felépítése

6.1.6.2. Előkészítő eljárások (AGD_PRE)

Az AGD_PRE garanciacsalád keretében dokumentálni kell a TOE biztonságos előkészületi eljárásait és lépéseit, s ezeknek biztonságos konfigurációt kell eredményezniük.
Az előkészítés folyamata megköveteli, hogy a TOE leszállított példányát a felhasználó átvegye, konfigurálja és aktiválja annak bizonyítása céljából, hogy a TOE üzemeltetése során aktívak lesznek a szükséges védelmi tulajdonságok. Az előkészítő eljárások biztosítják azt a garanciát, hogy a felhasználó tisztában lesz a TOE konfigurációs paramétereivel és hogy ezek hogyan befolyásolják a TSF-et.

6.1.6.2.1. AGD_PRE.1: Előkészítő eljárások

Függések: Nincsenek függések

Fejlesztői akcióelemek:

AGD_PRE.1.1D A fejlesztőnek biztosítania kell a TOE-t, s benne az előkészítő eljárásokat.

A bizonyíték elemek tartalma és bemutatása:

AGD_PRE.1.1C Az előkészítő eljárásoknak le kell írniuk a leszállított TOE biztonságos elfogadásához szükséges valamennyi lépést, a fejlesztő szállítási eljárásaival összhangban.

AGD_PRE.1.2C Az előkészítő eljárásoknak le kell írniuk a TOE biztonságos telepítéséhez, valamint az üzemeltetési környezethez való biztonságos előkészülethez szükséges valamennyi lépést, az ST-ben leírt, üzemeltetési környezetre vonatkozó biztonsági célokkal összhangban.

Értékelői akcióelemek:

AGD_PRE.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

AGD_PRE.1.2E Az értékelőnek végre kell hajtania az előkészítő eljárásokat annak megerősítése érdekében, hogy a TOE biztonságosan előkészíthető a működésre.

6.1.6.3. Üzemeltetési felhasználói útmutató (AGD_OPE)

Az AGD_OPE garanciacsalád keretében elkészítendő üzemeltetési felhasználói útmutató minden felhasználói szerepkörre leírja a TSF által nyújtott biztonsági funkcionalitást és interfészeket, tartalmazza a TOE biztonságos használatához szükséges utasításokat és útmutatást, lefedi az összes üzemeltetési mód biztonságos eljárásait, valamint lehetővé teszi a TOE nem biztonságos állapotainak megelőzését és észlelését.

A lehetséges felhasználói szerepkörök az értékelések nagy részénél a „végfelhasználó” és az „adminisztrátor” szerepköröket jelenti, de ezek szükség esetén tovább finomíthatók.

6.1.6.3.1. AGD_OPE.1: Üzemeltetési felhasználói útmutató

Függések: ADV_FSP.1

Fejlesztői akcióelemek:

AGD_OPE.1.1D A fejlesztőnek üzemeltetési felhasználói útmutatót kell biztosítania.

A bizonyíték elemek tartalma és bemutatása:

AGD_OPE.1.1C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre le kell írnia azokat a felhasználó által elérhető funkciókat és jogosultságokat (beleértve a megfelelő figyelmeztetéseket is), melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

AGD_OPE.1.2C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre le kell írnia, hogy a TOE által biztosított, elérhető interfészeket hogyan kell biztonságos módon használni.

AGD_OPE.1.3C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre le kell írnia az elérhető funkciókat és interfészeket, különösen a felhasználó ellenőrzése alá tartozó minden biztonsági szempontból fontos paramétert, jelezve (ahol ez lehetséges) a biztonságos értékeket.

AGD_OPE.1.4C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre világosan be kell mutatnia a felhasználó által elérhető funkciókkal kapcsolatban végrehajtandó, biztonsági szempontból fontos minden esemény típust, beleértve a TSF ellenőrzése alá eső egyedek biztonsági tulajdonságainak megváltoztatását is.

AGD_OPE.1.5C Az üzemeltetési felhasználói útmutatónak azonosítani kell a TOE összes lehetséges üzemeltetési módját (beleértve a meghibásodás vagy üzemeltetési hiba utáni műveleteket is), valamint ezek biztonságos üzemeltetésre gyakorolt következményeit és kihatásait.

AGD_OPE.1.6C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre le kell írnia azokat a betartandó biztonsági intézkedéseket, melyek az ST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célok elérését szolgálják.

AGD_OPE.1.7C Az üzemeltetési felhasználói útmutatónak egyértelműnek és megalapozottnak kell lennie.

Értékelői akcióelemek:

AGD_OPE.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.7. Életciklus támogatás garanciaosztály (ALC)

6.1.7.1. Az Életciklus támogatás garanciaosztály áttekintése

Az ALC garanciaosztály követelményeket fogalmaz meg arra a garanciára, melyet egy jól meghatározott életciklus modell alkalmazásán keresztül a TOE fejlesztés (ideértve a hibajavítást is) minden lépésében, az eszközök és technikák, valamint a fejlesztői környezet védelméhez használt biztonsági intézkedésekben követni kell.

A 6. ábra az ALC CC garanciaosztályon belüli családokat, s a családokon belül az összetevők hierarchiáját mutatja. A jelen dokumentum által meghatározott értékelési módszertannak csak az ábrán külön megjelölt garancia-összetevők képezik részét.

6. ábra - Az életciklus támogatás garanciaosztály felépítése

A konfiguráció kezeléshez kapcsolódó tevékenységnek az a célja, hogy segítséget nyújtson a fogyasztónak az értékelt TOE beazonosításában, hogy biztosítsa a konfiguráció elemek egyedi azonosítását, és biztosítsa a fejlesztő által a TOE-n történt változtatások ellenőrzéséhez és nyomonkövetéséhez használt eljárások megfelelőségét.

A szállításhoz kapcsolódó tevékenység célja azoknak az eljárásoknak a dokumentálása, amelyek biztosítják, hogy a TOE-t változtatás nélkül szállítják ki a fogyasztóhoz.

A fejlesztő biztonsági eljárásainak az a célja, hogy megvédjék a TOE-t és a kapcsolódó tervezési információkat a hamisításokkal vagy illetéktelen felfedésekkel szemben. A fejlesztési folyamatba történő hamisítás lehetővé teheti sebezhetőségek szándékos bevitelét is. A tervezési információk felfedése lehetővé teheti a sebezhetőségek könnyebb kiaknázhatóságát.

A TOE elégtelenül ellenőrzött fejlesztése és kezelése sebezhetőségekhez vezethet a megvalósításban. Egy meghatározott életciklus modellnek való megfelelőség elősegítheti az intézkedések javítását ezen a területen.

Ha a fejlesztő és a fejlesztési folyamatba bevont harmadik felek jól meghatározott fejlesztő eszközöket használnak és megvalósítási szabványokat alkalmaznak, akkor ez segít annak biztosításában, hogy sebezhetőségeket ne vigyenek be figyelmetlenségből a pontosítás során.

A hibajavításhoz kapcsolódó tevékenység célja, hogy nyomonkövessék a biztonsági réseket, meghatározzák a javító műveleteket, és hogy eljuttassák a javító műveletekre vonatkozó információkat a TOE felhasználóknak. (A hibajavítási tevékenységek garanciacsalád nem képezi kötelező részét egyetlen garanciaszintnek sem. A TOE garancia folyamatosságának biztosításához azonban kötelező követelmény. A hibajavításra vonatkozó követelményeket és ezek értékelési követelményeit [8] részletezi.)

6.1.7.2. A konfiguráció kezelés képességei (ALC_CMC)

6.1.7.2.1. ALC_CMC.1: A TOE megcímkézése

Függések: ALC_CMS.1

Fejlesztői akcióelemek:

ALC_CMC.1.1D A fejlesztőnek meg kell adnia a TOE-t és a TOE egy hivatkozását.

A bizonyíték elemek tartalma és bemutatása:

ALC_CMC.1.1C A TOE-t meg kell jelölni egyedi hivatkozásával.

Értékelői akcióelemek:

ALC_CMC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.7.2.2. ALC_CMC.2: CM rendszer használata

Függések: ALC_CMS.2

Fejlesztői akcióelemek:

ALC_CMC.2.1D A fejlesztőnek meg kell adnia a TOE-t és a TOE egy hivatkozását.

ALC_CMC.2.2D **A fejlesztőnek biztosítania kell a konfiguráció kezelés dokumentációt.**

ALC_CMC.2.3D **A fejlesztőnek egy konfiguráció kezelés rendszert kell használnia.**

A bizonyíték elemek tartalma és bemutatása:

ALC_CMC.2.1C A TOE-t meg kell jelölni egyedi hivatkozásával.

ALC_CMC.2.2C **A konfiguráció kezelés dokumentációnak le kell írnia a konfiguráció elemek egyértelmű azonosítására alkalmazott módszert.**

ALC_CMC.2.3C **A konfiguráció kezelés rendszernek egyértelműen azonosítania kell minden konfiguráció elemet.**

Értékelői akcióelemek:

ALC_CMC.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.7.2.3. ALC_CMC.3: Engedélyezéssel kapcsolatos intézkedések

Függések: ALC_CMS.2, ALC_DVS.1

Fejlesztői akcióelemek:

ALC_CMC.3.1D A fejlesztőnek meg kell adnia a TOE-t és a TOE egy hivatkozását.

ALC_CMC.3.2D A fejlesztőnek biztosítania kell a konfiguráció kezelés dokumentációt.

ALC_CMC.3.3D A fejlesztőnek egy konfiguráció kezelés rendszert kell használnia.

A bizonyíték elemek tartalma és bemutatása:

ALC_CMC.3.1C A TOE-t meg kell jelölni egyedi hivatkozásával.

ALC_CMC.3.2C A konfiguráció kezelés dokumentációnak le kell írnia a konfiguráció elemek egyértelmű azonosítására alkalmazott módszert.

ALC_CMC.3.3C A konfiguráció kezelés rendszernek egyértelműen azonosítania kell minden konfiguráció elemet.

ALC_CMC.3.4C **A konfiguráció kezelés rendszernek olyan eszközöket kell biztosítania, mely csak jogosult változtatásokat enged végrehajtani a konfiguráció elemekben.**

ALC_CMC.3.5C **A konfiguráció kezelés dokumentációnak tartalmaznia kell egy konfiguráció kezelés tervet.**

ALC_CMC.3.6C **A konfiguráció kezelés tervnek le kell írnia a konfiguráció kezelés rendszer TOE fejlesztéséhez történő használatát.**

ALC_CMC.3.7C **Bizonyítéknak kell kimutatnia, hogy konfiguráció kezelés rendszer minden konfiguráció elemet kezel.**

ALC_CMC.3.8C **Bizonyítéknak kell kimutatnia, hogy a konfiguráció kezelés rendszer a konfiguráció kezelés tervnek megfelelően működik.**

Értékelői akcióelemek:

ALC_CMC.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.7.2.4. ALC_CMC.4: A TOE előállítás támogatása, átvételi eljárások és automatizálás

Függések: ALC_CMS.2, ALC_DVS.1, ALC_LCD.1

Fejlesztői akcióelemek:

ALC_CMC.4.1D A fejlesztőnek meg kell adnia a TOE-t és a TOE egy hivatkozását.

ALC_CMC.4.2D A fejlesztőnek biztosítania kell a konfiguráció kezelés dokumentációt.

ALC_CMC.4.3D A fejlesztőnek egy konfiguráció kezelés rendszert kell használnia.

A bizonyíték elemek tartalma és bemutatása:

ALC_CMC.4.1C A TOE-t meg kell jelölni egyedi hivatkozásával.

ALC_CMC.4.2C A konfiguráció kezelés dokumentációnak le kell írnia a konfiguráció elemek egyértelmű azonosítására alkalmazott módszert.

ALC_CMC.4.3C A konfiguráció kezelés rendszernek egyértelműen azonosítania kell minden konfiguráció elemet.

ALC_CMC.4.4C A konfiguráció kezelés rendszernek olyan automatizált eszközöket kell biztosítania, mely csak jogosult változtatásokat enged végrehajtani a konfiguráció elemekben.

ALC_CMC.4.5C **A konfiguráció kezelés rendszernek automatizált eszközökkel támogatnia kell a TOE előállítását.**

ALC_CMC.4.6C A konfiguráció kezelés dokumentációnak tartalmaznia kell egy konfiguráció kezelés tervet.

ALC_CMC.4.7C A konfiguráció kezelés tervnek le kell írnia a konfiguráció kezelés rendszer TOE fejlesztéséhez történő használatát.

ALC_CMC.4.8C **A konfiguráció kezelés tervnek le kell írnia azokat az eljárásokat, melyeket a módosított vagy újonnan létrehozott konfiguráció elemeknek a TOE részeként történő elfogadására használnak.**

ALC_CMC.4.9C Bizonyítéknak kell kimutatnia, hogy konfiguráció kezelés rendszer minden konfiguráció elemet kezel.

ALC_CMC.4.10C Bizonyítéknak kell kimutatnia, hogy a konfiguráció kezelés rendszer a konfiguráció kezelés tervnek megfelelően működik.

Értékelői akcióelemek:

ALC_CMC.4.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.7.3. A konfiguráció kezelés hatásköre (ALC_CMS)

6.1.7.3.1. ALC_CMS.1: A TOE CM lefedettsége

Függések: Nincsenek függések

Fejlesztői akcióelemek:

ALC_CMS.1.1D A fejlesztőnek meg kell adnia egy TOE-ra vonatkozó konfiguráció listát.

A bizonyíték elemek tartalma és bemutatása:

ALC_CMS.1.1C A konfiguráció listának tartalmaznia kell a következőket: maga a TOE; és a garanciális biztonsági követelmények (SAR) által megkövetelt értékelési bizonyítékok.

ALC_CMS.1.2C A konfiguráció listának egyértelműen azonosítania kell a konfiguráció elemeket.

Értékelői akcióelemek:

ALC_CMS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.7.3.2. ALC_CMS.2: A TOE részeinek CM lefedettsége

Függések: Nincsenek függések

Fejlesztői akcióelemek:

ALC_CMS.2.1D A fejlesztőnek meg kell adnia egy TOE-ra vonatkozó konfiguráció listát.

A bizonyíték elemek tartalma és bemutatása:

ALC_CMS.2.1C A konfiguráció listának tartalmaznia kell a következőket: maga a TOE; a garanciális biztonsági követelmények (SAR) által megkövetelt értékelési bizonyítékok **és a TOE-t alkotó részek.**

ALC_CMS.2.2C A konfiguráció listának egyértelműen azonosítania kell a konfiguráció elemeket.

ALC_CMS.2.3C **A konfiguráció listának a TSF szempontból fontos minden konfiguráció elemre meg kell adni az elem fejlesztőjét.**

Értékelői akcióelemek:

ALC_CMS.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.7.3.3. ALC_CMS.3: A megvalósítási reprezentáció CM lefedettsége

Függések: Nincsenek függések

Fejlesztői akcióelemek:

ALC_CMS.3.1D A fejlesztőnek meg kell adnia egy TOE-ra vonatkozó konfiguráció listát.
A bizonyíték elemek tartalma és bemutatása:

ALC_CMS.3.1C A konfiguráció listának tartalmaznia kell a következőket: maga a TOE; a garanciális biztonsági követelmények (SAR) által megkövetelt értékelési bizonyítékok, a TOE-t alkotó részek **és a megvalósítási reprezentáció**.

ALC_CMS.3.2C A konfiguráció listának egyértelműen azonosítania kell a konfiguráció elemeket.

ALC_CMS.3.3C A konfiguráció listának a TSF szempontból fontos minden konfiguráció elemre meg kell adni az elem fejlesztőjét.

Értékelői akcióelemek:

ALC_CMS.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.7.3.4. ALC_CMS.4: A probléma követés CM lefedettsége

Függések: Nincsenek függések

Fejlesztői akcióelemek:

ALC_CMS.4.1D A fejlesztőnek meg kell adnia egy TOE-ra vonatkozó konfiguráció listát.

A bizonyíték elemek tartalma és bemutatása:

ALC_CMS.4.1C A konfiguráció listának tartalmaznia kell a következőket: maga a TOE; a garanciális biztonsági követelmények (SAR) által megkövetelt értékelési bizonyítékok, a TOE-t alkotó részek; a megvalósítási reprezentáció; **biztonsági hiba jelentések és megoldási állapotuk**.

ALC_CMS.4.2C A konfiguráció listának egyértelműen azonosítania kell a konfiguráció elemeket.

ALC_CMS.4.3C A konfiguráció listának a TSF szempontból fontos minden konfiguráció elemre meg kell adni az elem fejlesztőjét.
Értékelői akcióelemek:

ALC_CMS.4.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.7.4. Szállítás (ALC_DEL)

A szállítás az életciklus azon szakasza, amikor a kész TOE az előállítási környezetből a felhasználó hatáskörébe kerül. Beletartozhat a csomagolás és tárolás a fejlesztői telephelyen, de nem terjed ki a befejezetlen TOE vagy részeinek különböző fejlesztői színhelyek közötti továbbítására. Ennek a garanciacsaládnak a fókuszában a befejezett TOE-nak a felhasználóhoz való biztonságos továbbítása áll.

6.1.7.4.1. ALC_DEL.1: Szállítási eljárások

Függések: Nincsenek függések

Fejlesztői akcióelemek:

ALC _DEL.1.1D A fejlesztőnek dokumentálnia kell a TOE vagy annak részei felhasználóhoz való szállításának eljárásait.

ALC _DEL.1.2D A fejlesztőnek használnia kell a szállítási eljárásokat.

A bizonyíték elemek tartalma és bemutatása:

ALC _DEL.1.1C A szállítási dokumentációnak le kell írnia minden olyan eljárást, amely a TOE verzióinak felhasználókhoz történő szállítása során a biztonság fenntartásához szükséges.

Értékelői akcióelemek:

ALC_DEL.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.7.5. A fejlesztés biztonsága (ALC_DVS)

Az ALC_DVS garanciacsalád a fejlesztői környezetben használt fizikai, eljárásrendi, személyi és egyéb biztonsági intézkedéseket fedi le. Tartalmazza a fejlesztői helyszín(ek) fizikai biztonságát, és felügyeli a fejlesztői állomány kiválasztását és szerződtetését.

6.1.7.5.1. ALC_DVS.1: A biztonsági intézkedések azonosítása

Függések: Nincsenek függések

Fejlesztői akcióelemek:

ALC_DVS.1.1D A fejlesztőnek fejlesztés biztonsági dokumentációt kell biztosítania.

A bizonyíték elemek tartalma és bemutatása:

ALC_DVS.1.1C A fejlesztés biztonsági dokumentációnak le kell írnia minden olyan fizikai, eljárásbeli, személyi és egyéb biztonsági intézkedést, mely a TOE tervek és TOE megvalósítás bizalmasságának és sértetlenségének a védelméhez szükséges, fejlesztési környezetében.

Értékelői akcióelemek:

ALC_DVS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ALC_DVS.1.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági intézkedéseket betartják.

6.1.7.6. Életciklus meghatározás (ALC_LCD)

Az életciklus definíció annak alapját teremti meg, hogy a fejlesztő által a TOE előállításához használt fejlesztés, gyártás gyakorlata terjedjen ki a fejlesztési folyamatban és az üzemeltetési támogatás követelményeiben azonosított szempontokra és tevékenységekre.

A fejlesztői környezet értékeléséhez az értékelőnek meg kell ismernie a fejlesztő által használt életciklus modellt. Ezért a fejlesztőnek meg kell adnia az értékelő számára az alkalmazott életciklus modellt.

6.1.7.6.1. ALC_LCD.1: A fejlesztő által meghatározott életciklus modell

Függések: Nincsenek függések

Fejlesztői akcióelemek:

ALC_LCD.1.1D A fejlesztőnek egy életciklus modellt kell felállítania a TOE fejlesztésére és karbantartására vonatkozóan.

ALC_LCD.1.2D A fejlesztőnek dokumentálnia kell az életciklus modellt.

A bizonyíték elemek tartalma és bemutatása:

ALC_LCD.1.1C Az életciklus modell dokumentációnak le kell írnia a TOE fejlesztéséhez és karbantartásához használt modellt.

ALC_LCD.1.2C Az életciklus modellnek biztosítania kell a TOE fejlesztéséhez és karbantartásához szükséges ellenőrzést.

Értékelői akcióelemek:

ALC_LCD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.7.7. Eszközök és technikák (ALC_TAT)

Az ALC_TAT garanciacsalád a TOE fejlesztéséhez, vizsgálatához és megvalósításához használt eszközök kiválasztásának szempontjaival foglalkozik. Jól meghatározott, ellentmondás-mentes és helyesen működő eszközök használatát követeli meg a TOE fejlesztéséhez.

6.1.7.7.1. ALC_TAT.1: Jól meghatározott fejlesztő eszközök

Függések: ADV_IMP.1

Fejlesztői akcióelemek:

ALC_TAT.1.1D A fejlesztőnek azonosítania kell a TOE-hez használt minden fejlesztő eszközt.

ALC_TAT.1.2D A fejlesztőnek minden fejlesztő eszközre dokumentálnia kell a kiválasztott megvalósítás-függő opciókat.

A bizonyíték elemek tartalma és bemutatása:

ALC_TAT.1.1C A megvalósításhoz használt minden fejlesztő eszköznek jól meghatározottnak kell lennie.

ALC_TAT.1.2C Minden fejlesztő eszköz dokumentációnak egyértelműen meg kell határoznia a megvalósítás során használt valamennyi utasítás, konvenció és direktíva jelentését.

ALC_TAT.1.3C Minden fejlesztő eszköz dokumentációnak egyértelműen meg kell határoznia valamennyi megvalósítás-függő opció jelentését.

Értékelői akcióelemek:

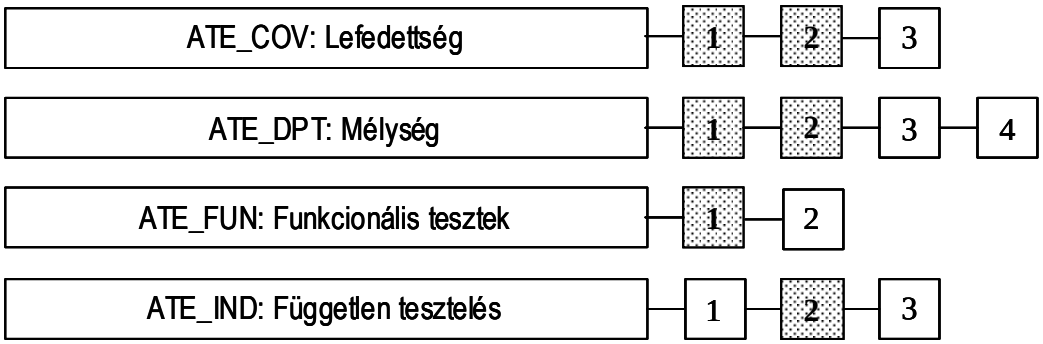
ALC_TAT.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.8. Tesztelés garanciaosztály (ATE)

6.1.8.1. A Tesztelés garanciaosztály áttekintése

Az ATE garanciaosztály által előírt tevékenységek célja annak meghatározása, hogy a TOE az ST-ben leírtaknak megfelelően, egyúttal az ADV osztály értékelési bizonyítékaiban specifikáltak szerint működik-e. E döntés meghozatalát a fejlesztő által elvégzett TSF funkcionális tesztelés és az értékelő által elvégzett független TSF tesztelés segíti.

A 7. ábra az ATE CC garanciaosztályon belüli családokat, s a családokon belül az összetevők hierarchiáját mutatja. A jelen dokumentum által meghatározott értékelési módszertannak csak az ábrán külön megjelölt garancia-összetevők képezik részét.



7. ábra - A tesztelés garanciaosztály felépítése

A funkcionális tesztelés (ATE_FUN) célja az, hogy a fejlesztő dokumentálja azokat a tesztjeit, melyeket a TOE megfelelő (terv dokumentációkban meghatározott) működésének kimutatására hajtott végre.

Az ATE_COV család a fejlesztő által végrehajtott, a TOE funkcionális specifikációjának megfelelő biztonsági tesztelést dokumentálja.

Az ATE_DPT garanciacsalád összetevői az mondják meg, hogy a fejlesztő milyen részletességgel (mélységben) végezte el a TOE biztonsági tesztelését.

Az ATE_IND garanciacsalád azzal foglalkozik, hogy a TOE biztonsági funkcionalitását (TSF-et) milyen mértékű független (az értékelő által végrehajtott) funkcionális tesztelésnek vetették alá.

6.1.8.2. Funkcionális tesztek (ATE_FUN)

A fejlesztő által végrehajtott funkcionális tesztelés arra nyújt garanciát, hogy a tesztdokumentációban szereplő teszteket elvégezték és megfelelően dokumentálták. A tesztek és a TSF tervleírásának megfeleltetése a teszt lefedettség (ATE_COV) és mélység (ATE_DPT) családok segítségével történik.

6.1.8.2.1. ATE_FUN.1: Funkcionális tesztelés

Függések: ATE_COV.1

Fejlesztői akcióelemek:

ATE_FUN.1.1D A fejlesztőnek tesztelnie kell a TSF-t, és ennek eredményeit dokumentálnia kell.

ATE_FUN.1.2D A fejlesztőnek teszt dokumentációt kell biztosítania.

A bizonyíték elemek tartalma és bemutatása:

ATE_FUN.1.1C A tesztelési dokumentációnak tartalmaznia kell a tesztelési terveket, a várt teszteredményeket és a tényleges teszteredményeket.

ATE_FUN.1.2C A tesztelési terveknek azonosítaniuk kell a végrehajtandó teszteket, és le kell írniuk minden teszt végrehajtásának forgatókönyvét. Ezen forgatókönyveknek tartalmazniuk kell a más tesztek eredményeitől való minden sorrendbeli függést.

ATE_FUN.1.3C A várt teszteredményeknek be kell mutatniuk a tesztek sikeres végrehajtásából keletkező várható kimeneteket.

ATE_FUN.1.4C A tényleges teszteredményeknek összhangban kell állniuk a várt teszteredményekkel.

Értékelői akcióelemek:

ATE_FUN.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.8.3. Lefedettség (ATE_COV)

Az ATE_COV család azt garantálja, hogy a TSF-et a funkcionális specifikációnak megfelelően tesztelték. Az ellenőrzés a fejlesztői bizonyíték megfelelőség vizsgálatával történik.

6.1.8.3.1. ATE_COV.1: A lefedettség bizonyítéka

Függések: ADV_FSP.2, ATE_FUN.1

Fejlesztői akcióelemek:

ATE_COV.1.1D A fejlesztőnek biztosítania kell a teszt lefedettség bizonyítékát.

A bizonyíték elemek tartalma és bemutatása:

ATE_COV.1.1C A teszt lefedettség bizonyítékának be kell mutatnia a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikációban leírt TSFI-k közötti megfeleltetést.

Értékelői akcióelemek:

ATE_COV.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.8.3.2. ATE_COV.2: A lefedettség vizsgálata

Függések: ADV_FSP.2, ATE_FUN.1

Fejlesztői akcióelemek:

ATE_COV.2.1D A fejlesztőnek biztosítania kell a teszt lefedettség **elemzését**.

A bizonyíték elemek tartalma és bemutatása:

ATE_COV.2.1C A teszt lefedettség **elemzésének** szemléltetnie kell a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikációban leírt TSFI-k közötti megfelelést.

ATE_COV.2.2C **A teszt lefedettség elemzésének szemléltetnie kell, hogy a funkcionális specifikációban leírt összes TSFI-t letesztelték.**

Értékelői akcióelemek:

ATE_COV.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.8.4. Mélység (ATE_DPT)

Az ATE_DPT garanciacsalád összetevői az mondják meg, hogy a fejlesztő milyen részletességi szint szerint végzi a TSF tesztelését.

6.1.8.4.1. ATE_DPT.1: Az alap terv tesztelése

Függések: ADV_ARC.1, ADV_TDS.2, ATE_FUN.1

Fejlesztői akcióelemek:

ATE_DPT.1.1D A fejlesztőnek teszt mélység elemzést kell biztosítania.

A bizonyíték elemek tartalma és bemutatása:

ATE_DPT.1.1C A teszt mélység elemzésnek szemléltetnie kell a tesztelési dokumentációban azonosított tesztek és a TOE tervben szereplő TSF alrendszerek közötti megfelelést.

ATE_DPT.1.2C A teszt mélység elemzésnek szemléltetnie kell, hogy a TOE tervben szereplő összes TSF alrendszert letesztelték.

Értékelői akcióelemek:

ATE_DPT.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.8.4.2. ATE_DPT.2: A biztonságot érvényre juttató modulok tesztelése

Függések: ADV_ARC.1, ADV_TDS.3, ATE_FUN.1

Fejlesztői akcióelemek:

ATE_DPT.2.1D A fejlesztőnek teszt mélység elemzést kell biztosítania.

A bizonyíték elemek tartalma és bemutatása:

ATE_DPT.2.1C A teszt mélység elemzésnek szemléltetnie kell a tesztelési dokumentációban azonosított tesztek és a TOE tervben szereplő TSF alrendszerek és modulok közötti megfelelést.

ATE_DPT.2.2C A teszt mélység elemzésnek szemléltetnie kell, hogy a TOE tervben szereplő összes TSF alrendszert letesztelték.

ATE_DPT.2.3C **A teszt mélység elemzésnek szemléltetnie kell, hogy a TOE tervben szereplő SFR-t érvényre juttató modulokat letesztelték.**

Értékelői akcióelemek:

ATE_DPT.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.8.5. Független tesztelés (ATE_IND)

Az ATE_IND garanciacsalád azzal foglalkozik, hogy a TSF-et milyen mértékű független (az értékelő által végrehajtott) funkcionális tesztelésnek vetik alá.

6.1.8.5.1. ATE_IND.1: Független tesztelés – megfelelőség

Függések: ADV_FSP.1, AGD_OPE.1, AGD_PRE.1

Fejlesztői akcióelemek:

ATE_IND.1.1D A fejlesztőnek a teszteléshez biztosítania kell a TOE-t.
A bizonyíték elemek tartalma és bemutatása:

ATE_IND.1.1C A TOE-nek tesztelésre alkalmas állapotban kell lennie.

Értékelői akcióelemek:

ATE_IND.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ATE_IND.1.2E Az értékelőnek tesztelnie kell a TSF interfészeinek egy részét annak megerősítése érdekében, hogy a TSF a specifikáltaknak megfelelően működik.

6.1.8.5.2. ATE_IND.2: Független tesztelés – minta

Függések: ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1

Fejlesztői akcióelemek:

ATE_IND.2.1D A fejlesztőnek a teszteléshez biztosítania kell a TOE-t.

A bizonyíték elemek tartalma és bemutatása:

ATE_IND.2.1C A TOE-nek tesztelésre alkalmas állapotban kell lennie.

ATE_IND.2.2C **A fejlesztőnek biztosítania kell a TSF fejlesztői funkcionális tesztelése során használt erőforrás-készlettel azonos eszközkészletet.**

Értékelői akcióelemek:

ATE_IND.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ATE_IND.2.2E **Az értékelőnek végre kell hajtania a tesztelési dokumentációban szereplő tesztek valamely részhalmazát (mintáját) a fejlesztői teszt eredmények ellenőrzése érdekében.**

ATE_IND.2.3E Az értékelőnek tesztelnie kell a TSF interfészeinek egy részét annak megerősítése érdekében, hogy a TSF a specifikáltaknak megfelelően működik.

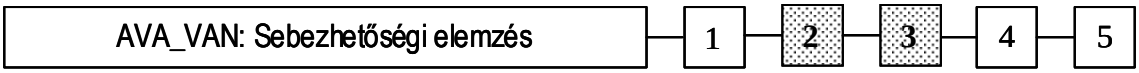
6.1.9. Sebezhetőség felmérés garanciaosztály (AVA)

6.1.9.1. A Sebezhetőség felmérés garanciaosztály áttekintése

Az AVA garanciaosztály a TOE fejlesztése vagy üzemeltetése során bevezetett kihasználható sebezhetőségek lehetőségével foglalkozik. Olyan elemzést jelent, melynek célja annak megállapítása, hogy a TOE fejlesztése és elvárt működése értékelése során vagy egyéb módszerekkel azonosított lehetséges sebezhetőségek vezethetnek-e oda, hogy egy támadó megsérti a funkcionális biztonsági követelményeket.

A sebezhetőség felmérés az értékelő feladata, ehhez a fejlesztőnek csak az értékelés tárgyához való hozzáférést kell biztosítania.

A 8. ábra az AVA CC garanciaosztályon belüli családokat, s a családokon belül az összetevők hierarchiáját mutatja. A jelen dokumentum által meghatározott értékelési módszertannak csak az ábrán külön megjelölt garancia-összetevők képezik részét.



8. ábra - A sebezhetőség felmérés garanciaosztály felépítése

6.1.9.2. Sebezhetőségi elemzés (AVA_VAN)

Az AVA_VAN garanciacsalád azt a fenyegetést fedi le, amit egy támadó jelent olyan hibák felfedezésével, amelyek jogosulatlan hozzáférést adnak számára adatokhoz és funkcionalitáshoz, lehetővé teszik, hogy beavatkozzon a TSF-be vagy módosítsa annak működését, illetve beavatkozzon jogosult felhasználók műveleteibe.

A család összetevőinek szintjei az értékelő által elvégzendő sebezhetőségi elemzés emelkedő szigora, illetve a lehetséges sebezhetőségek támadó általi azonosításához szükséges támadó képesség szintjei szerint különböznek.

6.1.9.2.1. AVA_VAN.2: Sebezhetőség vizsgálat

Függések: ADV_ARC.1, ADV_FSP.1, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1

Fejlesztői akcióelemek:

AVA_VAN.2.1D A fejlesztőnek a teszteléshez biztosítania kell a TOE-t.

A bizonyíték elemek tartalma és bemutatása:

AVA_VAN.2.1C A TOE-nak alkalmasnak kell lennie tesztelésre.

Értékelői akcióelemek:

AVA_VAN.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

AVA_VAN.2.2E Az értékelőnek egy keresést kell végrehajtania nyilvános forrásokban a TOE lehetséges sebezhetőségeinek azonosítása érdekében.

AVA_VAN.2.3E Az értékelőnek egy független sebezhetőség vizsgálatot kell végrehajtania a TOE-ra, az útmutató dokumentációt, funkcionális specifikációt, TOE tervet, és a biztonsági szerkezet leírást használva, a TOE lehetséges sebezhetőségeinek azonosítása érdekében.

AVA_VAN.2.4E Az értékelőnek az azonosított lehetséges sebezhetőségek alapján áthatolás tesztelést kell végrehajtania, annak megállapítása érdekében, hogy a TOE ellenáll egy alap támadó képességgel rendelkező támadó által végrehajtott támadásnak.

6.1.9.2.2. AVA_VAN.3: Célirányos sebezhetőség vizsgálat

Függések: ADV_ARC.1, ADV_FSP.2, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1

Fejlesztői akcióelemek:

AVA_VAN.3.1D A fejlesztőnek a teszteléshez biztosítania kell a TOE-t.

A bizonyíték elemek tartalma és bemutatása:

AVA_VAN.3.1C A TOE-nak alkalmasnak kell lennie tesztelésre.

Értékelői akcióelemek:

AVA_VAN.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

AVA_VAN.3.2E Az értékelőnek egy keresést kell végrehajtania nyilvános forrásokban a TOE lehetséges sebezhetőségeinek azonosítása érdekében.

AVA_VAN.3.3E Az értékelőnek egy független sebezhetőség vizsgálatot kell végrehajtania a TOE-ra, az útmutató dokumentációt, funkcionális specifikációt, TOE tervet, a biztonsági szerkezet leírást **és a megvalósítási reprezentációt** használva, a TOE lehetséges sebezhetőségeinek azonosítása érdekében.

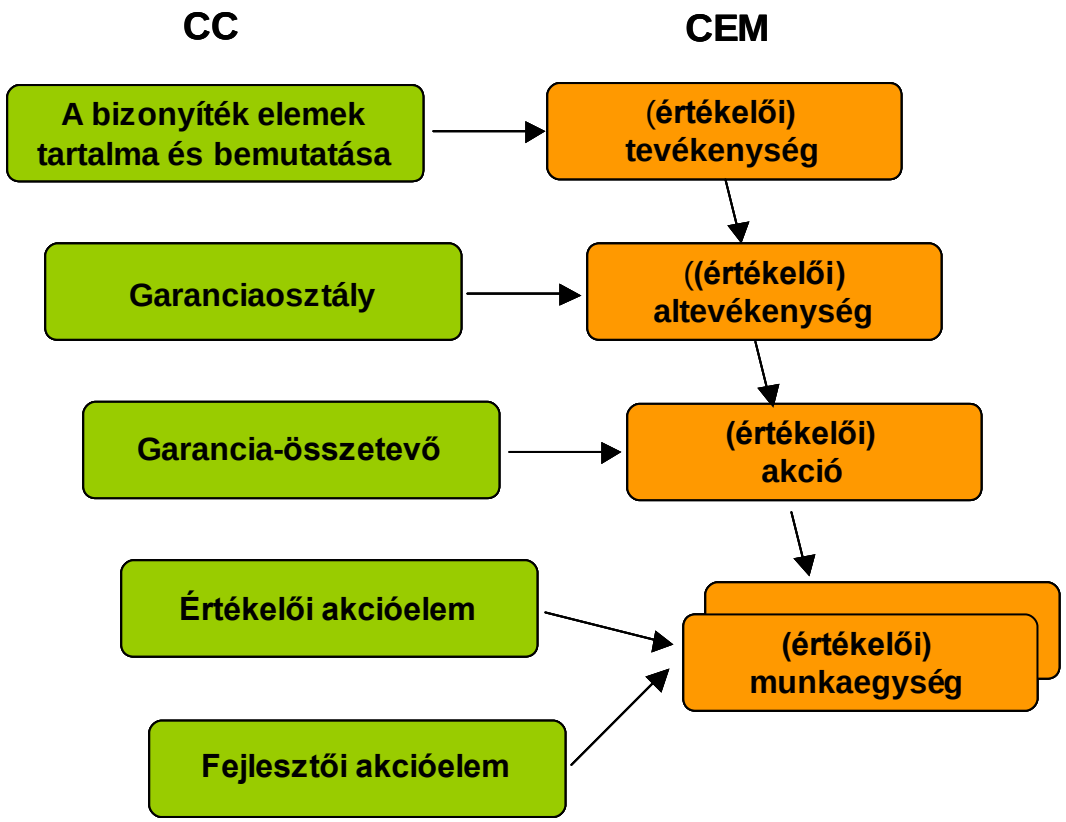
AVA_VAN.3.4E Az értékelőnek az azonosított lehetséges sebezhetőségek alapján áthatolás tesztelést kell végrehajtania, annak megállapítása érdekében, hogy a TOE ellenáll egy **megemelt-alap** támadó képességgel rendelkező támadó által végrehajtott támadásnak.

6.2. Útmutató a termékek biztonsági értékelői számára

6.2.1. Általános értékelői feladatok

6.2.1.1. A CC és a CEM struktúrák közötti kapcsolat

Közvetlen összefüggés áll fenn a CC struktúra (vagyis osztály, család, összetevő és elem) és a CEM struktúrája között. A 9. ábra bemutatja a megfelelést a CC-t alkotó osztály, összetevő és értékelői akcióelemek, valamint a CEM tevékenységek, altevékenységek és akciók között. Számos CEM munkaegység származhat a CC fejlesztői akcióelemeknél, illetve a bizonyítékelemek tartalma és bemutatása elemeknél megjegyzett követelményekből is.



9. ábra – A CC és a CEM struktúráinak megfeleltetése

Ez az alfejezet áttekinti az értékelés folyamatát, s meghatározza azokat a feladatokat, melyeket egy értékelőnek az értékelés során végre kell hajtania.

Minden értékelés ugyanazt a folyamatot követi, és négy általános értékelői feladatból áll: bemeneti feladat, kimeneti feladat, értékelői altevékenységek, valamint a műszaki alkalmasság demonstrálása a tanúsító szervezet számára.

A bemeneti és kimeneti feladatot, melyek az értékelési bizonyíték kezelésével, illetve a jelentés készítéssel állnak kapcsolatban, teljes mértékben ez a fejezet ismerteti. Mindkét feladathoz tartoznak olyan kapcsolódó részfeladatok, amelyek minden értékelésre kötelezően vonatkoznak.

Az értékelői altevékenységekkel kapcsolatban ez a fejezet csak bevezetőt tartalmaz, azokat a következő fejezetek részletezik.

Az értékelői altevékenységekkel szemben a bemeneti és kimeneti feladatokhoz nem kapcsolódnak határozatok, minthogy ezek nem kapcsolódnak CC értékelői akcióelemhez; ezeket az általános elveknek és a CEM-nek való megfelelés céljából végzik el.

Az a feladat, hogy a műszaki alkalmasságot bizonyítani kell a tanúsító szervezet felé, teljesíthető azáltal, hogy a tanúsító szervezet megvizsgálja a kimeneti feladatok eredményeit, vagy magában foglalhatja az értékelői bizonyítást az értékelői altevékenységek bemeneteinek

megértésére vonatkozóan. Ehhez a feladathoz értékelői döntés nem tartozik, de tartozik hozzá a tanúsító szervezet egy döntése.

6.2.1.2. Az értékelési folyamat áttekintése

Ez az fejezet a módszer általános modelljét mutatja be, és meghatározza a következőket:

a) az értékelési folyamatban érintett felek szerepköreit és felelősségeit;
b) az általános értékelési modellt.

6.2.1.2.1. Az egyes szereplők felelősségei

Az általános modell a következő szerepköröket definiálja: megbízó, fejlesztő, értékelő és értékelési hatóság (tanúsító szervezet).

A megbízó felelős az értékelés kérelmezéséért és támogatásáért. Ez azt jelenti, hogy a megbízó köti meg az értékeléshez szükséges különböző szerződéseket (pl. értékelés megrendelése). Ezenfelül a megbízó a felelős annak biztosításáért, hogy az értékelő megkapja az értékelési bizonyítékokat.

A fejlesztő állítja elő a TOE-t, és felelős azoknak a bizonyítékoknak a biztosításáért, amelyek az értékeléshez szükségesek (pl. képzés, terv információk), a megbízó képviseletében.

Az értékelő hajtja végre az értékelési feladatokat, amik szükségesek egy értékeléssel összefüggésben: az értékelő átveszi az értékelési bizonyítékokat a megbízót képviselő fejlesztőtől vagy közvetlenül a megbízótól, végrehajtja az értékelési altevékenységeket, és az értékelési megállapítások eredményeit a tanúsító szervezet részére rendelkezésre bocsátja.

A tanúsító szervezet kialakítja és fenntartja a sémát, figyeli az értékelő által lefolytatott értékelést, és az értékelő által átadott értékelési eredmények alapján tanúsítási jelentéseket és tanúsítványokat bocsát ki.

6.2.1.2.2. A szereplők közötti kapcsolat

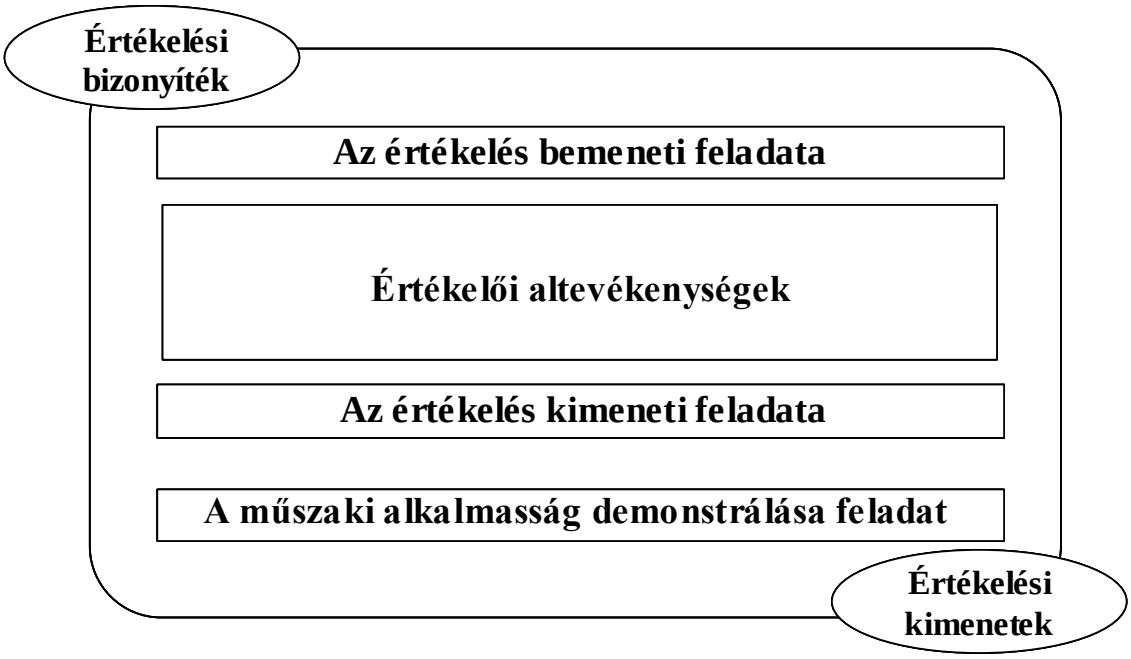
Annak megelőzésére, hogy illetéktelen hatás helytelenül befolyásoljon egy értékelést, a szerepköröknek bizonyos elkülönítése szükséges. Ez azt jelenti, hogy a fentebb ismertetett szerepköröket eltérő entitások töltik be, kivéve, hogy a fejlesztői és a megbízói szerepkört kielégítheti egyetlen entitás.

6.2.1.2.3. Általános értékelési modell

Az értékelési folyamat az értékelő által végrehajtott értékelés bementi feladatból, értékelés kimeneti feladatból, valamint az értékelői altevékenységekből áll. A 10. ábra áttekintést nyújt ezen feladatok és altevékenységek közötti kapcsolatról.

Az értékelési folyamatot megelőzheti egy előkészítési szakasz, amikor a megbízó és az értékelő közötti kezdeti kapcsolat kialakítása történik. Az ebben a szakaszban végrehajtandó

munka és a különböző szerepkörök bevonása változatos lehet. Tipikus, hogy az értékelő ennek a szakasznak a folyamán végrehajt egy megvalósíthatósági vizsgálatot a sikeres értékelés valószínűségének felmérésére.



10. ábra – Általános értékelési modell

6.2.1.2.4. Értékelői határozatok

Az értékelő a CC követelményeire hozza meg a határozatokat (nem az értékelési módszertan követelményeire). A legelemibb CC struktúra, melyhez határozat rendelhető a (közvetlen vagy közvetett) értékelői akcióelem. Egy CC értékelői akcióelemhez rendelt határozat a kapcsolódó CEM akció és az azt alkotó munkaegységek végrehajtásának eredményeként születik. Végül előáll egy értékelési eredmény (általános határozat).

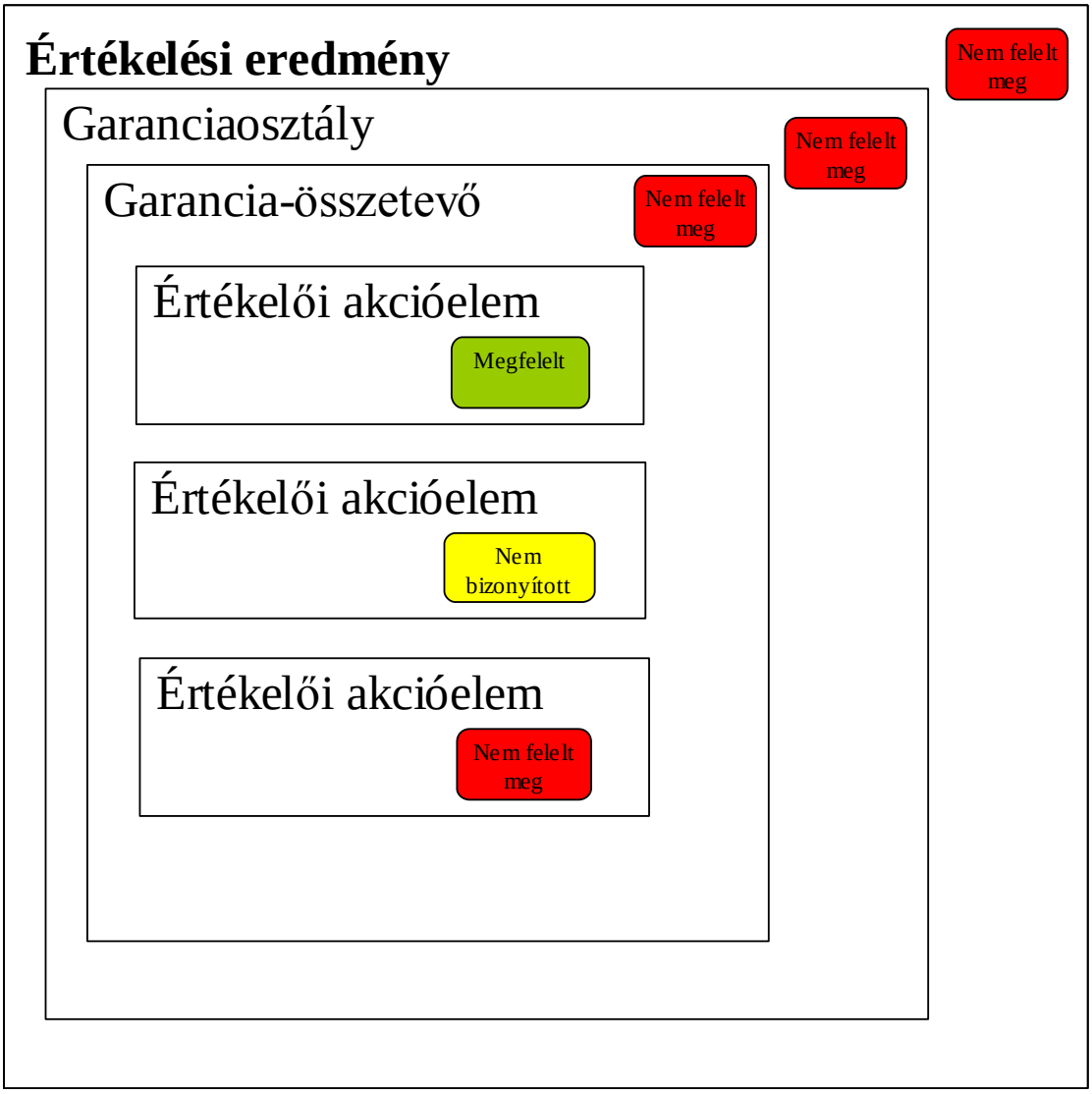
Az értékelési módszertan három, egymást kölcsönösen kizáró határozatot ismer el:

a) Egy *"Megfelelt"* határozat feltétele, hogy az értékelő befejezze a CC értékelői akcióelemet, s megállapítsa, hogy az értékelés alatt álló ST-re vagy TOE-re vonatkozó követelmények teljesülnek. Az értékelői akcióelem megfelelésének feltételeit az alábbiak határozzák meg:
   aa) az érintett CEM akcióhoz tartozó munkaegységek, továbbá
   ab) az érintett munkaegység végrehajtásához megkövetelt valamennyi értékelési bizonyíték az értékelő számára teljesen érthető, valamint
   ac) az érintett munkaegység végrehajtásához megkövetelt valamennyi értékelési bizonyíték mentes a nyilvánvaló belső, vagy más értékelői bizonyítékkal való ellentmondásoktól. (A nyilvánvaló kifejezés itt azt jelenti, hogy az értékelő az ellentmondást a munkaegység végrehajtása során feltárja: az értékelőnek nem kell egy teljes

konzisztencia-vizsgálatot végeznie az összes értékelési bizonyítékon minden egyes végrehajtott munkaegység során.)

b) Egy *"Nem felelt meg"* határozat feltétele, hogy az értékelő befejezze a CC értékelői akcióelemet, s megállapítsa, hogy az értékelés alatt álló ST-re vagy TOE-re vonatkozó követelmények nem teljesülnek, vagy a bizonyíték nem érthető, vagy az értékelési bizonyítékban nyilvánvaló ellentmondást találtak.
c) Minden határozat kezdetben *"Nem bizonyított"*, s mindaddig az marad, amíg vagy *"Megfelelt"* vagy *"Nem felelt meg"* határozat nem születik.

Az általános határozat akkor és csak akkor „Megfelelt", ha a részét képező valamennyi határozat is „Megfelelt". A 11. ábrán szemléltetett példában egyetlen értékelői akcióelemre hozott „Nem felelt meg" határozat az érintett garancia-összetevő és garanciaosztály, valamint az általános határozat „Nem felelt meg" eredményét okozza.



11. ábra – Példa a határozat hozatal szabályra

6.2.1.3. Az értékelés bemeneti feladata

Ennek a feladatnak a célja annak biztosítása, hogy az értékelő számára hozzáférhető legyen az összes szükséges értékelési bizonyíték, egyben azokat megfelelően védjék is meg. Máskülönben nem garantálható sem az értékelés műszaki pontossága, sem az értékelés megismételhetősége és újraelőállíthatósága.

Az összes elvárt értékelési bizonyíték biztosítása a megbízó felelőssége. Ugyanakkor az értékelési bizonyíték nagy részét valószínűleg a fejlesztő állítja elő és szállítja a megbízó nevében.

Minthogy a garanciális biztonsági követelmények a teljes TOE-ra vonatkoznak, a TOE részét képező valamennyi termékhez kapcsolódó értékelési bizonyítékot az értékelő rendelkezésére kell bocsátani. Az ilyen értékelési bizonyíték érvényességi köre és megkívánt tartalma független attól az ellenőrzési szinttől, amellyel a fejlesztő rendelkezik a TOE részét képező valamennyi termék felett. Például ha egy magas-szintű terv meg van követelve, akkor a „TOE terv” (ADV_TDS) követelmények minden olyan alrendszerre vonatkoznak, amelyek a TSF részét képezik. Ezenfelül azok a garanciális biztonsági követelmények, amelyek eljárások meglétét teszik szükségessé (például a „Konfiguráció kezelési képességek” (ALC_CMC) és a „Szállítás” (ADO_DEL)), ugyancsak a teljes TOE-ra vonatkoznak (beleértve a más fejlesztőtől származó bármilyen terméket).

Ajánlott, hogy az értékelő a megbízóval együtt készítse el az elvárt értékelési bizonyítékok listáját. Ez a lista a dokumentációkra való hivatkozásokból állhat. Erősen ajánlott, hogy ez a lista elegendő információt tartalmazzon ahhoz, hogy segítse az értékelőt az elvárt bizonyíték könnyű megtalálásában (pl. minden dokumentum rövid összefoglalásával, vagy legalább a cím tételes megadásával és az érdeklődésre számot tartó részek feltüntetésével).
Az értékelési bizonyítékban foglalt információ a követelmény, nem pedig valamilyen sajátos dokumentum szerkezet. Egy altevékenységre vonatkozó értékelési bizonyíték megadható különálló dokumentumok formájában, vagy egy dokumentum kielégítheti egy altevékenység több bemeneti követelményét is.

Az értékelő megbízható és hivatalosan kibocsátott értékelési bizonyítékot igényel. Ugyanakkor egy értékeléshez tervezet is adható, például annak elősegítése érdekében, hogy az értékelő korai, informális megállapításokra juthasson, de ez nem használható a határozat hozatal alapjául. Az értékelőt az egyes értékelési bizonyítékok tervezet verziói az alábbi esetekben segíthetik:

a) teszt dokumentáció, mely biztosítja, hogy az értékelő a tesztekről és teszt eljárásokról egy előzetes értékelést készítsen,
b) terv dokumentációk, melyek segítik az értékelőt, hogy megértse a TOE tervezését,
c) forráskód vagy hardver vázlatok, melyek azt segítik elő, hogy az értékelő felmérje a fejlesztői szabványok alkalmazását (csak kiemelt garanciaszinten).

A bizonyítékok tervezetével általában akkor találkozunk, ha a TOE értékelése a fejlesztéssel párhuzamosan történik. Akkor is találkozhatunk ezzel, amikor egy már kifejlesztett TOE értékelése során a fejlesztő - az értékelő által felvetett probléma megoldására - további módosítást hajt végre (pl. egy tervezési vagy kivitelezési hiba javítására), vagy amikor a

biztonságot érintő olyan bizonyítékra van szükség, melyet a dokumentáció nem tartalmaz (pl. egy olyan TOE esetén, melyet eredetileg nem a CC követelményei szerint fejlesztettek).

Az értékelés bemeneti feladata az értékelési bizonyíték kezelésének alábbi három részfeladatából áll:

a) konfiguráció ellenőrzés
b) eltávolítás
c) a bizalmasság biztosítása

6.2.1.3.1. Konfiguráció ellenőrzés

Az értékelőnek végre kell hajtania az értékelési bizonyíték konfiguráció ellenőrzését.
Az értékelőnek képesnek kell lennie az értékelési bizonyíték kézhez vétele után annak minden tételének az azonosítására és elhelyezésére, valamint annak meghatározására is, hogy egy adott dokumentum verzió a birtokában van-e.

Az értékelőnek meg kell védenie az értékelési bizonyítékot a módosítástól vagy elvesztéstől mindazon idő alatt, míg a birtokában van.

6.2.1.3.2. Eltávolítás

Az értékelési folyamat végén az értékelési bizonyítékokat el kell távolítani. Az értékelési bizonyítékok eltávolítására az alábbi lehetőségek vannak, melyből egy vagy több is alkalmazható:

a) az értékelési bizonyíték visszaszolgáltatása,
b) az értékelési bizonyíték archiválása,
c) az értékelési bizonyíték megsemmisítése.

A fenti lehetőségekből való választás az értékelő és a megbízó közötti megállapodástól függ.

6.2.1.3.3. A bizalmasság biztosítása

Az értékelőnek egy értékelés során valószínűleg a megbízó és a fejlesztő érzékeny üzleti információihoz (pl. TOE tervezési információ, szakértői eszközök), esetleg nemzetbiztonsági szempontból érzékeny információkhoz is hozzá kell férniük. Az értékelés séma (MIBÉTS) megköveteli az értékelőtől az értékelési bizonyíték bizalmasságának megtartását. A megbízó és az értékelő kölcsönösen megegyezhet további követelményekben is, amennyiben azok nem mondanak ellent a séma előírásainak.

A bizalmasság követelményei az értékelő munka sok szempontját érintik, beleértve az értékelési bizonyíték kézhez vételét, kezelését, tárolását és eltávolítását is.

6.2.1.4. Értékelői altevékenységek

Az értékelési altevékenységek a kiválasztott garanciális követelményektől, vagyis a garanciaszinttől függnek (lásd 2. táblázat).

6.2.1.5. Az értékelés kimeneti feladata

Az értékelés kimenti feladata az észrevételezési jelentés (OR, Observation Report) és az értékelési jelentés (ETR, Evaluation Technical Report) készítéséből áll.

Annak érdekében, hogy az eredmények megismételhetősége és újraelőállíthatósága általános elve teljesüljön, az értékelési eredményeket konzisztens módon kell rögzíteni. A konzisztencia magában foglalja az OR-ben és ETR-ben jelentett információk típusát és mennyiségét is. Az ETR-ek és OR-ek különböző értékelések közötti konzisztenciájának az ellenőrzése és biztosítása a tanúsító szervezet felelőssége.

Az értékelőnek az alábbi két részfeladatot kell elvégeznie:

a) OR írás részfeladat (amennyiben az értékelés szükségessé teszi),
b) ETR írás részfeladat.

6.2.1.5.1. Az értékelés kimeneteinek a kezelése

Az értékelőnek – mihelyt elkészülnek – át kell adnia az ETR-t és az összes OR-t a tanúsító szervezetnek.

Az értékelőnek – mihelyt elkészülnek – véleményezésre át kell adnia az ETR-t a megbízónak.

Az értékelőnek – a benne foglalt TOE-ra vonatkozó problémák tisztázása vagy megoldása érdekében - át kell adnia az OR-t a megbízónak.

Az ETR és OR-k érzékeny információt vagy magántitkot is tartalmazhat, ezért a megbízónak való átadás előtt egy kivonatolásra lehet szükség.

6.2.1.5.2. Észrevételezési jelentés írás részfeladat

Az észrevételezési jelentések (OR-ek) azt a mechanizmust biztosítják az értékelő számára, amivel egy értékelést érintő problémát tisztázni, illetve azonosítani lehet.

Egy "Nem felelt meg" határozat esetén az értékelőnek OR-t kell biztosítania az értékelési eredmény alátámasztására. Ezen kívül az értékelő az OR-t egy probléma tisztázására vonatkozó igény kifejezésére is felhasználhatja.

Az értékelőnek minden OR-ben legalább az alábbiakat kell jelentenie:

a) az értékelt TOE azonosítója,
b) az az értékelői feladat/altevékenység, mely során az észrevétel felbukkant,
c) az észrevétel,
d) az észrevétel súlyosságának megbecslése (pl. „Nem felelt meg” határozatot eredményez, az értékelési folyamat felfüggesztését okozza, még az értékelés befejezése előtt megoldást vár),
e) a probléma megoldásáért felelős szervezet azonosítása,
f) ajánlás a probléma megoldására szolgáló időtartamra;

g) az értékelést érintő hatások megbecslése az észrevétel által felvetett probléma megoldásának kudarca esetén.

Egy OR olvasói köre és a jelentés kezelésére vonatkozó eljárások a jelentés tartalmától és a séma előírásaitól függnek. A MIBÉTS séma az alábbi típusú OR-ek különbözteti meg:

a) OR a tanúsító szervezetnek (pl. egy követelmény alkalmazására vonatkozóan),
b) OR a megbízóknak (pl. egy TOE-n belül talált probléma megoldására).

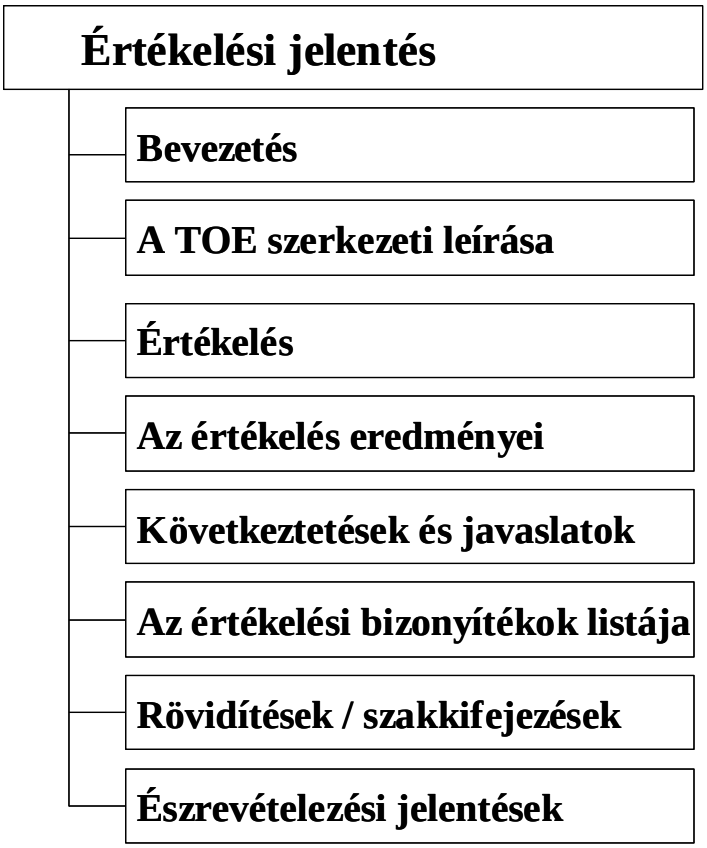
6.2.1.5.3. Értékelési jelentés írás részfeladat

Az értékelőnek ETR-t kell biztosítania a TOE értékelésére vonatkozó határozatok műszaki indoklásának bemutatására.

Az ETR olvasójáról feltételezés, hogy tisztában van az információ biztonság, a CC, a CEM, az értékelési megközelítés, valamint az informatika alapkoncepcióival.

Az ETR támogatja a tanúsító szervezetet annak megerősítésében, hogy az értékelést az elvárt szabványnak megfelelően folytatták.

Az alábbiak a TOE értékelésekre vonatkozó ETR-ek minimális tartalmát ismertetik. Az ETR tartalmát a 12. ábra mutatja be; ez az ábra útmutatóként használható az ETR dokumentum szerkezetének kialakításakor.



12. ábra – Az ETR információ tartalma egy TOE értékelése esetén

Bevezetés

Az értékelőnek jelentésbe kell foglalnia az értékelési séma azonosítókat.

Az értékelési séma azonosítók (pl. MIBÉTS logó) azok az információk, amelyeket az értékelés átvizsgálásáért felelős séma egyértelmű azonosításához követelnek meg.

Az értékelőnek jelentésbe kell foglalnia az ETR konfiguráció ellenőrzési azonosítókat.

Az ETR konfiguráció ellenőrzési azonosítók olyan információkat tartalmaznak, amelyek azonosítják az ETR-t (pl. megnevezés, dátum és verziószám).

Az értékelőnek jelentésbe kell foglalnia az ST és TOE konfiguráció ellenőrzési azonosítókat.

Az ST és TOE konfiguráció ellenőrzési azonosítókat (pl. megnevezés, dátum és verziószám) az értékelés alatt álló ST és TOE azonosításához követelik meg abból a célból, hogy a tanúsító szervezet ellenőrizhesse, hogy az értékelő a határozatokat helyesen rendelte ezekhez.

Amennyiben az ST a TOE egy vagy több PP-nek való megfelelését állítja, akkor az ETR-nek jelentésbe kell foglalnia a megfelelő PP-(k)re való hivatkozást.

A PP-kre való hivatkozás olyan információkat tartalmaz, amelyek egyértelműen azonosítják a PP-ket (pl. cím, dátum és verziószám).

Az értékelőnek jelentésbe kell foglalnia a fejlesztő azonosítóját.

A TOE fejlesztő azonosítóját azért követelik meg, hogy azonosítva legyen a TOE készítéséért felelős fél.

Az értékelőnek jelentésbe kell foglalnia a megbízó azonosítóját.

A megbízó azonosítóját azért követelik meg, hogy azonosítva legyen az a fél, aki az értékelési bizonyítéknak az értékelő rendelkezésére bocsátásáért felelős.

Az értékelőnek jelentésbe kell foglalnia az értékelő azonosítóját.

Az értékelő azonosítóját azért követelik meg, hogy azonosítva legyen az értékelést végrehajtó fél, aki az értékelési határozatokért felelős.

A TOE szerkezeti leírása

Az értékelőnek jelentésbe kell foglalnia a TOE és legfőbb összetevői magas szintű leírását, a "TOE terv” (ADV_TDS) garanciacsaládban meghatározott értékelési bizonyíték alapján.

Ennek a fejezetnek a célja a fő összetevők szerkezeti elkülönülésének a jellemzése.

Az értékelés jellemzése

Az értékelőnek jelentésbe kell foglalnia az alkalmazott értékelési módszereket, technikákat, eszközöket és szabványokat.

Az értékelő hivatkozhat a TOE értékelésénél felhasznált értékelési követelményekre, módszertanra és értelmezésekre, illetve a tesztelés során használt eszközökre.

Az értékelőnek jelentésbe kell foglalnia minden értékelésre, illetve az értékelési eredmények terjesztésére vonatkozó korlátozást, valamint az értékelés során tett mindazon feltételezést, mely az eredményekre hatással van.

Az értékelő ebben a részben elhelyezhet jogi kötöttségekre, szervezetre vagy bizalmasságra vonatkozó információkat is.

Az értékelés eredményei

A TOE értékelés minden tevékenységére az értékelőnek jelentésbe kell foglalnia:
- az érintett tevékenység elnevezését;
- egy határozatot és az ezt alátámasztó indoklást, az adott tevékenységet alkotó valamennyi garancia-összetevőre vonatkozóan, a megfelelő CEM akció és az ezt alkotó munkaegységek végrehajtásának eredményeképpen.

Az indoklás igazolja a határozatot a CC, a CEM, valamilyen értelmezés és a vizsgált értékelési bizonyíték felhasználásával, valamint bemutatja, hogy az értékelési bizonyíték hogyan teljesíti vagy nem teljesíti a szempontok valamennyi aspektusát. Leírja a végrehajtott munkát, a felhasznált módszert és az eredmények levezetését. Az indoklás CEM munkaegység szintű részleteket is megadhat.

Az értékelőnek jelentésbe kell foglalnia minden információt, amit egy munkaegység kimondottan megkövetel.

Az AVA és ATE tevékenységekre leírt számos munkaegység meghatározza az ETR-ben megadandó információkat is.

Következtetések és javaslatok

Az értékelőnek jelentésbe kell foglalnia az értékelés következtetéseit, amelyek arra vonatkoznak, hogy a TOE megfelel-e a kapcsolódó ST-nek, ahogyan azt a 6.2.1.2.4 által leírt határozat hozatal eljárás meghatározza.

Az értékelő javaslatokat tehet, mely hasznos lehet a tanúsító szervezetnek. Ezek a javaslatok az IT termék értékelés során feltárt hiányosságaira, gyengeségeire, vagy ellenkezőleg, a különösen hasznos tulajdonságaira vonatkozhatnak.

Az értékelési bizonyítékok listája

Az értékelőnek valamennyi értékelési bizonyítékra jelentésbe kell foglalnia az alábbi információkat:

— a kibocsátó szervezet (pl. fejlesztő, megbízó),
— cím,
— egyedi azonosító (pl. kibocsátási dátum és verziószám).

Rövidítések és szakkifejezések

Az értékelőnek jelentésbe kell foglalnia az ETR-ben használt valamennyi szakkifejezést és rövidítést.

A jelen értékelési módszertanban már meghatározott szakkifejezéseket és rövidítéseket nem kell megismételni.

Észrevételezési jelentések

Az értékelőnek jelentésbe kell foglalnia az értékelés során keletkezett észrevételezési jelentéseket egyedileg azonosító teljes listát, az OR-ek állapotát is feltüntetve.

A listának minden észrevételezési jelentésre tartalmaznia kell az OR azonosítóját, illetve a címét vagy rövid tartalmi összefoglalását.

6.2.2. A biztonsági előirányzat értékelése

6.2.2.1. Bevezetés

Ez a fejezet egy ST értékelését írja le. Az ST értékelést minden egyéb TOE értékelési altevékenység előtt kell megkezdeni, mivel az ST szolgáltatja ezen altevékenységek alapját és környezetét. E fejezet értékelési módszertana az ST követelményein alapul, amit a CC 3. részének ASE osztálya határoz meg.

6.2.2.2. Alkalmazási megjegyzések

Egy vagy több tanúsított PP-n alapuló ST értékelése során lehetőség van annak a ténynek a felhasználására, hogy a szóban forgó PP-ket már tanúsították. Egy tanúsított PP eredményeinek újrafelhasználási lehetősége nagyobb, ha az ST nem ad hozzá fenyegetéseket, szervezeti biztonsági szabályzatokat, feltételezéseket, biztonsági célokat és/vagy biztonsági követelményeket a PP-ben szereplőkhöz. Amennyiben a ST sokkal több mindent tartalmaz, mint a tanúsított PP, akkor az eredmények újrafelhasználása egyáltalán nem biztos, hogy hasznos lesz.

Az értékelő számára lehetőség van a PP értékelési eredmények újrafelhasználására úgy, hogy bizonyos elemzéseket csak részben vagy egyáltalán nem végez el, ha ezek az elemzések vagy elemeik már a PP értékelés részét képezték. Ennek a folyamatnak a során az értékelő feltételezheti, hogy a PP–hez kötődő vizsgálatokat jól végezték el.

Példa a fentiekre: a PP tartalmaz adott biztonsági követelmény készletet, és ezeket a PP értékelés során belső ellentmondásoktól mentesnek találták. Ha az ST pontosan ugyanezeket a

követelményeket használja, akkor az ellentmondás-mentességi vizsgálatot nem kell megismételni az ST értékelés folyamán. Amennyiben az ST egy vagy több követelménnyel kiegészíti a védelmi profilt, vagy ezen követelményeken műveletet hajt végre, akkor az elemzést meg kell ismételni. Azonban ekkor is meg lehet takarítani munkát az ellentmondás-mentességi elemzés során azon tény alapján, hogy az eredeti követelmények belső ellentmondásoktól mentesek voltak. Ha az eredeti követelményekre ez utóbbi igaz, akkor az értékelőnek csak azt kell megállapítania, hogy:

a) az összes új és/vagy módosított követelmény belső ellentmondásoktól mentes-e, és
b) az összes új és/vagy módosított követelmény összhangban van-e az eredeti követelményekkel, nem mond-e ellent azoknak.

Az értékelő az ETR-ben megjegyzést tehet minden olyan esetről, amikor az elemzést nem ismételte meg, vagy csak részlegesen végezte el a fenti okok miatt.

6.2.2.3. Az ST bevezetés (ASE_INT.1) értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy az ST-t és a TOE-t helyesen azonosították-e, a TOE-t helyesen írták-e le az absztrakció három szintjén (TOE hivatkozás, TOE áttekintés, TOE leírás), továbbá ez a három leírás összhangban áll-e egymással.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST.

6.2.2.3.1. Az ASE_INT.1.1E értékelői akció

ASE_INT.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASE_INT.1.1C Az ST bevezetésnek tartalmaznia kell egy ST hivatkozást, egy TOE hivatkozást, egy TOE áttekintést és egy TOE leírást.

ASE_INT.1-1 Az értékelőnek ellenőriznie kell, hogy az ST bevezetés tartalmaz-e egy ST hivatkozást, egy TOE hivatkozást, egy TOE áttekintést és egy TOE leírást.

ASE_INT.1.2C Az ST hivatkozásnak egyértelműen azonosítania kell az ST-t.

ASE_INT.1-2 Az értékelőnek meg kell vizsgálnia az ST hivatkozást annak megállapítása érdekében, hogy az egyértelműen azonosítja-e az ST-t.

Az értékelő állapítsa meg, hogy az ST hivatkozás azonosítja-e az ST-t magát, úgy, hogy az jól megkülönböztethető legyen más ST-ktől, és egyedi módon azonosítja-e az ST minden egyes verzióját, például verziószámmal és/vagy a közzététel dátumával.

Mivel mindhárom garanciaszint elvárja a CM rendszer használatát, az értékelő érvényesítheti a hivatkozások egyediségét a konfiguráció lista ellenőrzésével.

ASE_INT.1.3C A TOE hivatkozásnak egyértelműen azonosítania kell a TOE-t.

ASE_INT.1-3 Az értékelőnek meg kell vizsgálnia a TOE hivatkozást annak megállapítása érdekében, hogy az egyértelműen azonosítja-e a TOE-t.

Az értékelő állapítsa meg, hogy a TOE hivatkozás oly módon azonosítja a TOE-t, hogy nyilvánvaló, melyik TOE verzióra vonatkozik az ST, továbbá azonosítja a TOE verzióját, például verzió/kibocsátás/build szám vagy a kiadás dátuma segítségével.

ASE_INT.1-4 Az értékelőnek meg kell vizsgálnia a TOE hivatkozást annak megállapítása érdekében, hogy az nem félrevezető-e.

Amennyiben a TOE egy vagy több jól ismert termékhez kapcsolódik, akkor ezt lehet szerepeltetni a TOE hivatkozásban. Azonban, ez nem vezetheti félre a felhasználókat, vásárlókat: nem megengedett olyan helyzet előállása, amikor egy terméknek csupán kis részét értékelik, de a TOE hivatkozás ezt nem tükrözi.

ASE_INT.1.4C A TOE áttekintésnek össze kell foglalnia a TOE használatát és fő biztonsági tulajdonságait.

ASE_INT.1-5 Az értékelőnek meg kell vizsgálnia a TOE áttekintést annak megállapítása érdekében, hogy az leírja-e a TOE használatát és fő biztonsági tulajdonságait.

A TOE áttekintésnek röviden (néhány bekezdésben) le kell írnia a TOE használatát és fő biztonsági tulajdonságait. A TOE áttekintésnek lehetővé kell tennie, hogy a potenciális vásárlók gyorsan el tudják dönteni ez alapján, hogy a TOE alkalmas-e biztonsági céljaik kielégítésére.

Az értékelő állapítsa meg, hogy az áttekintés érthető-e a fogyasztók számára, és kielégítő-e abból a szempontból, hogy a TOE tervezett használatáról és fő biztonsági tulajdonságairól általános leírást ad.

ASE_INT.1.5C A TOE áttekintésnek azonosítania kell a TOE típusát.

ASE_INT.1-6 Az értékelőnek ellenőriznie kell, hogy a TOE áttekintés azonosítja-e a TOE típusát.

ASE_INT.1-7 Az értékelőnek meg kell vizsgálnia a TOE áttekintést annak megállapítása érdekében, hogy az nem félrevezető-e.

Vannak olyan helyzetek, amikor az általános felhasználó a TOE típusa miatt elvár bizonyos funkcionalitást a TOE-tól. Ha ez a funkcionalitás hiányzik, akkor az értékelő állapítsa meg, hogy a TOE áttekintés megfelelően tárgyalja-e ezen funkció hiányát.

Vannak olyan TOE-k, melyek esetén egy általános felhasználó a TOE típusa miatt azt várja el, hogy a TOE képes működni egy adott üzemeltetési környezetben. Ha a TOE nem képes teljesíteni ezt az elvárást, akkor az értékelő állapítsa meg, hogy a TOE áttekintés megfelelően tárgyalja-e ezt.

ASE_INT.1.6C A TOE áttekintésnek azonosítania kell a TOE által megkövetelt valamennyi TOE-n kívüli hardvert/szoftvert/förmvert.

ASE_INT.1-8 Az értékelőnek meg kell vizsgálnia a TOE áttekintést annak megállapítása érdekében, hogy az azonosít-e minden TOE által megkövetelt TOE-n kívüli hardvert/szoftvert/förmvert.

Míg egyes TOE-k képesek stand-alone módban üzemelni, más TOE-k (különösen a szoftver TOE-k) számára szükség van hardverre, más szoftver vagy förmver komponensre. Ha a TOE nem igényel semmilyen hardvert, szoftvert vagy förmvert, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekintendő.

Az értékelő állapítsa meg, hogy a TOE áttekintés azonosít-e minden egyéb hardvert, szoftvert és förmvert, ami a TOE működéséhez szükséges. Ez az azonosítás nem feltétlenül minden apró részletre kiterjedő, de kellően részletes ahhoz, hogy a TOE potenciális felhasználói meg tudják mondani ez alapján, hogy az ő általuk alkalmazott hardver, szoftver és förmver támogatja-e a TOE használatát, és ha nem, akkor milyen hardver, szoftver és/vagy förmver beszerzésére lenne szükség.

ASE_INT.1.7C A TOE leírásnak le kell írnia a TOE fizikai hatókörét.

ASE_INT.1-9 Az értékelőnek meg kell vizsgálnia a TOE leírást annak megállapítása érdekében, hogy az leírja-e a TOE fizikai hatókörét.

Az értékelő állapítsa meg, hogy a TOE leírás felsorolja-e a TOE-t alkotó hardvert, szoftvert, förmvert és útmutatót, valamint olyan részletességgel jellemzi-e ezeket, amely kielégítő ahhoz, hogy az olvasó ezen elemekről általános képet kapjon.

Az értékelő állapítsa meg azt is, hogy nincs lehetséges félreértés a tekintetben, hogy valamely hardver, szoftver, förmver vagy útmutató elem része-e a TOE-nak vagy sem.

ASE_INT.1.8C A TOE leírásnak le kell írnia a TOE logikai hatókörét.

ASE_INT.1-10 Az értékelőnek meg kell vizsgálnia a TOE leírást annak megállapítása érdekében, hogy az leírja-e a TOE logikai hatókörét.

Az értékelő állapítsa meg, hogy a TOE leírás olyan részletességgel tárgyalja-e a TOE által nyújtott logikai biztonsági szolgáltatásokat, amely elegendő ahhoz, hogy az olvasó átfogó képet kapjon ezen szolgáltatásokról.

Az értékelő állapítsa meg továbbá, hogy nincs esetleges félreértés a tekintetben, hogy valamely logikai biztonsági tulajdonságot biztosít-e a TOE vagy sem.

6.2.2.3.2. Az ASE_INT.1.2E értékelői akció

ASE_INT.1.2E Az értékelőnek meg kell erősítenie, hogy a TOE hivatkozás, a TOE áttekintés és a TOE leírás összhangban áll egymással.

ASE_INT.1-11 Az értékelőnek meg kell vizsgálnia a TOE hivatkozást, a TOE áttekintést és a TOE leírást annak megállapítása érdekében, hogy összhangban állnak-e egymással.

6.2.2.4. A megfelelőség nyilatkozatok (ASE_CCL.1) értékelése

Ennek az altevékenységnek a célja a különböző megfelelőségi nyilatkozatok érvényességének a megállapítása. A megfelelőségi nyilatkozatok azt írják le, hogy hogyan felel meg az ST és a TOE a CC-nek, illetve az ST a PP-knek és a csomagoknak.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) az a PP (vagy azok a PP-k), amely(ek)nek való megfelelőséget az ST kinyilvánítja.
c) az a csomag (vagy azok a csomagok), amely(ek)nek való megfelelőséget az ST kinyilvánítja.

6.2.2.4.1. Az ASE_CCL.1.1E értékelői akció

ASE_CCL.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASE_CCL.1.1C A megfelelőségi nyilatkozatnak tartalmaznia kell egy CC megfelelőségi nyilatkozatot, ami azonosítja azt a CC verziót, melyhez az ST és a TOE megfelelőséget állít.

ASE_CCL.1-1 Az értékelőnek ellenőriznie kell, hogy a megfelelőségi nyilatkozat tartalmaz-e egy CC megfelelőségi nyilatkozatot, ami azonosítja azt a CC verziót, melyhez az ST és a TOE megfelelőséget állít.

Az értékelő vizsgálja meg, hogy a CC megfelelőségi nyilatkozat azonosítja-e azt a CC verziót, melyet az adott ST kidolgozásához használtak. Ennek tartalmaznia kell a CC verziószámot, és amennyiben nem a CC nemzetközi angol verzióját használták, akkor az alkalmazott CC verzió nyelvét. (Jelen módszertan alkalmazása esetén a CC verziószáma 3.1, a használható nyelv pedig a magyar.)

ASE_CCL.1.2C A CC megfelelőségi nyilatkozatnak le kell írni az ST megfelelőségét a CC 2.részéhez képest, hogy az megfelel-e a CC 2. részének vagy kiterjeszti azt.

ASE_CCL.1-2 Az értékelőnek ellenőriznie kell, hogy a CC megfelelőségi nyilatkozat állítja-e, hogy az ST megfelel a CC 2. részének vagy kiterjeszti azt.

ASE_CCL.1.3C A CC megfelelőségi nyilatkozatnak le kell írni az ST megfelelőségét a CC 3. részéhez képest, hogy az megfelel-e a CC 3. részének vagy kiterjeszti azt.

ASE_CCL.1-3 Az értékelőnek ellenőriznie kell, hogy a CC megfelelőségi nyilatkozat állítja-e, hogy az ST megfelel a CC 3. részének vagy kiterjeszti azt.

Jelen értékelési módszertan az alap, fokozott és kiemelt garanciaszinteken kívül nem engedi más garanciacsomagok használatát. Mindhárom garanciaszint megfelel a CC 3. résznek, ezért egy biztonsági előirányzatban kizárólag CC 3. rész megfelelést lehet állítani (kiterjesztett CC 3. rész megfelelést nem).

ASE_CCL.1.4C A CC megfelelőségi nyilatkozatnak összhangban kell lennie a kiterjesztett összetevők meghatározásával.

ASE_CCL.1-4 Az értékelőnek meg kell vizsgálnia a CC 2. részére vonatkozó CC megfelelőségi nyilatkozatot annak megállapítása érdekében, hogy az összhangban áll-e a kiterjesztett összetevők meghatározásával.

Amennyiben a CC megfelelőségi nyilatkozat CC 2. rész megfelelést állít, az értékelő állapítsa meg, hogy a kiterjesztett összetevők meghatározása nem határoz meg funkcionális összetevőt. Amennyiben a CC megfelelőségi nyilatkozat kiterjesztett CC 2. rész megfelelést állít, akkor az értékelő állapítsa meg, hogy a kiterjesztett összetevők meghatározása meghatároz legalább egy kiterjesztett funkcionális összetevőt.

ASE_CCL.1-5 Az értékelőnek meg kell vizsgálnia a CC 3. részére vonatkozó CC megfelelőségi nyilatkozatot annak megállapítása érdekében, hogy az összhangban áll-e a kiterjesztett összetevők meghatározásával.

Amennyiben a CC megfelelőségi nyilatkozat CC 3. rész megfelelést állít, az értékelő állapítsa meg, hogy a kiterjesztett összetevők meghatározása nem határoz meg garanciális összetevőt. Ha a CC megfelelőségi nyilatkozat kiterjesztett CC 3. rész megfelelést állít, akkor az értékelő állapítsa meg,, hogy a kiterjesztett összetevők meghatározása meghatároz legalább egy kiterjesztett garanciális összetevőt.

Jelen értékelési módszertan az alap, fokozott és kiemelt garanciaszinteken kívül nem engedi más garanciacsomagok használatát. Mindhárom garanciaszint megfelel a CC 3. résznek, ezért ebben a munkaszakaszban kizárólag CC 3. rész megfelelést lehet állítani (kiterjesztett CC 3. rész megfelelést nem).

ASE_CCL.1.5C A megfelelőségi nyilatkozatnak azonosítania kell minden PP-t és biztonsági követelmény csomagot, melyhez az ST megfelelőséget vállal.

ASE_CCL.1-6 Az értékelőnek ellenőriznie kell, hogy a CC megfelelőségi nyilatkozat tartalmaz-e egy PP nyilatkozatot, mely azonosítja az összes olyan PP-t, melyhez az ST megfelelőséget vállal.

Ha az ST nem állít PP megfelelőséget, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy mindennemű hivatkozás valamely PP-re egyértelműen azonosított (például cím és verziószám, vagy a PP bevezetésében szereplő azonosítók által).

ASE_CCL.1-7 Az értékelőnek ellenőriznie kell, hogy a CC megfelelőségi nyilatkozat tartalmaz-e egy csomag nyilatkozatot, mely azonosítja az összes olyan csomagot, melyhez az ST megfelelőséget vállal.

Amennyiben az ST nem állít megfelelőséget egy csomaghoz, ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy bármely hivatkozott csomagot egyértelműen azonosítottak (például cím és verziószám, vagy a csomag bevezetésében szereplő azonosítók által).
Az értékelő nem hagyhatja figyelmen kívül azt, hogy csomagnak való részleges megfelelés nem megengedett.

ASE_CCL.1.6C A megfelelőségi nyilatkozatnak le kell írnia az ST minden csomagra vonatkozó megfelelésére, hogy megfelel-e a csomagnak, vagy szigorítja azt.

ASE_CCL.1-8 Az értékelőnek ellenőriznie kell, hogy minden azonosított csomagra a megfelelőségi nyilatkozat tartalmaz-e csomag-név megfelelést vagy csomag-név szigorítást.

Amennyiben az ST nem állít megfelelőséget egy csomaghoz, ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Ha a csomag megfelelőségi nyilatkozat csomag-név megfelelést tartalmaz, akkor az értékelő vizsgálja meg, hogy:

a) amennyiben a csomag garanciacsomag, akkor az ST tartalmazza-e az összes SAR-t a csomagból, de azon kívül más SAR-t nem;
b) amennyiben a csomag funkcionális csomag, akkor az ST tartalmazza-e az összes SFR-t a csomagból, de azon kívül más SFR-t nem.

Jelen értékelési módszertan az alap, fokozott és kiemelt garanciaszinteken kívül nem engedi más garanciacsomagok használatát.

Ha a csomag megfelelőségi nyilatkozat csomag-név szigorítást tartalmaz, akkor az értékelő vizsgálja meg, hogy:

a) amennyiben a csomag garanciacsomag, akkor az ST tartalmazza-e az összes SAR-t a csomagból, és azon felül legalább egy további SAR-t, vagy legalább egy SAR-t, ami hierarchikus a csomagban szereplő valamely SAR-hez képest;
b) amennyiben a csomag funkcionális csomag, akkor az ST tartalmazza-e az összes SFR-t a csomagból, és azon felül legalább egy további SFR-t, vagy legalább egy SFR-t, ami hierarchikus a csomagban szereplő valamely SFR-hez képest.

Jelen értékelési módszertan az alap, fokozott és kiemelt garanciaszinteken kívül nem engedi más garanciacsomagok használatát.

ASE_CCL.1.7C A megfelelőségi nyilatkozat indoklásának meg kell mutatnia, hogy a TOE típus összhangban van azon PP-k TOE típusával, melyekhez megfelelést állít.

ASE_CCL.1-9 Az értékelőnek meg kell vizsgálnia a megfelelőségi nyilatkozat indoklását annak megállapítása érdekében, hogy a TOE TOE típusa összhangban áll-e valamennyi érintett PP TOE típusával.

Amennyiben az ST nem állít megfelelőséget egy PP-hez, ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

A típusok közötti kapcsolat lehet egyszerű: egy tűzfal ST tűzfal PP-nek való megfelelést állít, de lehet bonyolultabb is: egy intelligens kártya ST több PP-nek való megfelelést állít egyidejűleg (PP az integrált áramkörhöz, PP a kártya OS-hez, és két PP az intelligens kártyán lévő két alkalmazáshoz).

ASE_CCL.1.8C A megfelelőségi nyilatkozat indoklásának meg kell mutatnia, hogy a biztonsági probléma meghatározás állításai összhangban vannak azon PP-k biztonsági probléma meghatározásával, melyekhez az ST megfelelést állít.

ASE_CCL.1-10 Az értékelőnek meg kell vizsgálnia a megfelelőségi nyilatkozat indoklását annak megállapítása érdekében, hogy az bemutatja-e a biztonsági probléma meghatározás állításainak összhangját azon PP-k biztonsági probléma meghatározásával, melyekhez az ST megfelelést állít.

Amennyiben az ST nem állít megfelelőséget egy PP-hez, ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Amennyiben a PP nem tartalmaz biztonsági probléma meghatározást, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Amennyiben az a PP, amely a megfelelőségi nyilatkozat alapja, szigorú megfelelést vár el, akkor nincs szükség megfelelőségi nyilatkozat indoklásra. Ehelyett az értékelőnek meg kell határoznia, hogy:

a) az ST-ben szereplő fenyegetések bővebb halmazát alkotják-e a megfelelés alapjául szolgáló PP-ben szereplő fenyegetéseknek vagy megegyeznek azokkal;
b) az ST-ben szereplő szervezeti biztonsági szabályzatok bővebb halmazát alkotják-e a megfelelés alapjául szolgáló PP-ben szereplők szervezeti biztonsági szabályzatoknak vagy megegyeznek azokkal;
c) az ST-ben szereplő feltételezések megegyeznek a megfelelés alapjául szolgáló PP-ben lévő feltételezésekkel.

Amennyiben a PP kimutatható megfelelést követel meg, az értékelő vizsgálja meg a megfelelőségi nyilatkozat indoklását annak meghatározása érdekében, hogy az indoklás kimutatja-e azt, hogy a biztonsági probléma meghatározás nyilatkozat az ST-ben „megegyező vagy szigorúbb” a megfelelőség alapjául szolgáló PP-ben szereplő biztonsági probléma meghatározással összehasonlítva.

A „megegyező vagy szigorúbb” kifejezés jelentésére útmutató található a 7.1.3. mellékletben.
ASE_CCL.1.9C A megfelelőségi nyilatkozat indoklásának meg kell mutatnia, hogy a biztonsági célok állításai összhangban vannak azon PP-k biztonsági céljaival, melyekhez az ST megfelelést állít.

ASE_CCL.1-11 Az értékelőnek meg kell vizsgálnia a megfelelőségi nyilatkozat indoklását annak megállapítása érdekében, hogy a biztonsági célok állításai összhangban vannak azon PP-k biztonsági céljaival, melyekhez az ST megfelelést állít.
Amennyiben az ST nem állít PP megfelelőséget, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekintendő.

Amennyiben a PP szigorú megfelelőséget követel meg, nincs szükség megfelelőségi nyilatkozat indoklásra. Ehelyett az értékelő állapítsa meg, hogy:

a) Az ST tartalmazza a megfelelés alapjául szolgáló PP összes TOE-ra vonatkozó biztonsági célját. Megjegyzés: megengedett, hogy az értékelés alatt álló ST további biztonsági célokat tartalmazzon a TOE-ra;
b) Az ST pontosan tartalmazza az összes üzemeltetési környezetre vonatkozó biztonsági célt (a következő pontban részletezett kivételtől eltekintve). Megjegyzés: megengedett, hogy az értékelés alatt álló ST további biztonsági célokat tartalmazzon az üzemeltetési környezetre;
c) Az ST megszabhatja, hogy a megfelelés alapjául szolgáló PP üzemeltetési környezetre vonatkozó bizonyos biztonsági céljai az ST-ben TOE-ra vonatkozó biztonsági célok legyenek. Ez egy érvényes kivétel az előző pontban foglaltakhoz képest.

Amennyiben a PP kimutatható megfelelőséget követel meg, az értékelő vizsgálja meg a megfelelőségi nyilatkozat indoklását annak megállapítása érdekében, hogy az ST biztonsági célokról szóló nyilatkozata „megegyező vagy szigorúbb” a megfelelés alapját adó PP-ben szereplő biztonsági célok nyilatkozatával összehasonlítva.

A „megegyező vagy szigorúbb” kifejezés jelentésére útmutató található a 7.1.3. mellékletben.
ASE_CCL.1.10C A megfelelőségi nyilatkozat indoklásának meg kell mutatnia, hogy a biztonsági követelmények összhangban vannak azon PP-k biztonsági követelményeivel, melyekhez az ST megfelelést állít.

ASE_CCL.1-12 Az értékelőnek meg kell vizsgálnia a megfelelőségi nyilatkozat indoklását annak megállapítása érdekében, hogy a biztonsági követelmények összhangban vannak-e azon PP-k biztonsági követelményeivel, melyekhez az ST megfelelést állít.
Amennyiben az ST nem állít PP megfelelőséget, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekintendő.

Amennyiben a PP szigorú megfelelést vár el, akkor nincs szükség megfelelőségi nyilatkozat indoklására. Ehelyett, az értékelő állapítsa meg, hogy az ST-ben szereplő biztonsági követelmények bővebb halmazát alkotják-e a megfelelőség alapját adó PP biztonsági követelményeinek vagy megegyeznek azokkal (szigorú megfeleléshez).

Amennyiben kimutatható megfelelést követel meg a PP, az értékelő vizsgálja meg a megfelelőségi nyilatkozat indoklását annak megállapítása érdekében, hogy az megmutatja-e, hogy az ST-ben szereplő biztonsági követelményekről szóló nyilatkozata „megegyező vagy szigorúbb” a megfelelés alapjául szolgáló PP-ben lévő biztonsági követelményekkel összehasonlítva.

A „megegyező vagy szigorúbb” kifejezés jelentésére útmutató található a 7.1.3. mellékletben.

6.2.2.5. A biztonsági probléma meghatározás (ASE_SPD.1) értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a TOE-ra és üzemeltetési környezetére vonatkozó biztonsági problémát világosan meghatározták.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST.

6.2.2.5.1. Az ASE_SPD.1.1E értékelői akció

ASE_SPD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASE_SPD.1.1C A biztonsági probléma meghatározásnak le kell írnia a fenyegetéseket.

ASE_SPD.1-1 Az értékelőnek ellenőriznie kell, hogy a biztonsági probléma meghatározás leírja-e a fenyegetéseket.

Amennyiben minden biztonsági cél csupán a feltételezésekből és a szervezeti biztonsági szabályokból levezethető, akkor a fenyegetésekről szóló nyilatkozatnak nem kell szerepelnie az ST-ben. Ekkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekintendő.

Az értékelő állapítsa meg, hogy a biztonsági probléma meghatározás leírja-e a TOE és/vagy üzemeltetési környezete által kivédendő fenyegetéseket.

ASE_SPD.1.2C Minden fenyegetést le kell írni a támadó, a támadás tárgyát képező vagyon és a támadó tevékenység szerint.

ASE_SPD.1-2 Az értékelőnek meg kell vizsgálnia a biztonsági probléma meghatározást, hogy az leírja-e a fenyegetéseket a támadó, a támadás tárgyát képező vagyon és a támadó tevékenység szerint.

Amennyiben minden biztonsági cél csupán a feltételezésekből és a szervezeti biztonsági szabályokból levezethető, akkor a fenyegetésekről szóló nyilatkozatnak nem kell szerepelnie az ST-ben. Ekkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekintendő.

A támadók tovább jellemezhetők a szakértelem, az erőforrás, a lehetőség és a motiváció alapján.

ASE_SPD.1.3C A biztonsági probléma meghatározásnak le kell írnia a szervezeti biztonsági szabályokat.

ASE_SPD.1-3 Az értékelőnek ellenőriznie kell, hogy a biztonsági probléma meghatározás leírja-e a szervezeti biztonsági szabályokat.

Amennyiben minden biztonsági cél csupán a feltételezésekből és a fenyegetésekből levezethető, akkor a szervezeti biztonsági szabályoknak nem kell szerepelnie az ST-ben. Ekkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekintendő.

Az értékelő állapítsa meg, hogy a szervezeti biztonsági szabályokra vonatkozó nyilatkozatok a TOE és/vagy annak üzemeltetési környezete által követendő szabályok vagy útmutatók szerint fogalmazták-e meg.

Az értékelő állapítsa meg, hogy minden szervezeti biztonsági szabályt megfelelő részletességgel megmagyaráztak és/vagy értelmeztek ahhoz, hogy érthetőek legyenek. A szabályok világos leírása szükséges ahhoz, hogy a biztonsági célokat vissza lehessen vezetni rájuk.

ASE_SPD.1.4C A biztonsági probléma meghatározásnak le kell írnia a TOE üzemeltetési környezetére vonatkozó feltételezéseket.

ASE_SPD.1-4 Az értékelőnek meg kell vizsgálnia a biztonsági probléma meghatározást annak megállapítása érdekében, hogy az leírja-e a TOE üzemeltetési környezetére vonatkozó feltételezéseket.

Amennyiben nincsenek feltételezések, ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekintendő.

Az értékelő állapítsa meg, hogy a TOE üzemeltetési környezetére vonatkozó minden feltételezést kellő részletességgel megmagyaráztak ahhoz, hogy a vásárlók ebből meg tudják állapítani, vajon az ő üzemeltetési környezetük megfelel-e a feltételezésnek. Amennyiben a feltételezések nem eléggé világosak, akkor a vásárlók olyan üzemeltetési környezetben is alkalmazhatják a TOE-t, amelyben az nem biztonságos módon működik.

6.2.2.6. A biztonsági célok (ASE_OBJ.2) értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a biztonsági célok teljes mértékben és megfelelő módon fedik-e le a biztonsági probléma meghatározást, valamint hogy világosan meghatározták ezen probléma TOE és üzemeltetési környezet közötti megosztását.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST.

6.2.2.6.1. Az ASE_OBJ.2.1E értékelői akció

ASE_OBJ.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASE_OBJ.2.1C A biztonsági célokról szóló nyilatkozatnak le kell írnia a TOE-ra vonatkozó biztonsági célokat, valamint az üzemeltetési környezetre vonatkozó biztonsági célokat.

ASE_OBJ.2-1 Az értékelőnek ellenőriznie kell, hogy a biztonsági célokról szóló nyilatkozat megadja-e a TOE-ra, valamint az üzemeltetési környezetre vonatkozó biztonsági célokat.

Az értékelő ellenőrizze, hogy a biztonsági célok mindkét kategóriáját egyértelműen azonosították-e, illetve hogy megkülönböztették-e ezeket egymástól.

ASE_OBJ.2.2C A biztonsági célok indoklásának minden TOE-ra vonatkozó biztonsági célt vissza kell vezetnie az adott biztonsági cél által kivédett fenyegetésekre, valamint az adott biztonsági cél által érvényre juttatott szervezeti biztonsági szabályzatokra.

ASE_OBJ.2-2 Az értékelőnek ellenőriznie kell, hogy a biztonsági célok indoklása minden TOE-ra vonatkozó biztonsági célt visszavezet-e a biztonsági célok által kivédett fenyegetésekre, valamint a biztonsági célok által érvényre juttatott szervezeti biztonsági szabályzatokra.

Minden TOE-ra vonatkozó biztonsági cél visszavezethető a fenyegetésekre, a szervezeti biztonsági szabályokra vagy ezek kombinációjára, de legalább egy fenyegetésre vagy szervezeti biztonsági szabályra való visszavezetés kötelező.

A visszavezethetőség sikertelensége egyaránt jelezheti a biztonsági célok indoklásának hiányosságát, a biztonsági probléma meghatározás hiányosságát, vagy azt, hogy egy TOE-re vonatkozó biztonsági célnak nincs valódi rendeltetése.

ASE_OBJ.2.3C A biztonsági célok indoklásának minden üzemeltetési környezetre vonatkozó biztonsági célt vissza kell vezetnie az adott biztonsági cél által kivédett fenyegetésekre, az adott biztonsági cél által érvényre juttatott szervezeti biztonsági szabályzatokra, valamint az adott biztonsági cél által támasztott feltételezésekre.

ASE_OBJ.2-3 Az értékelőnek ellenőriznie kell, hogy a biztonsági célok indoklása minden üzemeltetési környezetre vonatkozó biztonsági célt visszavezet-e az adott biztonsági cél által kivédett fenyegetésekre, az adott biztonsági cél által érvényre juttatott szervezeti biztonsági szabályzatokra, valamint az adott biztonsági cél által támasztott feltételezésekre.

Minden üzemeltetési környezetre vonatkozó biztonsági cél visszavezethető a fenyegetésekre, a szervezeti biztonsági szabályokra, a feltételezésekre, vagy ezek valamely kombinációjára, de legalább egy fenyegetésre, szervezeti biztonsági szabályra vagy feltételezésre való visszavezetés kötelező.

A visszavezethetőség sikertelensége egyaránt jelezheti a biztonsági célok indoklásának hiányosságát, a biztonsági probléma meghatározás hiányosságát, vagy azt, hogy egy üzemeltetési környezetre vonatkozó biztonsági célnak nincs valódi rendeltetése.

ASE_OBJ.2.4C A biztonsági célok indokolásának szemléltetnie kell, hogy a biztonsági célok lefednek minden fenyegetést.

ASE_OBJ.2-4 Az értékelőnek meg kell vizsgálnia a biztonsági célok indoklását annak megállapítása érdekében, hogy minden egyes fenyegetésre tartalmaz-e megfelelő igazolást arra nézve, hogy a biztonsági célok alkalmasak az adott fenyegetés elhárítására.
Amennyiben nincs fenyegetésre visszavezethető biztonsági cél, e munkaegység „Nem felelt meg" eredményt ad.

Az értékelő állapítsa meg, hogy egy fenyegetésre vonatkozó indoklás megmutatja-e azt, hogy a fenyegetést elhárították, csökkentették, vagy következményeit csillapították.

Az értékelő állapítsa meg, hogy egy fenyegetésre vonatkozó indoklás szemlélteti-e a biztonsági célok elégségességét: ha egy fenyegetésre visszavezetett összes biztonsági cél teljesül, akkor az adott fenyegetést elhárították, elfogadható szintre csökkentették, vagy a fenyegetés következményeit kielégítő módon csillapították.

Megjegyzendő, hogy a biztonsági célok visszavezetése a fenyegetésekre (a biztonsági célok indoklásában) része lehet az igazolásnak, de önmagában nem képez igazolást. Még abban az esetben is szükség van igazolásra, amikor egy biztonsági cél csupán azt mondja ki, hogy egy adott fenyegetés bekövetkezését kívánja megakadályozni, de ekkor az igazolás olyan rövid lehet, mint „az X biztonsági cél közvetlenül kivédi az Y fenyegetést".

Az értékelő azt is állapítsa meg, hogy egy fenyegetésre visszavezetett összes biztonsági cél szükséges: ha a biztonsági cél teljesül, akkor az ténylegesen hozzájárul az adott fenyegetés elhárításához, csökkentéséhez vagy a következmények csillapításához.

ASE_OBJ.2.5C A biztonsági célok indokolásának szemléltetnie kell, hogy a biztonsági célok érvényre juttatják az összes szervezeti biztonsági szabályzatot.

ASE_OBJ.2-5 Az értékelőnek meg kell vizsgálnia a biztonsági célok indoklását annak megállapítása érdekében, hogy minden szervezeti biztonsági szabályra tartalmaz-e megfelelő igazolást arra, hogy a biztonsági célok alkalmasak az adott szervezeti biztonsági szabály érvényre juttatására.

Amennyiben nincsenek a szervezeti biztonsági szabályokra visszavezethető biztonsági célok, e munkaegység „Nem felelt meg" eredményt ad.

Az értékelő állapítsa meg, hogy egy szervezeti biztonsági szabályra vonatkozó indoklás szemlélteti-e a biztonsági célok elégségességét: ha egy adott szervezeti biztonsági szabályra visszavezetett összes biztonsági cél teljesül, akkor az adott szervezeti biztonsági szabály érvényre jut.

Az értékelő azt is állapítsa meg, hogy egy szervezeti biztonsági szabályra vonatkozó összes biztonsági cél szükséges: ha a biztonsági cél teljesül, akkor az ténylegesen hozzájárul az adott szervezeti biztonsági szabály érvényre juttatásához.

Megjegyzendő, hogy a biztonsági célok visszavezetése a szervezeti biztonsági szabályokra (a biztonsági célok indoklásában) része lehet az igazolásnak, de önmagában nem képez igazolást. Még abban az esetben is szükség van igazolásra, amikor egy biztonsági cél csupán azt mondja ki, hogy egy adott szervezeti biztonsági szabály érvényre jutását kívánja elérni, de

ekkor az igazolás olyan rövid lehet, mint „az X biztonsági cél közvetlenül érvényre juttatja az Y szervezeti biztonsági szabályt”.

ASE_OBJ.2.6C A biztonsági célok indokolásának szemléltetnie kell, hogy az üzemeltetési környezetre vonatkozó biztonsági célok az összes feltételezést igénylik.

ASE_OBJ.2-6 Az értékelőnek meg kell vizsgálnia a biztonsági célok indoklását annak megállapítása érdekében, hogy minden üzemeltetési környezetre vonatkozó feltételezésre tartalmaz-e megfelelő igazolást arra, hogy az üzemeltetési környezetre vonatkozó biztonsági célok alkalmasak az adott feltételezés alátámasztására.

Amennyiben nincsenek a feltételezésre visszavezethető, üzemeltetési környezetre vonatkozó biztonsági célok, e munkaegység „Nem felelt meg” eredményt ad.

Az értékelő állapítsa meg, hogy egy a TOE üzemeltetési környezetével kapcsolatos feltételezésre vonatkozó indoklás szemlélteti-e a biztonsági célok elégségességét: ha egy adott feltételezésre visszavezetett összes üzemeltetési környezetre vonatkozó biztonsági cél teljesül, akkor az üzemeltetési környezet alátámasztja az adott feltételezést.

Az értékelő azt is állapítsa meg, hogy egy feltételezésre visszavezetett, a TOE üzemeltetési környezetére vonatkozó összes biztonsági cél szükséges: ha a biztonsági cél teljesül, akkor az ténylegesen hozzájárul ahhoz, hogy az üzemeltetési környezet az adott feltételezést alátámassza.

Megjegyzendő, hogy az üzemeltetési környezetre vonatkozó biztonsági célok visszavezetése a feltételezésekre (a biztonsági célok indoklásában) része lehet az igazolásnak, de önmagában nem képez igazolást. Még abban az esetben is szükség van igazolásra, amikor egy üzemeltetési környezetre vonatkozó biztonsági cél csupán megismétlése egy feltételezésnek, de ekkor az igazolás olyan rövid lehet, mint „az X biztonsági cél közvetlenül alátámasztja az Y feltételezést”.

6.2.2.7. A kiterjesztett összetevő meghatározás (ASE_ECD.1) értékelése

Ezen altevékenység célja annak megállapítása, hogy a kiterjesztett összetevőket egyértelműen és világosan meghatározták, valamint szükség van rájuk, azaz nem fejezhetők ki érthetően a meglévő CC 2. rész vagy CC 3. rész összetevőivel.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST.

6.2.2.7.1. Az ASE_ECD.1.1E értékelői akció

ASE_ECD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASE_ECD.1.1C A biztonsági követelményekről szóló nyilatkozatnak azonosítania kell minden kiterjesztett biztonsági követelményt.

ASE_ECD.1-1 Az értékelőnek ellenőriznie kell, hogy a biztonsági követelményekről szóló nyilatkozatában szereplő összes olyan biztonsági követelmény, amelyet nem kiterjesztett biztonsági követelményként azonosítottak, szerepel a CC 2. vagy 3. részében.

ASE_ECD.1.2C A kiterjesztett összetevők meghatározásának minden kiterjesztett biztonsági követelményre meg kell határoznia egy kiterjesztett összetevőt.

ASE_ECD.1-2 Az értékelőnek ellenőriznie kell, hogy a kiterjesztett összetevők meghatározása minden kiterjesztett biztonsági követelményre meghatároz egy kiterjesztett összetevőt.

Amennyiben az ST nem tartalmaz kiterjesztett biztonsági követelményt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Egyetlen kiterjesztett összetevő használható egy kiterjesztett biztonsági követelmény több ismétlésének meghatározásához, nem szükséges megismételni ezt a meghatározást minden ismétlésre.

ASE_ECD.1.3C A kiterjesztett összetevők meghatározásának le kell írnia, hogy az egyes kiterjesztett összetevők hogyan kapcsolódnak a meglévő CC összetevőkhöz, családokhoz és osztályokhoz.

ASE_ECD.1-3 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy az leírja, hogy az egyes kiterjesztett összetevők hogyan kapcsolódnak a meglévő CC összetevőkhöz, családokhoz és osztályokhoz.

Amennyiben az ST nem tartalmaz kiterjesztett biztonsági követelményt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy a kiterjesztett összetevő:

a) a CC 2. rész meglévő családjának tagja, vagy
b) az ST-ben meghatározott új család tagja.

Amennyiben a kiterjesztett összetevő egy CC 2. részbeli meglévő család tagja, akkor az értékelő állapítsa meg, hogy a kiterjesztett összetevő meghatározása megfelelően leírja-e, hogy a kiterjesztett összetevő miért tagja a szóban forgó családnak, és hogyan kapcsolódik a család más összetevőihez.

Ha a kiterjesztett összetevő az ST-ben megadott új család tagja, akkor az értékelő győződjön meg arról, hogy a kiterjesztett összetevő nem illeszkedik egy meglévő családba sem.

Ha az ST új családot határoz meg, az értékelő állapítsa meg, hogy minden új család:

a) a CC 2. részbeli meglévő osztály tagja, vagy
b) az ST-ben meghatározott új osztály tagja.

Amennyiben a család egy CC 2. részbeli meglévő osztály tagja, akkor az értékelő állapítsa meg, hogy a kiterjesztett összetevő meghatározása megfelelően leírja-e, hogy a család miért tagja a szóban forgó osztálynak, és hogyan kapcsolódik az osztály más családjaihoz.

Ha a család az ST-ben megadott új osztály tagja, akkor az értékelő győződjön meg arról, hogy a család nem illeszkedik egy meglévő osztályba sem.

ASE_ECD.1-4 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy az minden kiterjesztett összetevőre azonosítja-e ezen összetevő minden alkalmazandó függését.

Amennyiben az ST nem tartalmaz kiterjesztett biztonsági követelményt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő ellenőrizze, hogy az ST szerzője nem hagyott ki alkalmazandó függést.

ASE_ECD.1.4C A kiterjesztett összetevők meghatározásának a meglévő CC funkcionális összetevőket, családokat, osztályokat és módszertant kell használnia megjelenítési modellként.

ASE_ECD.1-5 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden kiterjesztett funkcionális összetevő a CC 2. rész összetevőit megjelenítési modellként használja.

Ha az ST nem tartalmaz kiterjesztett SFR-t, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy a kiterjesztett funkcionális összetevő összhangban van-e a CC 2. rész 7.2.3 szakasz (Összetevő felépítés) alatt írtakkal.

Amennyiben a kiterjesztett funkcionális összetevőben műveleteket alkalmaztak, az értékelő állapítsa meg, hogy a kiterjesztett funkcionális összetevő összhangban van-e a 7.1.2 (CC műveletek) pontjával.

Amennyiben a kiterjesztett funkcionális összetevő hierarchia szerint alárendelt egy meglévő funkcionális összetevőnek, akkor az értékelő állapítsa meg, hogy a kiterjesztett funkcionális összetevő összhangban van-e a CC 2. rész 7.3.1 (Összetevő módosítások kiemelése) szakaszban írtakkal.

ASE_ECD.1-6 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden új funkcionális család a CC meglévő családjait megjelenítési modellként használja.

Ha az ST nem határoz meg új funkcionális családot, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy az összes meghatározott új funkcionális család megfelel-e a CC 2. rész 7.2.2 (A családok szerkezete) szakaszban foglaltaknak.

ASE_ECD.1-7 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden új funkcionális osztály a CC meglévő osztályait megjelenítési modellként használja.

Ha az ST nem határoz meg új funkcionális osztályt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy az összes meghatározott új funkcionális osztály megfelel-e a CC 2. rész 7.2.1 (Az osztályok szerkezete) szakaszban foglaltaknak.

ASE_ECD.1-8 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden kiterjesztett garanciális összetevő a CC 3. rész összetevőit megjelenítési modellként használja.

Mivel jelen értékelési módszertan nem engedi meg a kiterjesztett SAR használatát, ezért ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

ASE_ECD.1-9 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden kiterjesztett garanciális összetevőhöz biztosítottak alkalmazható módszertant.

Mivel jelen értékelési módszertan nem engedi meg a kiterjesztett SAR használatát, ezért ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

ASE_ECD.1-10 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden új garanciális család a CC meglévő családjait megjelenítési modellként használja.

Mivel jelen értékelési módszertan nem engedi meg a kiterjesztett SAR használatát, ezért ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

ASE_ECD.1-11 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden új garanciális osztály a CC meglévő osztályait megjelenítési modellként használja.

Mivel jelen értékelési módszertan nem engedi meg a kiterjesztett SAR használatát, ezért ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

ASE_ECD.1.5C A kiterjesztett összetevőknek mérhető és objektív elemekből kell állniuk, hogy megfelelőségük vagy nem megfelelőségük kimutatható legyen.

ASE_ECD.1-12 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden kiterjesztett összetevő minden eleme mérhető és olyan objektív értékelési követelményeket állít, amelyeknek való megfelelőség vagy nem megfelelőség kimutatható.

Mivel jelen értékelési módszertan nem engedi meg a kiterjesztett SAR használatát, ezért ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

6.2.2.7.2. Az ASE_ECD.1.2E értékelői akció

ASE_ECD.1.2E Az értékelőnek meg kell erősítenie, hogy nincs olyan kiterjesztett összetevő, amely egyértelműen kifejezhető lenne a meglévő összetevők segítségével.

ASE_ECD.1-13 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy egyetlen kiterjesztett összetevő sem fejezhető ki egyértelműen a meglévő összetevők segítségével.

Amennyiben az ST nem tartalmaz kiterjesztett biztonsági követelményt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelőnek ennek meghatározása során figyelembe kell vennie a CC 2. részében szereplő összetevőket, az ST-ben meghatározott egyéb kiterjesztett összetevőket, ezen összetevők kombinációit és a lehetséges műveleteket.

Az értékelőnek szem előtt kell tartania, hogy e munkaegység szerepe az olyan összetevők szükségtelen duplázásának megakadályozása, amelyek egyértelműen kifejezhetők más összetevők segítségével. Az értékelőnek nem kell végrehajtania az összetevők összes kombinációjának teljes feltárását, ideértve a műveleteket is, hogy mindenféleképpen kifejezze a kiterjesztett összetevőt a meglévőkkel.

6.2.2.8. A biztonsági követelmények (ASE_REQ.2) értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy az SFR-k és SAR-k világosak, egyértelműek, jól meghatározottak, belső ellentmondásoktól mentesek, valamint az SFR-k kielégítik a TOE biztonsági céljait.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST.

6.2.2.8.1. Az ASE_REQ.2.1E értékelői akció

ASE_REQ.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASE_REQ.2.1C A biztonsági követelményekről szóló nyilatkozatnak le kell írnia az SFR-ket és az SAR-eket.

ASE_REQ.2-1 Az értékelőnek ellenőriznie kell, hogy a biztonsági követelményekről szóló nyilatkozat leírja-e az SFR-ket.

Az értékelő állapítsa meg, hogy minden SFR-t azonosítottak az alábbi módszerek valamelyikével:

a) a CC 2. részében lévő egyedi összetevőre való hivatkozás;
b) az ST-ben való megismétlés.

Nem követelmény, hogy minden SFR azonosítása ugyanolyan módszerrel történjen.

ASE_REQ.2-2 Az értékelőnek ellenőriznie kell, hogy a biztonsági követelményekről szóló nyilatkozat leírja-e a SAR-kat.

Az értékelő állapítsa meg, hogy minden SAR-t azonosítottak az alábbi módszerek valamelyikével:

a) a CC 3. részében lévő egyedi összetevőre való hivatkozás;
b) az ST-ben a kiterjesztett összetevők meghatározásában lévő kiterjesztett összetevőre való hivatkozás;
c) olyan PP-ben lévő egyedi összetevőre való hivatkozás, amelyhez az ST megfelelőséget állít;
d) olyan biztonsági követelmény csomagban lévő egyedi összetevőre való hivatkozás, melyhez az ST-megfelelőséget állít;
e) az ST-ben való megismétlés.

Nem követelmény, hogy minden SAR azonosítása ugyanolyan módszerrel történjen.
ASE_REQ.2.2C Az SFR-ekben és SAR-ekben használt minden szubjektumot, objektumot, műveletet, biztonsági tulajdonságot, külső egyedet és egyéb terminológiai egységet meg kell határozni.

ASE_REQ.2-3 Az értékelőnek meg kell vizsgálnia az ST-t annak megállapítása érdekében, hogy az SFR-ekben és SAR-ekben használt minden szubjektumot, objektumot, műveletet, biztonsági tulajdonságot, külső egyedet és egyéb terminológiai egységet meghatároztak.

Az értékelő állapítsa meg, hogy az ST meghatározza az összes:

a) az SFR-ben használt szubjektumot és objektumot (ezek típusait);
b) a szubjektumok, felhasználók, objektumok, információk, munkaszakaszok és/vagy erőforrások biztonsági tulajdonságait (ezek típusait), ezen tulajdonságok lehetséges felvehető értékeit és ezen értékek közötti bármilyen kapcsolatot (pl. a szigorúan titkos „magasabb”, mint a titkos);
c) az SFR-ben használt műveletet (típusait), beleértve ezen műveletek hatásait;
d) az SFR-ben lévő külső entitást (típusait);
e) egyéb terminológiai elemet, melyeket az SFR-ekben és/vagy SAR-ekben bevezettek a műveletek befejezésével, ha ezek az elemek nem nyilvánvalóak, vagy szótári meghatározáson kívüli jelentésben használják azokat.

Ennek a munkaegységnek a célja annak biztosítása, hogy az SFR-ek és SAR-ek jól meghatározottak és nem fordulhat elő félreértés a homályos terminológia bevezetése miatt. E munkaegység nem szélsőséges módszert kíván meg, nem azt követeli az ST írójától, hogy minden szót meghatározzon. A biztonsági követelmény készlet általános közönségéről feltételezés a megalapozott IT, biztonsági és CC ismeret.

A fentiek szervezhetők csoportokba, osztályokba szerepkörökbe, típusokba vagy egyéb könnyen érthető szempontok, tulajdonságok alapján kategorizálhatók.

Az értékelőnek szem előtt kell tartania, hogy ezen listáknak és meghatározásoknak nem kell a biztonsági követelményekről szóló nyilatkozat részét képeznie, hanem különböző szekciókba helyezhetők (részben vagy egészben). Ez különösen akkor célszerű, ha az ST további részében ugyanazokat a szakkifejezéseket használják.

ASE_REQ.2.3C A biztonsági követelményekről szóló nyilatkozatnak azonosítania kell a biztonsági követelményekben szereplő összes műveletet.

ASE_REQ.2-4 Az értékelőnek ellenőriznie kell, hogy a biztonsági követelményekről szóló nyilatkozat azonosítja-e a biztonsági követelményekben szereplő összes műveletet.

Az értékelő állapítsa meg, hogy minden SFR-ben lévő minden műveletet azonosítottak, ahol használtak ilyet. Az azonosítás elérhető tipográfiai megkülönböztetéssel, vagy explicit azonosítással a környező szöveghez képest, vagy bármilyen más megkülönböztető eszközzel.

ASE_REQ.2.4C Minden műveletet helyesen kell végrehajtani.

ASE_REQ.2-5 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy minden értékadás műveletet helyesen hajtottak végre.

A műveletek helyes végrehajtásáról szóló útmutató megtalálható a 7.1 mellékletben (7.1.2 CC műveletek).

ASE_REQ.2-6 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy minden ismétlés műveletet helyesen hajtottak végre.

A műveletek helyes végrehajtásáról szóló útmutató megtalálható a 7.1 mellékletben (7.1.2 CC műveletek).

ASE_REQ.2-7 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy minden kiválasztás műveletet helyesen hajtottak végre.

A műveletek helyes végrehajtásáról szóló útmutató megtalálható a 7.1 mellékletben (7.1.2 CC műveletek).

ASE_REQ.2-8 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy minden pontosítás műveletet helyesen hajtottak végre.

A műveletek helyes végrehajtásáról szóló útmutató megtalálható a 7.1 mellékletben (7.1.2 CC műveletek).

ASE_REQ.2.5C A biztonsági követelmények minden függési viszonyát vagy teljesíteni kell, vagy a biztonsági követelmények indoklásának igazolnia kell a függés nem teljesítését.

ASE_REQ.2-9 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy a biztonsági követelmények minden függési viszonyát vagy teljesítették, vagy a biztonsági követelmények indoklása igazolja a függés nem teljesítését.

Egy függés kielégíthető a vonatkozó (vagy hierarchikusan hozzá tartozó) összetevő beemelésével a biztonsági követelményekről szóló nyilatkozatba. A függések kielégítéséhez használt összetevőnek szükség esetén műveletekkel módosíthatónak kell lennie a függés tényleges kielégítéséhez.

Egy függés nem teljesülésének indoklása során ki kell mutatni, hogy:

a) a függés teljesülésére miért nincs szükség, vagy miért nem jár haszonnal; ekkor nincs szükség további információra, vagy
b) a függést a TOE üzemeltetési környezete teljesíti; ekkor az igazolásnak le kell írnia, hogy az üzemeltetési környezetre vonatkozó biztonsági célok hogyan elégítik ki ezt a függést.

ASE_REQ.2.6C A biztonság követelmények indoklásában vissza kell vezetni minden SFR-t a TOE biztonsági céljaira.

ASE_REQ.2-10 Az értékelőnek ellenőriznie kell, hogy a biztonság követelmények indoklása visszavezet-e minden SFR-t a TOE biztonsági céljaira.

Az értékelő állapítsa meg, hogy minden egyes SFR visszavezethető legalább egy TOE biztonsági célra.

A visszavezetés sikertelensége vagy azt jelenti, hogy a biztonsági követelmények indoklása nem teljes, a TOE biztonsági céljai nem teljesek, vagy az SFR nem tölt be igazi célt.

ASE_REQ.2.7C A biztonsági követelmények indoklásának meg kell mutatnia, hogy az SFR-ek teljesítik a TOE összes biztonsági célját.

ASE_REQ.2-11 Az értékelőnek meg kell vizsgálnia a biztonsági követelmények indoklását annak megállapítása érdekében, hogy a TOE összes biztonsági céljára megmutatták, hogy az SFR-k alkalmasak az adott TOE biztonsági cél teljesítésére.

Amennyiben az SFR-ek nem vezethetők vissza a TOE biztonsági céljaira, az e munkaegységhez kapcsolódó értékelői tevékenység során „nem felelt meg” döntés születik.

Az értékelő állapítsa meg, hogy a TOE biztonsági céljainak indoklása megmutatja-e, hogy az SFR-ek kielégítők: azaz, ha a célra visszavezethető minden SFR-t kielégítenek, akkor a TOE biztonsági cél teljesül.

Az értékelő azt is állapítsa meg, hogy egy TOE biztonsági célra visszavezethető összes SFR szükséges: azaz az SFR teljesülése ténylegesen hozzájárul a biztonsági cél eléréséhez.

Megjegyzés: A biztonsági követelmények indoklásában szereplő, az SFR-ek TOE biztonsági célokra történő visszavezetése része lehet az indoklásnak, de nem alkot önmagában indoklást.

ASE_REQ.2.8C A biztonsági követelmények indoklásának meg kell magyaráznia, hogy miért az adott SAR-t választották.

ASE_REQ.2-12 Az értékelőnek ellenőriznie kell, hogy a biztonság követelmények indoklása megmagyarázza-e, hogy miért az adott SAR-t választották.

Az értékelőnek szem előtt kell tartania, hogy minden magyarázat helyes, ha összefüggő és sem a SAR-ek, sem a magyarázat nem tartalmaz nyilvánvaló ellentmondásokat az ST további részeihez képest.

A SAR-ek és az ST további része közötti nyilvánvaló ellentmondásra példa: magas képességekkel rendelkező fenyegetés forrásról van szó, de a AVA_VAN családból választott SAR nem véd ezen fenyegetés források ellen.

ASE_REQ.2.9C A biztonsági követelményekről szóló nyilatkozatnak belső ellentmondásoktól mentesnek kell lennie.

ASE_REQ.2-13 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy az belső ellentmondásoktól mentes.

Az értékelő állapítsa meg, hogy az összes SFR és SAR kombinációja belső ellentmondásoktól mentes.

Az értékelő állapítsa meg, hogy minden alkalommal, amikor különböző biztonsági követelmények vonatkoznak ugyanazon típusú fejlesztői bizonyítékra, eseményre, műveletre, adatra, végrehajtandó tesztekre stb. vagy “minden objektumra”, “minden szubjektumra”, ezek a követelmények nem mondanak ellent egymásnak.

Néhány lehetséges ellentmondás:

a) FAU_GEN.1 (Napló adatok generálása), ami specifikálja, hogy kinek van joga hozzáférni a napló állományokhoz, és az FPR_UNO.1 (Megfigyelhetetlenség), ami azt specifikálja, hogy a szubjektumok egyes tevékenységeit el kell rejteni más szubjektumok elől. Ha annak a szubjektumnak, aki nem láthat egy tevékenységet, hozzáférése van a naplóhoz, akkor ezek az SFR-ek ellentmondanak egymásnak;
b) FDP_RIP.1 (Részleges maradvány információ védelem) a tovább már nem szükséges információ törlését írja elő, az FDP_ROL.1 (Alapszintű visszagörgetés) azt specifikálja, hogy egy TOE visszaállhat egy előző állapotba. Amennyiben a visszagörgetendő információt az előző állapotban törölték, ez a két követelmény ellentmond egymásnak;
c) Az FDP_ACC.1 (Részleges hozzáférés ellenőrzés) ismétlése, főleg amikor néhány ismétlés ugyanazon szubjektumokra, objektumokra vagy műveletekre vonatkozik. Ha egy hozzáférés ellenőrzési SFR lehetővé teszi egy szubjektumnak, hogy egy objektumon műveletet hajtson végre, miközben egy másik hozzáférés ellenőrzési SFR nem engedi ezt, akkor e követelmények ellentmondanak egymásnak.

6.2.2.9. A TOE összefoglaló előírás (ASE_TSS.2) értékelése

Ezen altevékenység célja annak megállapítása, hogy a TOE összefoglaló előírás foglalkozik-e az összes SFR-rel, a fizikai és a logikai hamisítással, a biztonsági funkciók megkerülésével, valamint összhangban van-e a TOE egyéb leíró részeivel.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST.

6.2.2.9.1. Az ASE_TSS.2.1E értékelői akció

ASE_TSS.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASE_TSS.2.1C A TOE összefoglaló előírásnak le kell írnia, hogy a TOE hogyan teljesíti az egyes SFR-eket.

ASE_TSS.2-1 Az értékelőnek meg kell vizsgálnia a TOE összefoglaló előírást annak megállapítása érdekében, hogy az leírja-e, hogy a TOE hogyan teljesíti az egyes SFR-eket.

Az értékelő állapítsa meg, hogy a TOE összefoglaló előírás a biztonsági követelményekről szóló nyilatkozatban szereplő minden SFR-re megadja annak leírását, hogyan teljesül az SFR.

Az értékelő tartsa szem előtt, hogy az egyes leírások célja a TOE lehetséges felhasználói számára magas szintű áttekintés nyújtása arról, hogy a fejlesztő hogyan szándékozik kielégíteni az SFR-eket, ezért a leírásnak nem kell túlzottan részletesnek lennie.

ASE_TSS.2.2C A TOE összefoglaló előírásnak le kell írnia, hogy a TOE hogyan védi meg magát a fizikai és a logikai hamisítás ellen.

ASE_TSS.2-2 Az értékelőnek meg kell vizsgálnia a TOE összefoglaló előírást annak megállapítása érdekében, hogy az leírja-e, hogy a TOE hogyan védi meg magát a fizikai és a logikai hamisítás ellen.

Az értékelő tartsa szem előtt, hogy az egyes leírások célja a TOE lehetséges felhasználói számára magas szintű áttekintés nyújtása arról, hogy a fejlesztő hogyan szándékozik védekezni a fizikai és a logikai hamisítás ellen, ezért a leírásnak nem kell túlzottan részletesnek lennie.

ASE_TSS.2.3C A TOE összefoglaló előírásnak le kell írnia, hogy a TOE hogyan védi meg magát a megkerülés ellen.

ASE_TSS.2-3 Az értékelőnek meg kell vizsgálnia a TOE összefoglaló előírást annak megállapítása érdekében, hogy az leírja-e, hogy a TOE hogyan védi meg magát a megkerülés ellen.

Az értékelő tartsa szem előtt, hogy az egyes leírások célja a TOE lehetséges felhasználói számára magas szintű áttekintés nyújtása arról, hogy a fejlesztő hogyan szándékozik védelmet biztosítani a megkerülés ellen, ezért a leírásnak nem kell túlzottan részletesnek lennie.

6.2.2.9.2. Az ASE_TSS.2.2E értékelői akció

ASE_TSS.2.2E Az értékelőnek meg kell erősítenie, hogy a TOE összefoglaló előírás összhangban van a TOE áttekintéssel és a TOE leírással, nem mond ellent azoknak.

ASE_TSS.2-4 Az értékelőnek meg kell vizsgálnia a TOE összefoglaló előírást annak megállapítása érdekében, hogy az összhangban áll-e a TOE áttekintéssel és a TOE leírással.

A TOE áttekintés, TOE leírás és TOE összefoglaló előírás leírja a TOE-t elbeszélő formában, a részletezettség növekvő szintjén. Ezért ezen leírásoknak összhangban kell lenniük.

6.2.3. Termék értékelés alap garanciaszinten

6.2.3.1. A Fejlesztés garanciaosztály (ADV) értékelése

A fejlesztési tevékenységnek az a célja, hogy a terv dokumentációt felmérje abból a szempontból, hogy az megfelelő-e annak megértéséhez, hogy a TSF hogyan teljesíti az SFR-eket, és hogy az SFR-ek megvalósítását nem lehet meghamisítani vagy megkerülni. Ezt a megértést a TSF terv dokumentációhoz tartozó egyre részletesebb leírások vizsgálatán keresztül lehet elérni. A terv dokumentáció a funkcionális specifikációból (ami a TSF interfészeit írja le), a TOE tervből (ami a TSF szerkezetét írja le abból a szempontból, hogy az hogyan működik a megkívánt SFR-ekhez kapcsolódó funkciók végrehajtása érdekében) és egy megvalósítási leírásból (forráskód szintű leírás) áll. (Az alap garanciaszint nem tartalmaz megvalósítási leírásra vonatkozó követelményeket.)

Ezenfelül létezik egy biztonsági szerkezet leírás, amely a TSF szerkezeti tulajdonságait ismerteti annak kifejtése céljából, hogy ennek biztonsági szempontú érvényre jutását nem lehet meghamisítani vagy megkerülni.

A terv dokumentációra vonatkozó CC követelmények szintjei aszerint különböznek, hogy mennyi és milyen részletes információt kell biztosítani, milyen mértékű formalizmussal. Az alacsonyabb szinteken a TSF biztonság szempontból legkritikusabb részeit a legnagyobb részletességgel kell ismertetni, míg a biztonság szempontjából kevésbé fontos részeket csak összegezni kell; további garancia nyerhető azáltal, ha növelik a TSF biztonság szempontból legkritikusabb részeire vonatkozó információk mennyiségét, és ha növelik a kevésbé fontos részekre vonatkozó részleteket. A legnagyobb garancia akkor érhető el, ha minden részre vonatkozóan mélyreható részleteket és információkat adnak meg.

A CC a dokumentumok formalizmusának a mértékét (vagyis azt, hogy a dokumentum informális-e vagy félformális) hierarchikusnak tekinti. Informális az a dokumentum, amelyet természetes nyelven fejeztek ki. A CEM nemzetközi módszertan nem ír elő kötelezően használandó meghatározott nyelvet; ez a kérdés a sémára van hagyva. (A MIBÉTS séma a

magyar és az angol nyelvet ismeri el használható természetes nyelvként.) A következő fejezetek a különböző informális dokumentumok tartalmát ismertetik.

Egy funkcionális specifikáció leírást nyújt a TSF-hez kapcsolódó interfészek rendeltetéséről és használati módjáról. Például, ha egy operációs rendszer eszközt biztosít a felhasználó számára az ön-azonosításra, fájlok létrehozására, fájlok módosítására vagy törlésére, olyan engedélyek beállítására, amelyek meghatározzák, hogy mely egyéb felhasználók férhetnek hozzá fájlokhoz, és eszközt biztosít a távoli gépekkel való kommunikációra, akkor az operációs rendszer funkcionális specifikációjának tartalmaznia kell mindezeknek az ismertetését, és azt, hogy ezeket hogyan valósítják meg a TSF-hez csatlakozó kívülről látható interfészeken keresztüli kölcsönhatások. Ha létezik egy naplózási funkcionalitás is, amely észleli és rögzíti az ilyen események előfordulásait, akkor az is elvárás, hogy ez a naplózási funkcionalitás része legyen a funkcionális specifikációnak; és bár ezt a funkcionalitást technikailag nem közvetlenül a felhasználó idézi elő a külső interfészen, biztosan kihat erre az, ami a felhasználói külső interfészen történik.

A terv leírást logikai alkotóelemek (alrendszerek vagy modulok) szerint fejezik ki, amelyek mindegyike egy érthető szolgáltatást vagy funkciót biztosít. Például egy tűzfal állhat olyan alrendszerekből, amelyek csomagszűréssel, távoli adminisztrációval, naplózással és kapcsolat-szintű szűréssel foglalkoznak. A tűzfal terv leírásnak ekkor ismertetnie kell, hogy az egyes alrendszerek milyen tevékenységeket hajtanak végre, amikor egy bejövő csomag megérkezik a tűzfalhoz.

6.2.3.1.1. Biztonsági szerkezet: Az ADV_ARC.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak a megállapítása, hogy a TSF olyan módon van-e megszerkesztve, hogy azt nem lehet meghamisítani vagy megkerülni, és hogy a biztonsági tartományokat biztosító TSF-ek a szóbanforgó tartományokat elkülönítik-e egymástól.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) TOE terv,
d) biztonsági szerkezet leírás,
e) megvalósítás reprezentáció (alap garanciaszinten ez nem kell),
f) üzemeltetési felhasználói útmutató.

Az önvédelem, a tartomány szétválasztás és a nem-megkerülhetőség elveit elkülönítik attól a biztonsági funkcionalitástól, melyet a CC 2. részbeli SFR-ek fejeznek ki, minthogy az önvédelem és nem-megkerülhetőség egyáltalán nem rendelkezik közvetlenül megfigyelhető interfésszel a TSF-en. Ezek inkább olyan tulajdonságai a TSF-nek, amelyeket a TOE és TSF tervezésén keresztül valósítanak meg, és amelyeket a szóbanforgó terv helyes megvalósításával juttatnak érvényre. Ezenfelül ezen tulajdonságok értékelése kevésbé célirányos, mint a mechanizmusok értékelése; egy funkcionalitásnak a hiányát sokkal nehezebb ellenőrizni, mint a meglétét. Annak a megállapítása azonban, hogy ezek a tulajdonságok teljesülnek, éppen olyan kritikus, mint annak a megállapítása, hogy egy mechanizmust helyesen valósítottak meg.

Az általánosan alkalmazott megközelítési mód szerint a fejlesztő biztosítja a fent említett tulajdonságokat teljesítő TSF-et, és bizonyítékot is átad (dokumentáció formájában), amelyet megvizsgálásával belátható, hogy a tulajdonságok valóban teljesülnek. Az értékelő felelőssége, hogy megtekintse a bizonyítékot, a TOE-hoz és TSF-hez átadott egyéb bizonyítékokkal társítva, és megállapítsa, hogy a tulajdonságok megvalósulnak-e. A munkaegységek jellemezhetők úgy, hogy vannak olyanok, amelyek azzal foglalkoznak, hogy milyen információt kell átadni, és vannak olyanok, amelyek az értékelő által végrehajtott tényleges vizsgálatokkal foglalkoznak.

A biztonsági szerkezet leírás ismerteti, hogy a biztonsági tartományokat hogyan definiálták, és a TSF hogyan tartja fenn ezek elkülönülését. Ismerteti, hogy mi gátolja meg a nem-megbízható eljárásokat abban, hogy hozzájussanak a TSF-hez és módosítsák azt. Ismerteti, hogy mi garantálja azt, hogy a TSF ellenőrzése alá tartozó minden erőforrás megfelelő módon védve van, és hogy minden SFR-vonatkozású tevékenységet a TSF közvetít. Megmagyaráz minden szerepet, amit a környezet tölt be ezek valamelyikénél (pl. hogyan történik a biztonsági funkcionalitás aktivizálása, feltételezve, hogy a tevékenységet az alátámasztó környezet helyesen aktivizálja?). Röviden, megmagyarázza, hogy a TOE az elgondolások szerint hogyan fog valamilyen biztonsági szolgáltatást nyújtani.

Az értékelők által végrehajtott vizsgálatokat a TOE-hoz átadott minden fejlesztői bizonyítékkal kapcsolatban olyan részletesen kell elvégezni, ahogyan az adott bizonyítékot szolgáltatták. Az alap garanciaszinten nem elvárás, hogy a TSF önvédelmet teljesen megvizsgálják, minthogy csak magas szintű terv reprezentációk állnak rendelkezésre. Az értékelőnek minden bizonnyal vizsgálatai egyéb részeiből nyert információk felhasználására is szüksége lesz (pl. a TOE terv vizsgálata), amikor a következő munkaegységeknél vizsgálandó tulajdonságok felbecsülését végzi.

6.2.3.1.1.1. Az ADV_ARC.1.1E értékelői akció

ADV_ARC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ADV_ARC.1.1C A biztonsági szerkezet leírást olyan szinten kell részletezni, amely összemérhető a TOE terv dokumentációban ismertetett, SFR-t érvényre juttató absztrakciók leírásával.
ADV_ARC.1-1 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy az ebben biztosított információk részletessége összemérhető-e a TOE terv dokumentációban és a funkcionális specifikációban ismertetett, SFR-t érvényre juttató absztrakciók leírásával.

A funkcionális specifikáció vonatkozásában az értékelő győződjön meg arról, hogy az ismertetett önvédelmi funkcionalitás lefedi-e azokat a hatásokat, amelyek nyilvánvalóak a TSFI-n. Egy ilyen leírás magában foglalhatja a TSF futtatható formáira, illetve az objektumokra (pl. TSF által használt fájlok) elhelyezett védelmet. Az értékelő győződjön meg arról, hogy a TSFI-n keresztül aktivizálható funkcionalitást leírták.

Az értékelő győződjön meg arról, hogy a biztonsági szerkezet leírása tartalmaz-e információt a TSF tartomány elkülönítéshez hozzájáruló egyes alrendszerei működésmódjáról.

Az ehhez a munkaegységhez kapcsolódó értékelői akció kapjon „nem felelt meg” határozatot, ha a biztonsági szerkezet leírás megemlít bármilyen olyan modult, alrendszert vagy interfészt, amelyet a funkcionális specifikáció vagy a TOE terv dokumentum nem ismertet.

ADV_ARC.1.2C A biztonsági szerkezet leírásnak ismertetnie kell a TSF által kezelt biztonsági tartományokat, összhangban az SFR-ekkel.

ADV_ARC.1-2 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy az ismerteti-e a TSF által kezelt biztonsági tartományokat.

A biztonsági tartományok olyan környezetekre vonatkoznak, amelyeket a TSF nyújt potenciálisan kárt-okozó egyedek általi használatra; például, egy tipikus biztonságos operációs rendszer számos erőforrást nyújt olyan eljárások számára, amelyek korlátozott hozzáférési jogokkal és biztonsági tulajdonságokkal rendelkeznek. Az értékelő állapítsa meg, hogy a biztonsági tartományok fejlesztői leírása minden olyan SFR-t figyelembe vesz, amit a TOE megkíván.

Bizonyos TOE-k esetében nem léteznek ilyen tartományok, mivel a felhasználók számára rendelkezésre álló minden kölcsönhatást szigorúan a TSF tartalmaz. Ilyen TOE-ra példa egy csomag-szűrő tűzfal. A LAN-on vagy WAN-on lévő felhasználók nem lépnek kölcsönhatásba a TOE-val, így nincsen szükség biztonsági tartományokra; csak a TSF által kezelt adat-struktúrák szolgálnak arra, hogy a felhasználói csomagokat elkülönítetten tartsák. Az értékelő győződjön meg arról, hogy minden olyan állítás, hogy nincsen biztonsági tartomány, alá van támasztva bizonyítékkal, és győződjön meg arról is, hogy ilyen tartományok valóban nem állnak rendelkezésre.

ADV_ARC.1.3C A biztonsági szerkezet leírásnak ismertetnie kell, hogy a TSF inicializálási eljárása milyen mértékben biztonságos.

ADV_ARC.1-3 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy a TSF inicializálási eljárása megőrzi a biztonságot.

A TSF inicializálására vonatkozó, a biztonsági szerkezet leírásban megadott információ azokra a TOE összetevőkre irányul, amelyek közreműködnek abban, hogy a TSF-et egy kezdeti biztonságos állapotba hozzák (vagyis amikor a TSF-nek már minden része működőképes), bekapcsoláskor vagy reset esetén. A biztonsági szerkezet leírásban ez a fejtegetés sorolja fel azokat a rendszer-inicializálási összetevőket és feldolgozásokat, amelyek érintve vannak a „kikapcsolt” állapotból a kezdeti biztonságos állapotba való átmenet során.

Gyakran fordul elő az az eset, hogy az inicializálási funkciót ellátó összetevők a biztonságos állapot elérése után már nem állnak rendelkezésre; ebben az esetben a biztonsági szerkezet leírás határozza meg ezeket az összetevőket, és magyarázza meg, hogy milyen mértékben igaz az, hogy nem-megbízható egyedek nem tudják elérni ezeket a TSF felállása után. Ebben a vonatkozásban az a tulajdonság, amelyet fenn kell tartani, az, hogy 1) a biztonságos állapot elérése után nem-megbízható egyedek nem férhetnek hozzá ezekhez az összetevőkhöz, vagy

pedig 2) ha ezek az összetevők nyújtanak is interfészeket nem-megbízható egyedek számára, akkor ezek a TSFI-k nem használhatók a TSF működésébe történő hamisításra.

A TSF inicializálásához kapcsolódó TOE összetevők a TSF inicializálását követően a TSF részeként kezelik magukat, és ebből a nézőpontból vizsgálandók. Meg kell jegyezni, hogy még ha ezeket a TSF részeként is kezelik, valószínűleg megindokolható, hogy ezeknek nem kell teljesíteni az ADV_INT belső szerkezeti követelményeket (ahogyan az ADV_INT erre lehetőséget nyújt).

ADV_ARC.1.4C A biztonsági szerkezet leírásnak szemléltetnie kell, hogy a TSF megvédi magát a hamisítással szemben.

ADV_ARC.1-4 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy az kellő információt biztosít annak megállapításához, hogy a TSF képes megvédi magát a nem-megbízható aktív egyedek hamisításával szemben.

Az „önvédelem” a TSF-nek arra a képességére utal, hogy meg tudja védeni saját magát a külső egyedek olyan manipulációival szemben, amelyek a TSF megváltoztatásaihoz vezethetnek. A más IT egyedektől függő TOE-k esetében gyakran előfordul, hogy a TOE olyan szolgáltatást használ fel funkciói végrehajtásához, amelyeket más IT egyedek szolgáltatnak. Az ilyen esetekben a TSF önmagában nem tudja megvédeni saját magát, mivel más IT egyedektől függ az, hogy valamilyen védelmet tud biztosítani. A biztonsági szerkezet leírás szempontjából az önvédelem elve csak azokra a szolgáltatásokra vonatkozik, amelyeket a TSF nyújt a TSFI-ken keresztül, és nem vonatkozik azokra a szolgáltatásokra, amelyeket az általa használt támogató IT egyedek szolgáltatnak.

Az önvédelem általában számos eszközzel elérhető, a TOE-hoz való hozzáférés fizikai és logikai korlátozásától kezdődően a hardver-alapú (pl. memóriakezelési funkcionalitás) és szoftver-alapú (pl. bemenetek korlát-érték ellenőrzései egy megbízható szerveren) eszközökig. Az értékelő állapítsa meg, hogy minden ilyen mechanizmus ismertetve lett.

Az értékelő állapítsa meg, hogy a terv leírás lefedi azt, hogy a TSF hogyan kezeli a felhasználói bemenetet abból a szempontból, hogy az ne ronthassa le a TSF-et. Például a TSF megvalósíthatja a privilégium elvét és megvédheti magát azzal, hogy privilegizált-módban futó rutinokat alkalmaz a felhasználói bemenetek kezelésére. A TSF hasznosíthatja az olyan processzor-alapú elkülönítési mechanizmusokat, mint amilyenek a privilégium szintek vagy gyűrűk. A TSF megvalósíthat olyan szoftver védelmi szerkezeteket vagy kódolási konvenciókat, amelyek hozzájárulnak a szoftver tartományok elkülönítésének megvalósításához, feltehetően azzal, hogy a felhasználói címteret elhatárolják a rendszer címtértől. Ezenfelül a TSF bízhat abban, hogy a környezet biztosít bizonyos védelmet.

A tartomány elválasztási funkciókhoz hozzájáruló összes mechanizmust le kell írni. Az értékelő mindazokat az ismereteket, amelyeket más bizonyítékokból (a TOE-hoz tartozó garanciacsomag tartalmától függően: funkcionális specifikáció, TOE terv, a TSF belső részeinek leírása, a biztonsági szerkezet egyéb részeinek leírása, megvalósítási reprezentáció) szerzett meg, használja fel annak megállapításánál, hogy az önvédelemhez hozzájáruló minden olyan funkcionalitást is ismertettek, amely a biztonsági szerkezet leírásban nem szerepel.

Az önvédelmi mechanizmusok leírásának helyessége az a tulajdonság, hogy a leírás hitelt érdemlően ismerteti, hogy mit valósítottak meg. Az értékelő használjon fel egyéb bizonyítékokat (alap garanciaszinten: funkcionális specifikáció, TOE terv, a biztonsági szerkezet leírás egyéb részei) annak megállapításához, hogy az önvédelmi mechanizmus leírásai ellentmondanak-e egymásnak. Ha a TOE-hoz tartozó garanciacsomag tartalmazza a „Megvalósítási reprezentáció”-t (ADV_IMP), az értékelő mintát fog venni a megvalósítási reprezentációból; ekkor az értékelő győződjön meg a leírások helyességéről a kiválasztott mintára vonatkozóan is. Ha egy értékelő nem látja át, hogy egy meghatározott önvédelmi mechanizmus hogyan működik, vagy hogyan működne a rendszer architektúrában, lehetséges, hogy ez egy olyan eset, amikor a leírás nem helyes.

ADV_ARC.1.5C A biztonsági szerkezet leírásnak szemléltetnie kell, hogy a TSF meggátolja az SFR-t érvényre juttató funkcionalitás megkerülését.

ADV_ARC.1-5 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy az bemutat-e olyan vizsgálatot, ami megfelelő módon ismerteti, hogy az SFR-t érvényre juttató mechanizmusokat milyen mértékben nem lehet megkerülni.

A nem-megkerülhetőség egy olyan tulajdonság, hogy a TSF biztonsági funkcionalitása (ahogyan azt az SFR-ek specifikálják) mindig működésbe lép. Például, ha a fájlokhoz való hozzáférés a TSF-nek az egyik, SFR-en keresztül specifikált tulajdonsága, akkor nem szabad előfordulnia olyan interfésznek, amin keresztül a fájlokhoz hozzá lehet férni a TSF hozzáférés ellenőrzési mechanizmusa aktivizálása nélkül (vagyis nem szabad előfordulnia például olyan interfésznek, amelyen keresztül közvetlenül hozzá lehet férni egy diszkhez).

Annak leírása, hogy a TSF mechanizmusokat miért nem lehet megkerülni, általában módszeres indoklást igényel a TSF-en és a TSFI-ken alapulva. Annak leírása, hogy a TSF hogyan működik (amit a terv lebontási bizonyítékok, vagyis a funkcionális specifikáció és TOE terv dokumentáció tartalmaznak) – a TSS-ben foglalt információ mellett – biztosítja a szükséges hátteret ahhoz, hogy az értékelő megértse, hogy mely erőforrásokat kell védeni, és milyen biztonsági funkciókat kell biztosítani. A funkcionális specifikáció adja meg a TSFI-k ismertetését, amelyeken keresztül az erőforrások/funkciók hozzáférhetők.

Az értékelő becsülje fel az átadott leírásokat (és a fejlesztő által biztosított egyéb információkat, mint például a funkcionális specifikáció), hogy meggyőződjön arról, hogy nem áll rendelkezésre olyan interfész, amelyet a TSF megkerülésére lehetne használni. Ez azt jelenti, hogy az egyes interfészeknek vagy nem szabad kapcsolatban állniuk az ST-ben előírt SFR-ekkel (és nem szabad kölcsönhatásban lenniük semmi olyannal sem, amit felhasználnak az SFR-ek kielégítésére), vagy a más fejlesztői bizonyítékokban leírt biztonsági funkcionalitást az ismertetett módon kell használniuk. Például egy játék valószínűleg nem áll kapcsolatban az SFR-ekkel, így meg kell magyarázni, hogy miért nem befolyásolja a biztonságot. A felhasználói adatokhoz való hozzáférés azonban feltehetően kapcsolatban áll hozzáférés ellenőrzési SFR-ekkel, így a magyarázatnak ismertetnie kell azt, hogy a biztonsági funkcionalitás hogyan működik, amikor az adathozzáférési interfészeken keresztül aktivizálódik. Ilyen leírás szükséges minden elérhető interfészre.

Leírásra példa a következő. Tegyük fel, hogy a TSF fájlvédelmet biztosít. Tegyük fel továbbá, hogy bár a „hagyományos” TSFI megnyitási, olvasási és írási rendszerhívások aktivizálják a TOE tervben ismertetett fájlvédelmi mechanizmusokat, létezik egy TSFI, amely hozzáférést biztosít egy batch job lehetőséghez (batch job-ok létrehozása, job-ok törlése, nem végrehajtott job-ok módosítása). Az értékelőnek a megbízó által biztosított leírásból dönteni kell tudnia arról, hogy a szóbanforgó TSFI ugyanazt a védelmi mechanizmust aktivizálja-e, mint a „hagyományos” interfészek. Ez elérhető például a TOE terv megfelelő részeire való hivatkozással, amely azt tárgyalja, hogy a batch job lehetőséggel rendelkező TSFI hogyan valósítja meg biztonsági céljait.

Ugyanezen példát használva tételezzük fel, hogy létezik egy TSFI, amelynek az egyetlen célja, hogy kijelezze az időpontot. Az értékelő állapítsa meg, hogy a leírás megfelelő módon bizonyítja, hogy ez a TSFI nem képes egyetlen védett erőforrás manipulálására sem, és nem aktivizálhat egyetlen biztonsági funkcionalitást sem.

A megkerülésre egy másik példa az, amikor feltételezik, hogy a TSF megőrzi egy kriptográfiai kulcs bizalmasságát (ami felhasználható kriptográfiai műveletekhez, de amit nem szabad írni és olvasni). Ha egy támadó közvetlenül fizikailag hozzáfér az eszközhöz, képes lehet arra, hogy oldal-csatornákat vizsgáljon -mint például az eszköz áramfelvételét, az eszköz pontos időzítését, vagy az eszköz valamilyen elektromágneses kisugárzását-, és ebből következtessen a kulcsra.

Ha létezhetnek ilyen oldal-csatornák, a szemléltetés vegye tekintetbe azokat a mechanizmusokat, amelyek meggátolják ezeknek az oldal-csatornáknak a bekövetkezését, mint például véletlen belső órák, két-utas technológia stb. A szóbanforgó mechanizmusok ellenőrizhetők a tisztán terv-alapú érvelések és a tesztelések kombinációjával.

Utolsó példáként arra, hogy biztonsági funkcionalitást használnak védett erőforrás helyett, tételezzünk fel egy olyan ST-t, amely tartalmazza az „Az eredet kikényszerített bizonyítása” (FCO_NRO_2) biztonsági követelményt, amely megkívánja, hogy a TSF bizonyítékot nyújtson az ST-ben specifikált információ-típusok eredetére vonatkozóan. Tételezzük fel, hogy az „információ-típusok” magukban foglalnak minden információt, amelyet a TOE felhasználásával küldenek e-mailen keresztül. Ebben az esetben az értékelő vizsgálja meg a leírást, hogy meggyőződjön arról, hogy minden TSFI részletezve van, amely aktivizálható e-mail küldése céljából, és ezek végrehajtják az „Az eredet kikényszerített bizonyítása” funkciót. A leírás utalhat az üzemeltetési felhasználói útmutatóra, hogy minden helyet bemutasson, ahonnan e-mail származhat (pl. levelező program, scriptektől/batch-job-októl származó értesítések), és hogy bemutassa, hogy mindezek a helyek hogyan aktivizálják az eredet előállítása funkciót.

Az értékelő győződjön meg arról is, hogy a leírás átfogó, amelyben minden interfészt megvizsgálnak a megkívánt SFR-ek teljes összessége szerint. Ez megkívánhatja az értékelőtől, hogy vizsgálja meg az alátámasztó információkat (funkcionális specifikáció, TOE terv, a biztonsági szerkezet leírás egyéb részei, az üzemeltetési felhasználói útmutató) annak megállapítása érdekében, hogy a leírás helyesen ragadta-e meg az egyes interfésznek minden vonatkozását. Az értékelő gondolja át, hogy az egyes TSFI-k mely SFR-ekre lehetnek befolyással (a TSFI leírásból és ennek megvalósításából az alátámasztó dokumentációban), és

ezután vizsgálja meg a leírást annak megállapítása érdekében, hogy az lefedi-e a szóbanforgó vonatkozást.

6.2.3.1.2. Funkcionális specifikáció: Az ADV_FSP.2 altevékenység értékelése

Ennek az altevékenységnek a célja annak a megállapítása, hogy a fejlesztő leírta-e a TSFI-t, a rendeltetés, használati mód és a paraméterek szempontjából. Ezen kívül minden SFR-t érvényre juttató TSFI-re az SFR-t érvényre juttató tevékenységeket, eredményeket és hibaüzeneteket is le kell írni.

Az ehhez az altevékenységhez a munkaegységek által megkövetelt értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) TOE terv.

Az ehhez az altevékenységhez felhasznált egyéb értékelési bizonyíték, amennyiben a TOE-ra vonatkozó ST ezt tartalmazza:

a) biztonsági szerkezet leírás,
b) üzemeltetési felhasználói útmutató.

6.2.3.1.2.1. Az ADV_FSP.2.1E értékelői akció

ADV_FSP.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ADV_FSP.2.1C A funkcionális specifikációnak teljes mértékben be kell mutatnia a TSF-et.

ADV_FSP.2-1 Az értékelőnek meg kell vizsgálnia a funkcionális specifikációt annak megállapítása érdekében, hogy az teljes mértékben bemutatja-e a TSF-t.

Ennél az altevékenységnél a TSFI azonosítása szükséges előfeltétel minden egyéb tevékenységhez. A TSFI azonosítása érdekében azonosítani kell a TSF-t (a „TOE terv” (ADV_TDS) munkaegységei részeként). Ez a tevékenység végrehajtható magas szinten, annak biztosításával, hogy az interfészek nagy csoportjai (hálózati protokollok, hardver interfészek, konfigurációs fájlok) nem maradtak ki, vagy alacsony szinten, ahogy a funkcionális specifikáció értékelése előrehalad.

Ezen munkaegység értékelésekor az értékelő állapítsa meg, hogy a TSF minden részét figyelembe vették-e a funkcionális specifikációban felsorolt interfészek szerint. A TSF minden részéhez tartozzon egy interfész leírás, vagy ha a TSF valamely részéhez nem tartozik interfész, az értékelő állapítsa meg, hogy ez elfogadható.

ADV_FSP.2.2C A funkcionális specifikációnak le kell írnia minden TSFI rendeltetését és használati módját.

ADV_FSP.2-2 Az értékelőnek meg kell vizsgálnia a funkcionális specifikációt annak megállapítása érdekében, hogy az meghatározza-e minden TSFI rendeltetését.

Egy TSFI rendeltetése egy olyan általános kijelentés, amely összegzi az interfész által nyújtott funkcionalitást. Az interfészhez kapcsolódó minden tevékenység és eredmény teljes megfogalmazása nem szükséges, de a felhasználót segítenie kell annak általános megértésében, hogy az interfészt mire szánták. Az értékelő ne csak a rendeltetés létezését állapítsa meg, hanem azt is, hogy ez helyesen tükrözi a TSFI-t, figyelembe véve az interfészre vonatkozó egyéb információkat is, mint például a tevékenységek leírása és a hibaüzenetek.

ADV_FSP.2-3 Az értékelőnek meg kell vizsgálnia a funkcionális specifikációt annak megállapítása érdekében, hogy az meghatározza-e minden TSFI használati módját.

Egy TSFI használati módja összegzi, hogy az interfészt hogyan kell kezelni a TSFI-vel kapcsolatos tevékenységek kiváltása és az eredmények megszerzése érdekében. Az értékelő állapítsa meg a funkcionális specifikációban megadott anyagból, hogy hogyan kell használni az interfészt. Ez nem feltétlenül jelenti azt, hogy minden egyes TSFI-hez léteznie kell egy külön használati módnak, például valószínűleg általánosan leírható a kernel-hívások aktivizálási módja, majd megadható minden olyan interfész, ami ezt az általános módszert használja. A különböző típusú interfészek eltérő használási mód meghatározást kívánnak. Az API-k, a hálózati protokoll interfészek, a rendszer konfigurációs paraméterek és hardver busz interfészek mindegyikéhez eltérő használati mód tartozik, és ezt a fejlesztőnek figyelembe kell vennie, amikor a funkcionális specifikációt kialakítja, ahogy az értékelőnek is figyelembe kell vennie, amikor a funkcionális specifikáció értékeli.

Az olyan adminisztrációs interfészek esetében, amelyek funkcionalitását úgy dokumentálták, hogy ahhoz nem-megbízható felhasználó nem férhet hozzá, az értékelőnek meg kell győződnie arról, hogy a funkcionális specifikáció leírja azt a módszert, amellyel a funkciót hozzáférhetetlenné teszik. Meg kell jegyezni, hogy a hozzáférhetetlenséget a fejlesztőnek tesztelnie kell tesztkészletében.

Az értékelőnek nemcsak a használati mód leírások létezését kell megállapítania, hanem azt is, hogy ezek pontosan lefednek minden TSFI-t.

ADV_FSP.2.3C A funkcionális specifikációnak azonosítania kell és le kell írnia minden TSFI-hez kapcsolódó összes paramétert.

ADV_FSP.2-4 Az értékelőnek meg kell vizsgálnia a TSFI bemutatását annak megállapítása érdekében, hogy az teljes mértékben azonosít-e minden TSFI-hez kacsolódó összes paramétert.

Az értékelő vizsgálja át a funkcionális specifikációt, hogy meggyőződjön arról, hogy minden egyes TSFI-hez kapcsolódó összes paramétert leírtak. A paraméterek olyan közvetlen bemenetei vagy kimenetei egy interfésznek, amelyek a szóbanforgó interfész működését irányítják. Például paraméterek az API-knak átadott argumentumok; a különféle mezők egy meghatározott hálózati protokoll csomagjaiban; a Windows Registry-ben lévő egyedi kulcs értékek; egy chip érintkezői közötti jelek; stb.

Annak megállapítása érdekében, hogy minden paraméter megvan-e a TSFI-ben, az értékelő vizsgálja át az interfész leírás további részeit is (tevékenységeket, hibaüzeneteket, stb.), hogy megállapítsa, vajon az interfész leírások figyelembe vették-e a paraméterek leírásait. Az értékelő ellenőrizze az értékeléshez átadott egyéb bizonyítékokat is (pl. TOE terv, biztonsági szerkezet leírás, üzemeltetési felhasználói dokumentáció), hogy észrevegye, ha ezek leírnak egy olyan működést meghatározó vagy kiegészítő paramétert, amit a funkcionális specifikáció nem tartalmaz.

ADV_FSP.2-5 Az értékelőnek meg kell vizsgálnia a TSFI bemutatását annak megállapítása érdekében, hogy az teljesen és pontosan leír-e minden TSFI-hez kacsolódó összes paramétert. Az összes paraméter azonosítása után az értékelőnek meg kell győződnie arról, hogy ezeket helyesen és teljesen írták le. Egy paraméter leírása azt közli valamilyen érthető módon, hogy mi is a paraméter. Például a foo(i) interfész leírható úgy, hogy tartozik hozzá egy „i paraméter, ami egy egész”; ez azonban nem egy elfogadható paraméter leírás. Sokkal inkább elfogadható egy olyan leírás, hogy „az i paraméter egy egész szám, amely jelzi a rendszerbe jelenleg bejelentkezett felhasználók számát”.

Annak megállapítása érdekében, hogy minden paraméter leírása teljes, az értékelő vizsgálja át az interfész leírások további részeit is (rendeltetés, felhasználási mód, tevékenységek, hibaüzenetek, stb.), hogy megállapítsa, vajon az interfész leírások figyelembe vették-e a paraméterek leírásait. Az értékelő ellenőrizze az értékeléshez átadott egyéb bizonyítékokat is (pl. TOE terv, biztonsági szerkezet leírás, üzemeltetési felhasználói dokumentáció), hogy észrevegye, ha ezek leírnak egy olyan működést meghatározó vagy kiegészítő paramétert, amit a funkcionális specifikáció nem tartalmaz.

ADV_FSP.2.4C Az SFR-t érvényre juttató TSFI-kre, a funkcionális specifikációnak le kell írnia a TSFI-hez kapcsolódó, SFR-t érvényre juttató tevékenységeket.

ADV_FSP.2-6 Az értékelőnek meg kell vizsgálnia a TSFI bemutatását annak megállapítása érdekében, hogy az teljesen és helyesen leír-e az SFR-t érvényre juttató TSFI-khez kapcsolódó minden SFR-t érvényre juttató tevékenységet.

Ha egy interfészen keresztül elérhető tevékenység szerepet játszik a TOE valamelyik biztonsági szabályzatának az érvényre juttatásában (vagyis ha az interfészen keresztül hozzáférhető tevékenységek egyike visszavezethető a TSF-től elvárt SFR-ek egyikére), akkor a szóbanforgó interfész SFR-t érvényre juttató. Az ilyen szabályzatok nem korlátozódnak a hozzáférés ellenőrzési szabályzatokra, hanem minden olyan funkcionalitásra vonatkoznak, amelyet az ST-ben megadott SFR-ek valamelyike specifikál. Meg kell jegyezni, hogy egy interfészhez számos tevékenység tartozhat, következésképpen ezek közül egyesek lehetnek SFR-t érvényre juttatók, míg mások nem.

A fejlesztőnek nem kell „felcímkéznie” az interfészeket SFR-t érvényre juttatóként, és ugyanígy nincs megkövetelve, hogy egy interfészen keresztül hozzáférhető tevékenységet SFR-t érvényre juttatóként azonosítson. Az értékelő felelőssége hogy megvizsgálja a fejlesztő által nyújtott bizonyítékokat, és megállapítsa a kívánt információ meglétét. Abban az esetben, amikor a fejlesztő beazonosította az SFR-t érvényre juttató TSFI-t és az ezen az interfészen keresztül rendelkezésre álló, SFR-t érvényre juttató tevékenységeket, az értékelőnek feltétlenül meg kell ítélnie a teljességet és pontosságot az értékeléshez átadott egyéb

információk alapján (pl. TOE terv, biztonsági szerkezet leírás, üzemeltetési felhasználói útmutató), és az interfészhez bemutatott egyéb információk alapján (paraméterek és paraméter leírások, hibaüzenetek, stb.).

Ebben az esetben (amikor a fejlesztő csak SFR-t érvényre juttató információkat adott meg az SFR-t érvényre juttató TSFI-re), az értékelő győződjön meg arról is, hogy nincsenek rosszul kategorizált interfészek. Ez elvégezhető az értékeléshez átadott egyéb információk vizsgálatával (pl. TOE terv, biztonsági szerkezet leírás, üzemeltetési felhasználói útmutató), valamint az interfészhez bemutatott olyan egyéb információk vizsgálatával (például paraméterek és paraméter leírások), amelyek nincsenek SFR-t érvényre juttatóként kategorizálva.

Abban az esetben, amikor a fejlesztő ugyanolyan szintű információt nyújt minden interfészre, az értékelő hajtsa végre az előző bekezdésben megemlített típusú vizsgálatot. Az értékelő állapítsa meg, hogy mely interfészek SFR-t érvényre juttatók, és melyek nem, majd ezt követően győződjön meg arról, hogy az SFR-t érvényre juttató tevékenységek SFR-t érvényre juttató vonatkozásait megfelelően leírták-e.

Az SFR-t érvényre juttató tevékenységek azok, amelyek valamelyik külső interfészen láthatók, és az elvárt SFR-k érvényre juttatására szolgálnak. Például, ha vannak naplózási követelmények az ST-ben, akkor a naplózással kapcsolatos tevékenységek SFR-t érvényre juttatók, ennélfogva kötelező leírni ezeket, még akkor is, ha ezen tevékenységek eredménye általában nem látható az érintett interfészen (minthogy a naplózással kapcsolatban egy interfészen kiváltott felhasználói tevékenység gyakran egy másik interfészen látható napló-bejegyzést idéz elő).

A leírás megkívánt szintje olyan, ami elegendő az olvasó számára annak megértéséhez, hogy a TSFI tevékenységek milyen szerepet játszanak az SFR vonatkozásában. Az értékelő tartsa szem előtt, hogy a leírásnak elegendően részletesnek kell lennie ahhoz, hogy támogassa a teszt-esetek előállítását (és kiértékelését) a szóbanforgó interfész vonatkozásában. Ha a leírás nem világos, vagy nem eléggé részletes a TSFI értelmes teszteléséhez, akkor valószínű, hogy a leírás nem megfelelő.

ADV_FSP.2.5C Az SFR-t érvényre juttató TSFI-kre, a funkcionális specifikációnak le kell írnia az SFR-t érvényre juttató tevékenységek feldolgozásából származó közvetlen hibaüzeneteket.

ADV_FSP.2-7 Az értékelőnek meg kell vizsgálnia a TSFI bemutatását annak megállapítása érdekében, hogy az teljesen és helyesen leírja-e az SFR-t érvényre juttató tevékenységek feldolgozásából származó közvetlen hibaüzeneteket.

Ezt a munkaegységet vagy az ADV_FSP.2-6 munkaegységgel összekapcsolva, vagy utána kell végrehajtani, hogy biztosított legyen az SFR-t érvényre juttató TSFI és az SFR-t érvényre juttató tevékenységek helyes azonosítása. A fejlesztő az elvártnál több információt is biztosíthat (például az összes interfészhez kapcsolódó összes hibaüzenetet), mely esetben az értékelő a pontosságra és teljességre vonatkozó felmérését az SFR-t érvényre juttató TSFI SFR-t érvényre juttató tevékenységeire korlátozhatja.

A hibák sokféle formát ölthetnek, a leírandó interfésztől függően. Egy API esetében maga az interfész visszaadhat hibakódot; beállíthat egy globális hibafeltételt; vagy beállíthat egy hibakóddal kapcsolatos meghatározott paramétert. Egy konfigurációs fájl esetében egy helytelenül beállított paraméter kiválthat egy naplófájlban rögzítendő hibaüzenetet. Egy hardver PCI kártya esetében egy hibafeltétel egy jelet válthat ki a buszon, vagy egy CPU-hoz kapcsolódó kivétel feltételt idézhet elő.

Hibák (és a kapcsolódó hibaüzenetek) egy interfész aktivizálásán keresztül következnek be. Az interfész aktivizálására adott válaszként jelentkező feldolgozás hiba körülményekkel találhatja szemben magát, ami egy hibaüzenet előállítását váltja ki (egy megvalósítás-specifikus mechanizmuson keresztül). Bizonyos esetekben ez lehet egy visszatérési érték magától az interfésztől; más esetekben lehetséges, hogy egy globális értéket állítanak be, és az interfész aktivizálása után ezt ellenőrzik. Valószínű, hogy a TOE számos olyan alacsony-szintű hibaüzenettel rendelkezik, amelyek alapvető erőforrás körülményekből erednek, mint például „a diszk megtelt”, vagy „erőforrás lock-olva van”. Bár az ilyen hibaüzenetek számos TSFI-hez hozzárendelhetők, felhasználhatók az olyan esetek felismerésére, amikor egy interfész leírás kimaradt. Például egy olyan TSFI, amely „a diszk megtelt” üzenetet állít elő, de amihez a tevékenységek ismertetésénél nem tartozik kézzelfogható leírás arról, hogy a TSFI miért idéz elő diszk hozzáférést, arra ösztönözheti az értékelőt, hogy a szóbanforgó TSFI-vel kapcsolatos egyéb bizonyítékokat is megvizsgálja (biztonsági szerkezet (ADV_ARC), TOE terv (ADV_TDS)), annak megállapítása érdekében, hogy a leírás teljes és helyes-e.

Annak megállapítása érdekében, hogy egy TSFI aktivizálása következtében fellépő hibaüzenet leírása pontos és teljes-e, az értékelő mérje össze az interfész leírásokat az értékeléshez átadott egyéb bizonyítékokkal (pl. TOE terv, biztonsági szerkezet leírás, üzemeltetési felhasználói dokumentáció), valamint az adott TSFI-hez szolgáltatott egyéb bizonyítékokkal (az SFR-t érvényre juttató tevékenységek leírása, a TSF-t támogató és a TSF-be nem beavatkozó tevékenységek és eredmények összegzése) is.

ADV_FSP.2.6C A visszavezetésnek szemléltetnie kell az SFR-ek visszavezetését a funkcionális specifikáció TSFI-eire.

ADV_FSP.2-8 Az értékelőnek ellenőriznie kell, hogy a visszavezetés összekapcsolja-e az SFR-eket a megfelelő TSFI-kkel.

A visszavezetés a fejlesztőnek kell megadnia abból a célból, hogy útmutatóként szolgáljon ahhoz, hogy mely SFR-ek, mely TSFI-kkel állnak kapcsolatban. Ez a visszavezetés lehet olyan egyszerű, mint például egy táblázat; ez bemenetként szolgál az értékelő számára a következő munkaegységekben való felhasználáshoz, amelyekben az értékelő ellenőrzi ennek helyességét és teljességét.

6.2.3.1.2.2. Az ADV_FSP.2.2E értékelői akció

ADV_FSP.2.2E Az értékelőnek meg kell állapítania, hogy a funkcionális specifikáció az SFR-ek pontos és teljes megjelenítése-e.

ADV_FSP.2-9 Az értékelőnek meg kell vizsgálnia a funkcionális specifikációt annak megállapítása érdekében, hogy az az SFR-ek teljes megjelenítése-e.

Az értékelő építhet a fejlesztő visszavezetésére (lásd ADV_FSP.2-8), ami egy megfeleltetés a TOE biztonsági funkcionális követelmények és a TSFI között, hogy meggyőződjön arról, hogy a funkcionális specifikáció és a teszt lefedettség vizsgálat minden SFR-t lefed. Meg kell jegyezni, hogy a szóbanforgó megfeleltetés részletezettségi szintje lehet alacsonyabb, mint a követelmények összetevő-, sőt elem szintje, a funkcionális követelményeken végrehajtott műveletek miatt (értékadások, pontosítások és kiválasztások), amit az ST szerzője végez el.

Például az FDP_ACC.l komponens tartalmazhat egy értékadásokkal rendelkező elemet. Ha az ST például tíz szabályt tartalmaz az FDP_ACC.l értékadásban, és ezt a tíz szabályt esetleg három különböző TSFI fedi le, az értékelő számára nem lenne elegendő az FDP_ACC.l-hoz hozzárendelni a TSFI A, B és C-t, és kijelenteni, hogy ezzel teljesítetve van a munkaegység. Ehelyett az értékelő feltehetően hozzárendeli az FDP ACC.l (1-es szabály) –t a TSFI A-hoz; az FDP ACC.l (2-es szabály) –t a TSFI B-hez; stb. Lehetséges az az eset is, hogy az interfész egy gyűjtő interfész (pl. IOCTL), amikor a megfeleltetést az adott interfész bizonyos paraméterkészletére kell megadni.

Az értékelőnek fel kell ismernie, hogy az olyan követelményekre vonatkozóan, amelyek kevéssé vagy egyáltalán nem öltenek testet a TSF határán (pl. FDP_RIP), nincsen elvárva, hogy ezeket teljes mértékben megfeleltessék a TSFI-nek. A szóbanforgó követelmények vizsgálatát a TOE terv vizsgálatakor fogják elvégezni (ADV_TDS), ha ez benne van az ST-ben. Fontos megjegyezni azt is, hogy mivel a TSFI-hez kapcsolódó paramétereket, tevékenységeket és hibaüzeneteket teljes mértékben specifikálni kell, az értékelőnek képesnek kell lennie annak megállapítására, hogy egy SFR minden vonatkozásáról látszik-e, hogy azt interfész szinten valósították meg.

ADV_FSP.2-10 Az értékelőnek meg kell vizsgálnia a funkcionális specifikációt annak megállapítása érdekében, hogy az az SFR-ek helyes megjelenítése-e.

Az ST-ben lévő minden olyan funkcionális követelmény esetében, amely a TSF határán látható hatásokban nyilvánul meg, a követelményhez kapcsolódó TSFI-hez megadott információ specifikálja a követelmény által leírt megkívánt funkcionalitást. Ha például az ST hozzáférés ellenőrzési listákra vonatkozó követelményt tartalmaz, és ennek a követelménynek egyetlen olyan TSFI-t feleltettek meg, amely Unix-fajtájú védelmi bitekre specifikál funkcionalitást, akkor a funkcionális specifikáció az adott követelmény szempontjából helytelen.

Az értékelőnek tudnia kell, hogy az olyan követelményekre vonatkozóan, amelyek kevéssé vagy egyáltalán nem öltenek testet a TSF határán (pl. FDP_RIP), nem várják el, hogy teljes mértékben megfeleltessék a TSFI-nek. A szóbanforgó követelmények vizsgálatát a TOE terv vizsgálatakor fogják elvégezni (ADV_TDS), ha ez benne van az ST-ben.

6.2.3.1.3. TOE tervezés: Az ADV_TDS.1 altevékenység értékelése

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,

b) funkcionális specifikáció,
c) biztonsági szerkezet leírás,
d) TOE terv.

6.2.3.1.3.1. Az ADV_TDS.1.1E értékelői akció

ADV_TDS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ADV_TDS.1.1C A tervnek le kell írnia a TOE szerkezetét alrendszerek szerint.

ADV_TDS.1-1 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy a teljes TOE szerkezetet leírták-e alrendszerek szerint.

Az értékelő győződjön meg arról, hogy a TOE minden alrendszerét azonosították. Ez a TOE leírás bemenetként szolgál az ADV_TDS.3-2 munkaegységhez, ahol a TOE TSF-et alkotó részeit azonosítják. Vagyis ez a követelmény a teljes TOE-ra vonatkozik, nem csak a TSF-re.

A TOE (és a TSF) leírható az absztrakció több szintjén (vagyis alrendszerek és modulok szintjén). A TOE bonyolultságától függően a terv leírható alrendszerek és modulok szerint. Ezen a garanciaszinten a felbontást csak az alrendszerekig szükséges elvégezni.

E tevékenység végrehajtásakor az értékelő vizsgáljon meg a TOE-hoz bemutatott egyéb bizonyítékot is (pl. ST, üzemeltetési felhasználói útmutató) annak megállapítása érdekében, hogy a TOE leírása ezekben a bizonyítékokban összhangban áll-e a TOE tervben leírtakkal.

ADV_TDS.1.2C A tervnek azonosítania kell a TSF minden alrendszerét.

ADV_TDS.1-2 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy az a TSF minden alrendszerét azonosítja-e.

Az ADV_TDS.1-1 munkaegységben a TOE valamennyi alrendszere legyen azonosítva, és állapítsák meg, hogy a nem-TSF alrendszereket helyesen jellemezték-e. Erre a munkára alapozva, pontosan azonosítani kell azokat az alrendszereket, melyeket nem jellemeztek nem-TSF alrendszerként. Az értékelő állapítsa meg az „Előkészítő eljárások” (AGD_PRE) útmutatónak megfelelően installált hardverről és szoftverről, hogy minden alrendszert figyelembe vettek, akár része a TSF-nek, akár nem.

ADV_TDS.1.3C A tervnek le kell írnia a TSF minden SFR-t támogató és SFR-be nem beavatkozó alrendszerének működésmódját, kellő részletességgel annak megállapításához, hogy az nem SFR-t érvényre juttató.

ADV_TDS.1-3 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy a TSF minden SFR-t támogató és SFR-be be nem avatkozó alrendszerét leírták-e úgy, hogy az értékelő megállapíthassa, hogy ezek az alrendszerek valóban SFR-t támogatók vagy SFR-be be nem avatkozóak.

ADV_TDS.1.4C A tervnek összegeznie kell az SFR-t érvényre juttató alrendszerek SFR-t érvényre juttató működésmódját.

ADV_TDS.1-4 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy az biztosít-e egy teljes, pontos és magas szintű leírást az SFR-t érvényre juttató alrendszerek SFR-t érvényre juttató működésmódjáról.

A fejlesztő megjelölheti az alrendszereket SFR-t érvényre juttatóként, SFR-t támogatóként, és SFR-be nem beavatkozóként, bár ezek a „megjelölések" csak annak jelzésére szolgálnak, hogy a fejlesztőnek milyen mennyiségű és típusú információt kell szolgáltatnia, és felhasználható azon információ mennyiségének korlátozására, amelyet a fejlesztőnek kell kidolgoznia, ha az előkészítési munkálatok nem állítják elő a megkívánt dokumentációt. Akár kategorizálta az alrendszereket a fejlesztő, akár nem, az értékelő felelőssége annak megállapítása, hogy az alrendszerek rendelkeznek-e megfelelő információval a TOE-beli szerepüket illetően (SFR-t érvényre juttató, stb.), és a megfelelő információ megszerzése a fejlesztőtől, ha a fejlesztő elmulasztotta biztosítani a megkívánt információt egy meghatározott alrendszer esetében.

Az SFR-t érvényre juttató tulajdonság arra utal, hogy egy alrendszer hogyan biztosítja az SFR-t megvalósító funkcionalitást. Nem szükséges, hogy a magas-szintű leírás speciális adat-struktúrákra utaljon (bár lehetséges), ehelyett azonban legyen benne szó az alrendszeren belüli általánosabb adat-áramlásokról, üzenet-áramlásokról és szabályozási kapcsolatokról. Az ilyen leírásoknak az a célja, hogy az értékelőnek elegendő információt nyújtson az SFR-t érvényre juttató tulajdonság megvalósításának a megértéséhez. Az értékelő ehhez a munkaegységhez kutassa fel az SFR érvényre juttatására vonatkozó nem elfogadható állításokat a TOE terv dokumentációban. Meg kell jegyezni, hogy az értékelő döntésén múlik, hogy egy meghatározott TOE esetében mit jelent a „magas-szint", és hogy elegendő információt kapott-e a fejlesztőtől ahhoz, hogy megbízható határozatot hozhasson erre a munkaegységre.

Az értékelő a teljesség és pontosság megállapítás céljából egyéb rendelkezésre álló információkat is vizsgáljon meg (pl. funkcionális specifikáció, biztonsági szerkezet leírás). E dokumentumok funkcionalitásra vonatkozó leírásainak összhangban kell lenniük a munkaegységhez biztosított bizonyítékkal.

ADV_TDS.1.5C A tervnek leírást kell nyújtania a TSF-t érvényre juttató alrendszerek közötti, valamint a TSF-t érvényre juttató és egyéb alrendszerek közötti kölcsönhatásokról.

ADV_TDS.1-5 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy a TSF alrendszerei közötti kölcsönhatásokat leírja-e.

Az alrendszerek közötti kölcsönhatások leírásának az a célja, hogy segítse az olvasót annak jobb megértésében, hogy a TSF hogyan hajtja végre a funkcióit. Ezeket a kölcsönhatásokat nem szükséges megvalósítási szinten jellemezni (pl. egy alrendszer valamelyik rutinjából paramétereknek az átadása egy másik alrendszerhez tartozó rutin számára; globális változók; hardver jelzések (pl. megszakítások) az egyik hardver alrendszertől egy megszakítás-kezelő alrendszer felé), de ebben a fejtegetésben legyenek lefedve azok az adatelemek, amelyeket egy speciális alrendszerhez úgy határoztak meg, hogy ezeket egy másik alrendszerben való felhasználásra szántak. Az alrendszerek közötti minden felügyeleti kapcsolatot is ismertetni

kell (pl. az egyik alrendszer felelős egy tűzfal rendszer szabályzat-bázisának konfigurálásáért és a másik alrendszer megvalósítja a szóbanforgó szabályokat).

Az értékelőnek a saját megítélésére kell támaszkodnia a leírás teljességének kiértékelésekor. Ha egy kölcsönhatás oka nem világos, vagy ha vannak olyan SFR-vonzatú kölcsönhatások (például az alrendszer viselkedésére vonatkozó leírás vizsgálata közben felfedezve), amelyekről úgy tűnik, hogy nincsenek ismertetve, az értékelő gondoskodjon arról, hogy ezt az információt az értékelő átadja. Ha azonban az értékelő azt állapítja meg, hogy az alrendszerek egy meghatározott összessége közötti kölcsönhatások olyanok, hogy bár ezeket nem ismerteti teljes mértékben a fejlesztő, a teljes leírás nem járulna hozzá sem az általános funkcionalitás, sem pedig a TSF által nyújtott biztonsági funkcionalitás megértéséhez, akkor az értékelő dönthet úgy, hogy a leírást elegendőnek tekinti, és nem kívánja meg a teljességet csak a saját kedvéért.

ADV_TDS.1.6C A megfeleltetésnek szemléltetnie kell, hogy a TOE tervben ismertetett minden működésmódot megfeleltették az ezt aktivizáló TSFI-nek.

ADV_TDS.1-6 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy az tartalmaz-e teljes és helyes megfeleltetést a funkcionális specifikációban leírt TSFI és a TOE tervben leírt TSF modulok között.

A TOE tervben leírt alrendszerek a TSF működését ismertetik, a TSF SFR-t érvényre juttató részeit részletesen, az egyéb részeit pedig magas szinten. A TSFI azt ismerteti, hogy a megvalósítás hogyan használható. A fejlesztőtől származó bizonyíték azonosítja azt az alrendszert, ami először aktivizálódik, mikor műveletet kérnek a TSFI-től, valamint azonosítja a funkcionalitás megvalósításáért elsődlegesen felelős alrendszereket. A teljes hívási fa nem szükséges minden egyes TSFI-hez ennél a munkaegységnél.

Az értékelő mérje fel a megfeleltetés teljességét meggyőződve arról, hogy minden TSFI-hez legalább egy alrendszert hozzárendeltek. A helyesség ellenőrzése bonyolultabb.

A helyességre vonatkozó első szempont az, hogy minden egyes TSFI legyen megfeleltetve egy alrendszernek a TSF határánál. Ennek megállapítása megtehető az alrendszerek és kölcsönhatások ismertetésének áttekintésével, majd ezek helyének a meghatározásával az architektúrában a szóbanforgó információk alapján. A helyességre vonatkozó következő szempont az, hogy ennek a megfeleltetésnek van-e értelme. Például egy hozzáférés ellenőrzéssel foglalkozó TSFI-nek a hozzárendelése egy olyan alrendszerhez, amely jelszókat ellenőriz, nem helyes. Az értékelőnek itt is az ítélőképességét kell igénybe vennie ennek a megállapításnak a meghozatalakor. A cél az, hogy ez az információ segítse az értékelőt abban, hogy megértse a rendszert és az SFR-ek megvalósítását, valamint azt a módot, ahogyan az entitások a TSF határán kölcsönhatásba tudnak lépni a TSF-fel. Annak felmérését, hogy az SFR-eket pontosan írták-e le alrendszerek szerint, nagyrészt a többi munkaegységben hajtják végre.

6.2.3.1.3.2. Az ADV_TDS.1.2E értékelői akció

ADV_TDS.1.2E Az értékelőnek meg kell erősítenie, hogy a terv az összes funkcionális biztonsági követelmény (SFR) pontos és teljes megjelenítése.

ADV_TDS.1-7 Az értékelőnek meg kell vizsgálnia a TOE biztonsági funkcionális követelményeket és a TOE tervet annak megállapítása érdekében, hogy a TOE terv az ST minden funkcionális biztonsági követelményét (SFR) lefedi-e.

Az értékelő összeállíthat egy megfeleltetést a TOE funkcionális biztonsági követelményei és a TOE terv között. Ez a megfeleltetés feltehetően egy SFR-től az alrendszerek egy halmazáig fog vezetni. Meg kell jegyezni, hogy a szóbanforgó megfeleltetés részletezettségi szintje lehet alacsonyabb, mint a követelmények összetevő-, sőt elem szintje, az ST szerzője által az SFR-eken végrehajtott műveletek (értékadások, pontosítások és kiválasztások) miatt.

Például a „Részleges hozzáférés ellenőrzés” (FDP_ACC.l) összetevő tartalmazhat egy értékadásokkal rendelkező elemet. Ha az ST például tíz szabályt tartalmaz a „Részleges hozzáférés ellenőrzés” (FDP_ACC.l) értékadásában, és ezt a tíz szabályt tizenöt modulon belüli megadott helyeken valósították meg, nem lenne elegendő, ha az értékelő a „Részleges hozzáférés ellenőrzés”-t (FDP_ACC.l) egy alrendszerhez rendelné hozzá, majd kijelentené, hogy a munkaegység teljesítve lett. Ehelyett, az értékelő rendelje hozzá a „Részleges hozzáférés ellenőrzés” (FDP_ACC.l) (1-es szabály)-t az A alrendszer x, y, és z moduljaihoz, a „Részleges hozzáférés ellenőrzés” (FDP_ACC.l) (2-es szabály)-t az A alrendszer x, p, és q moduljaihoz, és így tovább.

ADV_TDS.1-8 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy az minden funkcionális biztonsági követelményt helyesen jelenít-e meg.

Az értékelő győződjön meg arról, hogy az ST TOE-ra vonatkozó SFR-eket felsoroló részének minden biztonsági követelményére létezik a TOE tervben egy megfelelő terv leírás, amely pontosan részletezi, hogy a TSF hogyan valósítja meg a szóbanforgó követelményt. Ez megkívánja az értékelőtől, hogy határozzon meg egy alrendszer összetételt, amely felelős egy megadott funkcionális követelmény megvalósításáért, majd vizsgálja meg a szóbanforgó alrendszereket annak megértése érdekében, hogy a követelmény hogyan valósul meg. Végül az értékelő mérje fel, hogy a követelmény helyesen lett-e megvalósítva.

Példaként, ha az ST követelmények szerepkör-alapú hozzáférés ellenőrzési mechanizmust specifikálnak, az értékelő először azonosítsa azokat az alrendszereket, amelyek hozzájárulnak ennek a mechanizmusnak a megvalósításához. Ez megtehető a TOE terv mélyreható ismerete vagy megértése alapján, vagy a megelőző munkaegységben elvégzett munkán keresztül. Meg kell jegyezni, hogy ennek a nyomkövetésnek csak az a célja, hogy azonosítsa az alrendszereket, nem pedig a teljes vizsgálat.

A következő lépés annak megértése, hogy az alrendszerek milyen mechanizmusokat valósítanak meg. Például, ha a terv egy olyan hozzáférés ellenőrzési megvalósítást ír le, amely UNIX-típusú védelmi biteken alapul, a terv nem pontos megvalósulása azoknak a hozzáférés ellenőrzési követelményeknek, amelyeket a fenti ST példa mutat be. Ha az értékelő a részletek hiánya miatt nem tudja megállapítani, hogy pontosan milyen mechanizmusokat valósítottak meg, becsülje fel, hogy minden SFR-t érvényre juttató alrendszert azonosítottak-e, vagy hogy a szóbanforgó alrendszerekről elegendő részleteket nyújtottak-e.

6.2.3.2. Az Útmutató dokumentumok garanciaosztály (AGD) értékelése

Az útmutató dokumentumokhoz kapcsolódó tevékenységnek az a célja, hogy elbírálják annak a dokumentációnak a megfelelőségét, amely ismerteti, hogy a felhasználó hogyan tudja a TOE-t biztonságos módon kezelni. Az ilyenfajta dokumentációnak figyelembe kell vennie a különféle felhasználó típusokat (például azokat, akik befogadják, telepítik, adminisztrálják vagy üzemeltetik a TOE-t), akiknek a helytelen akciói hátrányosan befolyásolhatják a TOE-nak vagy a saját adataiknak a biztonságát.

Az útmutató dokumentumok osztály két családra van osztva, amelyek elsősorban az előkészítő felhasználói dokumentációval foglalkoznak (ami mindazt tartalmazza, amit meg kell tenni annak érdekében, hogy a leszállított TOE-t átalakítsák a környezet értékelt konfigurációjához, ahogyan az az ST-ben le van írva, vagyis ahogyan a TOE-t befogadják és telepítik), másodsorban pedig az üzemeltetői felhasználói dokumentációval (ami mindazt tartalmazza, amit meg kell tenni a TOE üzemeltetése során az értékelt konfigurációban, vagyis az üzemeltetést és adminisztrációt).

Az útmutató dokumentumokhoz kapcsolódó tevékenység azokra a funkciókra és csatlakozási felületekre vonatkozik, amelyek a TOE biztonságához kapcsolódnak. A TOE biztonságos konfigurálása az ST-ben van leírva.

6.2.3.2.1. Előkészítő eljárások: Az AGD_PRE.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a TOE biztonságos előkészületi eljárásait és lépéseit dokumentálták, s hogy ezek biztonságos konfigurációt eredményeznek.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) a TOE, beleértve az előkészítő eljárásait,
c) a fejlesztő szállítási eljárásainak leírása.

Az előkészületi eljárások az összes olyan elfogadási és telepítési eljárást jelentik, melyek ahhoz szükségesek, hogy a TOE-t az ST-ben leírt biztonságos konfiguráció állapotába juttassák.

6.2.3.2.1.1. Az AGD_PRE.1.1E értékelői akció

AGD_PRE.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

AGD_PRE.1.1C Az előkészítő eljárásoknak le kell írniuk a leszállított TOE biztonságos elfogadásához szükséges valamennyi lépést, a fejlesztő szállítási eljárásaival összhangban.

AGD_PRE.1-1 Az értékelőnek ellenőriznie kell, hogy biztosították-e a leszállított TOE biztonságos elfogadásához szükséges eljárásokat.

Amennyiben a fejlesztő szállítási eljárásaival kapcsolatban nem várható elfogadási eljárások alkalmazása, akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

AGD_PRE.1-2 Az értékelőnek meg kell vizsgálnia a biztosított elfogadási eljárásokat annak megállapítása érdekében, hogy azok leírják-e a TOE biztonságos elfogadásához szükséges lépéseket, a fejlesztő szállítási eljárásaival összhangban.

Az elfogadási eljárásoknak legalább az arra vonatkozó felhasználói ellenőrzést tartalmazniuk kell, hogy a TOE valamennyi részét az ST-ben jelzett helyes verziókkal szállították-e le.

Az elfogadási eljárásoknak tükrözniük kell azokat a felhasználó által a leszállított TOE elfogadásához alkalmazott lépéseket, melyek a fejlesztő szállítási eljárásaiból származnak.

Az elfogadási eljárásoknak részletes információt kell szolgáltatniuk az alábbiakhoz, amennyiben azok alkalmazhatók:

a) az arról való meggyőződés, hogy a leszállított TOE a teljes értékelt példány.
b) a leszállított TOE módosításának vagy hamisításának az észlelése.

AGD_PRE.1.2C Az előkészítő eljárásoknak le kell írniuk a TOE biztonságos telepítéséhez, valamint az üzemeltetési környezethez való biztonságos előkészülethez szükséges valamennyi lépést, az ST-ben leírt, üzemeltetési környezetre vonatkozó biztonsági célokkal összhangban.

AGD_PRE.1-3 Az értékelőnek ellenőriznie kell, hogy biztosították-e a TOE biztonságos telepítéséhez szükséges eljárásokat.

Amennyiben a TOE-vel és üzemeltetési környezetével kapcsolatban nem várható telepítési eljárások alkalmazása (mert például a TOE-t már működésre alkalmas állapotban szállították le, s nincsenek a környezetére vonatkozó követelmények), akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

AGD_PRE.1-4 Az értékelőnek meg kell vizsgálnia a biztosított telepítési eljárásokat annak megállapítása érdekében, hogy azok leírják-e a TOE biztonságos telepítéséhez, valamint az üzemeltetési környezet biztonságos előkészítéséhez szükséges lépéseket, az ST biztonsági céljaival összhangban.

Amennyiben nem várható telepítési eljárások alkalmazása (mert például a TOE-t már működésre alkalmas állapotban szállították le, s nincsenek a környezetére vonatkozó követelmények), akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

A telepítési eljárásoknak részletes információt kell szolgáltatniuk az alábbiakról, amennyiben azok alkalmazhatók:

a) a biztonságos telepítéshez szükséges minimális rendszer követelmények,
b) az üzemeltetési környezetre vonatkozó követelmények, az ST-ben meghatározott biztonsági célokkal összhangban,
c) a TSF ellenőrzése alatt álló egyedek telepítés-specifikus biztonsági tulajdonságainak módosítása,
d) kivételek és problémák kezelése.

6.2.3.2.1.2. Az AGD_PRE.1.2E értékelői akció

AGD_PRE.1.2E Az értékelőnek végre kell hajtania az előkészítő eljárásokat annak megerősítése érdekében, hogy a TOE biztonságosan előkészíthető a működésre.

Az előkészítés megköveteli az értékelőtől, hogy a TOE-t egy leszállításra alkalmas állapotból olyan állapotba állítsa át, amelyben a TOE üzemel, beleértve a TOE elfogadását és telepítését, valamint az ST-ben megadott biztonsági célokkal összhangban álló SFR-ek érvényre juttatását.

Az értékelőnek a TOE elfogadására és telepítésére kizárólag a fejlesztői eljárásokat szabad követnie, s csak a vásárlóktól általánosan elvárt tevékenységeket szabad végrehajtania, csak az előkészületi útmutatót használva. A végrehajtás során tapasztalt bármilyen nehézség hiányos, nem egyértelmű vagy megalapozatlan útmutatót jelenthet.

Az értékelő ezt a munkaegységet végrehajthatja a „Független tesztelés – minta” (ATE_IND.2) értékelési altevékenységgel együtt.

6.2.3.2.2. Üzemeltetési felhasználói útmutató: Az AGD_OPE.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy az üzemeltetési felhasználói útmutató leírja-e minden felhasználói szerepkörre a TSF által nyújtott biztonsági funkcionalitást és interfészeket, tartalmazza-e a TOE biztonságos használatához szükséges utasításokat és útmutatást, lefedi-e az összes üzemeltetési mód biztonságos eljárásait, lehetővé teszi-e a TOE nem biztonságos állapotainak megelőzését és észlelését, egyúttal egyértelmű és megalapozott-e.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) a funkcionális specifikáció,
c) a TOE terv,
d) az üzemeltetési felhasználói útmutató.

6.2.3.2.2.1. Az AGD_OPE.1.1E értékelői akció

AGD_OPE.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

AGD_OPE.1.1C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre le kell írnia azokat a felhasználó által elérhető funkciókat és jogosultságokat (beleértve a megfelelő figyelmeztetéseket is), melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

AGD_OPE.1-1 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót, annak megállapítása érdekében, hogy az leírja-e azokat a felhasználó által elérhető funkciókat

és jogosultságokat (beleértve a megfelelő figyelmeztetéseket is), melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

A TOE konfigurálása lehetővé teheti, hogy a különböző felhasználói szerepkörök a TOE különböző funkcióihoz eltérő jogosultságokkal rendelkezzenek. Ezáltal egyes felhasználók számára engedélyezve lesznek olyan funkciók, melyek mások számára nem. Ezeket a funkciókat és jogosultságokat minden felhasználói szerepkörre le kell írni az üzemeltetési felhasználói útmutatóban.

Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre azonosítania kell az ellenőrzés alatt tartandó funkciókat és jogosultságokat, az ezek számára szükséges utasítás típusokat, valamint az utasítások okait. Az üzemeltetési felhasználói útmutatónak figyelmeztetéseket kell tartalmaznia az ellenőrzés alatt tartandó funkciókra és jogosultságokra vonatkozóan. A figyelmeztetéseknek a várt hatásokról, az esetleges mellékhatásokról és a más funkciókkal és jogosultságokkal kapcsolatos lehetséges kapcsolatokról kell szólniuk.

AGD_OPE.1.2C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre le kell írnia, hogy a TOE által biztosított, elérhető interfészeket hogyan kell biztonságos módon használni.

AGD_OPE.1-2 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e a TOE által biztosított, elérhető interfészek biztonságos használatát.
Az üzemeltetési felhasználói útmutatónak javaslatokat kell megfogalmaznia a TSF hatékony használatához (például jelszó kialakítási gyakorlat áttekintése, felhasználói állományok mentésének javasolt gyakorisága, felhasználói hozzáférési jogok megváltoztatása hatásának elemzése).

AGD_OPE.1.3C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre le kell írnia az elérhető funkciókat és interfészeket, különösen a felhasználó ellenőrzése alá tartozó minden biztonsági szempontból fontos paramétert, jelezve (ahol ez lehetséges) a biztonságos értékeket.

AGD_OPE.1-3 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e az elérhető funkciókat és interfészeket, különösen a felhasználó ellenőrzése alá tartozó minden biztonsági paramétert, jelezve (ahol ez lehetséges) a biztonságos értékeket is.
Az üzemeltetési felhasználói útmutatónak áttekintést kell adnia a felhasználói interfészeken keresztül látható biztonsági funkcionalitásról.

Az üzemeltetési felhasználói útmutatónak azonosítania kell, és le kell írnia a biztonsági funkciók és interfészek célját, működésüket, illetve egymás között kapcsolataikat.

Minden felhasználó által elérhető interfészre az üzemeltetési felhasználói útmutatónak:

a) le kell írnia azokat a módszereket, melyekkel az interfész hívható (pl. parancssor, programozási nyelvi rendszerhívások, menükiválasztás, parancsgombok);
b) le kell írnia a felhasználó által állítandó paramétereket, azok célját, érvényes és alapértelmezett értékeiket, a paraméterek biztonságos és nem biztonságos

használatát okozó beállításokat, mindezt egyenként vagy paraméter-kombinációkban;

c) le kell írnia a közvetlen TSF válaszokat, üzeneteket vagy visszaadott kódot.

Az értékelőnek elsősorban a funkcionális specifikációt és az ST-t kell figyelembe vennie annak megállapítása érdekében, hogy az ezekben leírt TSF összhangban áll-e az üzemeltetési felhasználói útmutatóval. Az értékelőnek meg kell győződnie az üzemeltetési felhasználói útmutató teljességéről, vagyis arról, hogy az összes emberi felhasználó számára lehető teszi az elérhető TSFI-k biztonságos használatát. Az értékelő segítségként elkészítheti az útmutató és ezen dokumentumok közötti informális leképezést. Az ebben fellelhető bármilyen hiányosság az útmutató teljességének csorbulását jelezheti.

AGD_OPE.1.4C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre világosan be kell mutatnia a felhasználó által elérhető funkciókkal kapcsolatban végrehajtandó, biztonsági szempontból fontos minden esemény típust, beleértve a TSF ellenőrzése alá eső egyedek biztonsági tulajdonságainak megváltoztatását is.

AGD_OPE.1-4 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e a felhasználói funkciókkal kapcsolatban végrehajtandó, biztonsági szempontból lényeges minden esemény típust, beleértve a TSF ellenőrzése alá tartozó egyedek biztonsági tulajdonságainak megváltoztatását is.

Minden biztonsági szempontból fontos esemény típust részletezni kell minden felhasználói szerepkörre, hogy minden felhasználó tudja, milyen események fordulhatnak elő, és mit kell tennie (ha szükséges) a biztonság fenntartása érdekében. A TOE üzemeltetése során előforduló biztonsági szempontból lényeges eseményeket (például naplótár túlcsordulás; rendszerösszeomlás; felhasználói rekordok felülírása, mint amikor egy felhasználó távozik a szervezettől, és a fiókját eltörlik) kellően meg kell határozni, hogy a felhasználó beavatkozhasson a biztonságos működés fenntartása érdekében.

AGD_OPE.1.5C Az üzemeltetési felhasználói útmutatónak azonosítani kell a TOE összes lehetséges üzemeltetési módját (beleértve a meghibásodás vagy üzemeltetési hiba utáni műveleteket is), valamint ezek biztonságos üzemeltetésre gyakorolt következményeit és kihatásait.

AGD_OPE.1-5 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót és az egyéb értékeléshez adott bizonyítékot annak megállapítása érdekében, hogy az útmutató azonosítja-e a TOE összes lehetséges üzemmódját (beleértve a meghibásodás vagy üzemeltetési hiba utáni működést is, amennyiben ilyen előfordulhat), valamint ezek következményét és kihatásait a biztonságos üzemelés fenntartására.

Más értékelési bizonyítékot, elsősorban a funkcionális specifikációt az értékelőnek annak megállapításához javasolt használnia, hogy az útmutató megfelelő eligazító leírást tartalmaz-e.

Amennyiben a garanciacsomaghoz tesztdokumentáció van csatolva, akkor az ebben a bizonyítékban nyújtott információ is felhasználható annak eldöntésére, hogy az útmutató

elegendő útmutató információt tartalmaz-e. A tesztlépéseknél megadott részletek felhasználhatók annak megerősítésére, hogy a nyújtott útmutató elégséges a TOE használatához és adminisztrálásához.

Az értékelőnek egy időben egy ember számára látható TSFI-t ajánlott vizsgálnia, úgy, hogy összehasonlítja a TSFI biztonságos használatáról szóló útmutatást egyéb bizonyítékokkal, annak kiderítése érdekében, hogy a TSFI-vel kapcsolatos információk valóban jól írják-e le annak biztonságos használatát (azaz megfelelnek-e az SFR-eknek). Az értékelőnek az interfészek közötti kapcsolatokat is át kell néznie, potenciális ellentmondásokat keresve.

AGD_OPE.1.6C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre le kell írnia azokat a betartandó biztonsági intézkedéseket, melyek az ST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célok elérését szolgálják.

AGD_OPE.1-6 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e azokat a betartandó biztonsági intézkedéseket, melyek az ST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célok elérését szolgálják.

Az értékelő elemezze az ST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célokat, majd állapítsa meg, hogy az üzemeltetési felhasználói útmutató minden felhasználói szerepkörre megfelelően leírja-e a fontos biztonsági intézkedéseket.

Az üzemeltetési felhasználói útmutatóban leírt biztonsági intézkedéseknek magukban kell foglalniuk az összes fontos külső eljárásrendi, fizikai, személyzeti és kapcsolódásra vonatkozó intézkedést.

Megjegyzendő, hogy a TOE biztonságos telepítésére vonatkozó intézkedéseket az Előkészítő eljárások (AGD_PRE) vizsgálja.

AGD_OPE.1.7C Az üzemeltetési felhasználói útmutatónak egyértelműnek és megalapozottnak kell lennie.

AGD_OPE.1-7 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az egyértelmű-e.

Az útmutató akkor nem egyértelmű (félrevezető), ha ez alapján egy egy felhasználó indokoltan félreértheti teendőit, és a TOE-ra vagy a TOE által nyújtott biztonságra nézve hátrányos módon alkalmazza a leírtakat.

AGD_OPE.1-8 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az megalapozott-e.

Az útmutató akkor tekinthető megalapozatlannak, ha olyan követelményeket támaszt a TOE használatával vagy üzemeltetési környezetével szemben, melyek nem felelnek meg az ST-nek, vagy indokolatlanul nagy terhet jelentenek a biztonság fenntartásához.

6.2.3.3. Az Életciklus támogatás garanciaosztály (ALC) értékelése

Az életciklus támogatáshoz kapcsolódó tevékenységnek az a célja, hogy elbírálja a fejlesztő által a TOE fejlesztése és kezelése során használt biztonsági eljárások megfelelőségét. Ezek az eljárások magukban foglalják a fejlesztő által használt életciklus modellt, a konfiguráció kezelést, a TOE fejlesztése során alkalmazott biztonsági intézkedéseket, a fejlesztő által a TOE életciklusa során használt eszközöket, a biztonsági rések kezelését és a szállítási tevékenységet.

A TOE elégtelenül ellenőrzött fejlesztése és kezelése sebezhetőségekhez vezethet a megvalósításban. Egy definiált életciklus modellnek való megfelelőség elősegítheti az intézkedések javítását ezen a területen. Egy, a TOE-hoz alkalmazott mérhető életciklus modell megszüntetheti a félreérthetőségeket a TOE fejlesztési eljárásának kiértékelésében. (Alap garanciaszinten nincsenek életciklus modellre vonatkozó követelmények.)

A konfiguráció kezeléshez kapcsolódó tevékenységnek az a célja, hogy segítséget nyújtson a fogyasztónak az értékelt TOE beazonosításában, hogy biztosítsa a konfiguráció elemek egyedi azonosítását, és biztosítsa a fejlesztő által a TOE-n történt változtatások ellenőrzéséhez és nyomonkövetéséhez használt eljárások megfelelőségét. Ez magában foglalja az arra vonatkozó részleteket, hogy milyen változtatások vannak nyomonkövetve, hogy a lehetséges változtatások hogyan vannak beépítve, és magában foglalja, hogy milyen mértékben használnak automatizálást a hibalehetőségek csökkentésére.

A fejlesztő biztonsági eljárásainak az a célja, hogy védjék a TOE-t és a kapcsolódó tervezési információkat a hamisításokkal vagy felfedésekkel szemben. A fejlesztési folyamatba történő hamisítás lehetővé teheti sebezhetőségek szándékos bevitelét. A tervezési információk felfedése lehetővé teheti a sebezhetőségek könnyebb kiaknázhatóságát. Az eljárások megfelelősége a TOE és a fejlesztési folyamat természetétől függ. (Alap garanciaszinten nincsenek fejlesztői biztonsági eljárásokra vonatkozó követelmények.)

Ha a fejlesztő és a fejlesztési folyamatba bevont harmadik felek jól meghatározott fejlesztő eszközöket használnak és megvalósítási szabványokat alkalmaznak, akkor ez segít annak biztosításában, hogy sebezhetőségeket ne vigyenek be figyelmetlenségből a pontosítás során. (Alap garanciaszinten nincsenek fejlesztő eszközökre vonatkozó követelmények.)

A hibajavításhoz kapcsolódó tevékenység célja, hogy nyomonkövessék a biztonsági réseket, meghatározzák a javító műveleteket, és hogy eljuttassák a javító műveletekre vonatkozó információkat a TOE felhasználóknak. (A hibajavítási tevékenységek garanciacsalád nem képezi kötelező részét egyetlen garanciaszintnek sem. A TOE garancia folyamatosságának biztosításához azonban kötelező követelmény. A hibajavításra vonatkozó követelményeket és ezek értékelési követelményeit [8] részletezi.)

A szállításhoz kapcsolódó tevékenység célja annak az elbírálása, hogy megfelelő azoknak az eljárásoknak a dokumentációja, amelyek biztosítják, hogy a TOE-t változtatás nélkül szállítják ki a fogyasztóhoz.

6.2.3.3.1. Konfiguráció kezelési képességek: Az ALC_CMC.2 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztő használ-e egy konfiguráció kezelés rendszert, mely egyértelműen azonosít minden konfiguráció elemet.
Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) a tesztelésre alkalmas TOE,
c) a konfiguráció kezelési dokumentáció.

Ez a komponens egy közvetett értékelői akciót foglal magában annak eldöntésére, hogy a CM rendszert használják-e. Minthogy az itt megadott követelmények a TOE beazonosítására és egy konfiguráció lista nyújtására korlátozódnak, ezt az akciót a meglévő munkaegységek már lefedik és azokra korlátozódik. Az ALC_CMC.3 altevékenység értékelésekor (fokozott garanciaszinten) a követelmények túlnyúlnak ezen a két tételen, és a művelet határozottabb bizonyítéka szükséges.

6.2.3.3.1.1. Az ALC_CMC.2.1E értékelői akció

ALC_CMC.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ALC_CMC.2.1C A TOE-t meg kell jelölni egyedi hivatkozásával.

ALC_CMC.2-1 Az értékelőnek ellenőriznie kell, hogy az értékelésre benyújtott TOE verzióját megjelölték-e hivatkozásával

Az értékelőnek gondoskodnia kell arról, hogy a TOE tartalmazza az ST-ben megadott egyedi hivatkozást. Ez elérhető megjelölt csomagolással vagy adathordozóval, illetve a működő TOE által megjelenített címkével. Ez biztosítja, hogy a vásárlók is képesek a TOE megfelelő azonosítására (a vásárlás vagy használat időpontjában).

A TOE biztosíthat is egy olyan módszert, mellyel egyszerűen azonosítható. Például egy szoftver TOE induláskor vagy egy parancs-sorra adott válaszként kijelezheti nevét és verziószámát. Egy hardver vagy förmver TOE azonosítható a TOE-ra fizikailag rábélyegzett sorozatszámmal.

ALC_CMC.2-2 Az értékelőnek ellenőriznie kell, hogy az alkalmazott TOE hivatkozások ellentmondás mentesek-e.

Amennyiben a TOE-t egynél több helyen jelölik meg (címkézik), akkor a címkéknek egyezniük kell. Lehetséges például, hogy a TOE részeként biztosított, címkézett útmutató dokumentációkat az értékelt működő TOE-hez kapcsoljuk. Ez biztosítja, hogy a vásárlók biztosak legyenek abban, hogy a TOE értékelt verzióját vették meg, telepítették, és az útmutató dokumentációból is a helyes verzióval rendelkeznek, az ST-nek megfelelő üzemeltetés érdekében.

Az értékelő azt is ellenőrizze, hogy a TOE hivatkozása megegyezik-e az ST-ben szereplővel.

ALC_CMC.2.2C A konfiguráció kezelés dokumentációnak le kell írnia a konfiguráció elemek egyértelmű azonosítására alkalmazott módszert.

ALC_CMC.2-3 Az értékelőnek meg kell vizsgálnia a konfiguráció elemek azonosításához alkalmazott módszert, annak megállapítása érdekében, hogy az leírja-e azt, hogy hogyan azonosítják egyedileg a konfiguráció elemeket.

Eljárások ismertessék, hogy az egyes konfiguráció elemek állapota hogyan követhető nyomon a TOE életciklusa során. Az eljárások részletezve lehetnek a CM tervben vagy a különböző CM dokumentumokban. A tartalmazott információ ismertesse a következőket:

a) azt a módszert, ahogyan az egyes konfiguráció elemeket egyedileg azonosították, hogy az adott konfiguráció elem verziói nyomon követhetők legyenek;
b) azt a módszert, ahogyan a konfiguráció elemekhez egyedi azonosítókat jelölnek ki, és ahogyan ezek a CM rendszerbe bekerülnek;
c) azt a módszert, amely egy konfiguráció elem kiváltott verzióinak azonosítására szolgál.

ALC_CMC.2.3C A konfiguráció kezelés rendszernek egyértelműen azonosítania kell minden konfiguráció elemet.

ALC_CMC.2-4 Az értékelőnek meg kell vizsgálnia a konfiguráció elemeket annak megállapítása érdekében, hogy azokat a konfiguráció kezelés rendszernek megfelelő módon azonosították.

Arra vonatkozó garancia, hogy a CM rendszer minden konfiguráció elemet egyedileg azonosít, a konfiguráció elemek azonosítóinak vizsgálatán keresztül nyerhető. Mind a TOE-t alkotó konfiguráció elemekre, mind pedig a fejlesztő által értékelési bizonyítékként átadott konfiguráció elem leírásokra vonatkozóan az értékelőnek meg kell erősítenie, hogy minden egyes konfiguráció elem olyan egyedi azonosítóval rendelkezik, amely összhangban áll a CM dokumentációban ismertetett egyedi azonosítási módszerrel.

6.2.3.3.2. Konfiguráció kezelés hatóköre: Az ALC_CMS.2 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a konfiguráció lista tartalmazza-e a TOE-t, a TOE-t alkotó részeket, valamint az értékelési bizonyítékokat.
Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) a konfiguráció lista.

6.2.3.3.2.1. Az ALC_CMS.2.1E értékelői akció

ALC_CMS.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ALC_CMS.2.1C A konfiguráció listának tartalmaznia kell a következőket: maga a TOE; a garanciális biztonsági követelmények (SAR) által megkövetelt értékelési bizonyítékok és a TOE-t alkotó részek.

ALC_CMS.2-1 Az értékelőnek ellenőriznie kell, hogy a konfiguráció lista tartalmazza-e az alábbi elem készletet:

a) maga a TOE;
b) a TOE-t alkotó részek;
c) az ST garanciális biztonsági követelményei (SAR) által megkövetelt értékelési bizonyítékok.

ALC_CMS.2.2C A konfiguráció listának egyértelműen azonosítania kell a konfiguráció elemeket.

ALC_CMS.2-2 Az értékelőnek meg kell vizsgálnia a konfiguráció listát annak megállapítása érdekében, hogy az egyértelműen azonosít-e minden konfiguráció elemet.

A konfiguráció lista elegendő információt tartalmazzon ahhoz, hogy egyértelműen azonosítja az összes konfiguráció elem használt verzióját (ez tipikusan egy verzió szám). Ezen lista használatával az értékelő ellenőrizheti, hogy az értékelés a helyes konfiguráció elemekre, és mindegyikük helyes verziójára irányul.

ALC_CMS.2.3C A konfiguráció listának a TSF szempontból fontos minden konfiguráció elemre meg kell adni az elem fejlesztőjét.

ALC_CMS.2-3 Az értékelőnek ellenőriznie kell, hogy a konfiguráció lista megadja-e a TSF szempontból fontos összes konfiguráció elem fejlesztőjét.

Amennyiben a TOE fejlesztésében csak egy fejlesztő érintett, akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

6.2.3.3.3. Szállítás: Az ALC_DEL.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a szállítási dokumentáció leírja-e az összes olyan eljárást, amelyet a TOE biztonság fenntartásához használnak a vásárlókhoz történő szállítás során.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) a szállítási dokumentáció.

6.2.3.3.3.1. Az ALC_DEL.1.1E értékelői akció

ALC_DEL.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ALC_DEL.1.1C A szállítási dokumentációnak le kell írnia minden olyan eljárást, amely a TOE verzióinak vásárlókhoz történő szállítása során a biztonság fenntartásához szükséges.

ALC_DEL.1-1 Az értékelőnek meg kell vizsgálnia a szállítási dokumentációt annak megállapítása érdekében, hogy az leírja-e az összes olyan eljárást, amely a TOE vagy részei verzióinak felhasználókhoz történő szállítása során a biztonság fenntartásához szükségesek.
A szállítási eljárások leírják a TOE vagy összetevőinek szállítása során a TOE biztonságának fenntartására, valamint a TOE azonosítására alkalmas eljárásokat.

A szállítási dokumentáció az egész TOE-re vonatkozik, ugyanakkor a TOE különböző részeire különböző eljárások vonatkozhatnak. Az értékelésnek az eljárások összességét figyelembe kell vennie.

A szállítási eljárásokat a szállítás teljes folyamatában, a gyártási környezettől a telepítési környezetig alkalmazni kell (például csomagolás, tárolás és szétosztás). A csomagolás és szállítás szabványos kereskedelmi gyakorlata elfogadható lehet. Ez magában foglalja a zsugorfóliás csomagolást, a biztonsági csíkot vagy egy pecsételt borítékot. A szétosztásra fizikai (pl. nyilvános levelezés vagy magán szolgáltató) vagy elektronikus (pl. elektronikus mail vagy interneten keresztüli letöltés) eljárások alkalmazhatók.

A fejlesztő kriptográfiai ellenőrző összegeket vagy elektronikus aláírást használhat a módosítás vagy a hamisítás észlelhetősége érdekében. A hamisítás ellen védő pecsétek a bizalmasság megsértését is jelzik. Szoftver TOE esetén a bizalmasság titkosítás alkalmazásával biztosítható. Amennyiben a rendelkezésre állás fontos szempont, megbízható továbbítás követelhető meg.

A "biztonság fenntartásához szükséges" kitétel értelmezésekor figyelembe kell venni az alábbiakat:

- a TOE jellege (pl. szoftver vagy hardver),
- A TOE-ra kinyilvánított általános, a sebezhetőség vizsgálatnál megválasztott biztonsági szint. Amennyiben a TOE-nak üzemeltetési környezetében ellent kell állnia egy bizonyos támadó képességgel rendelkező támadókkal szemben, akkor ez a TOE szállítására is alkalmazandó. Az értékelőnek meg kell állapítania, hogy kiegyensúlyozott megközelítést alkalmaztak-e annak érdekében, hogy a szállítás ne jelentsen gyenge pontot egy egyébként biztonságos fejlesztési folyamatban.
- Az ST által meghatározott biztonsági célok. A szállítási dokumentációknál a hangsúly valószínűleg a sértetlenséggel kapcsolatos intézkedéseken lesz. Ugyanakkor bizonyos TOE-k szállítása esetében a bizalmasság és a rendelkezésre állás is kiemelt fontosságú, ilyenkor ezeket a szempontokat is vizsgálni kell.

Az ALC_DEL.1.2D bizonyítékból származtatott értékelői akció

ALC_DEL.1.2D A fejlesztőnek használnia kell a szállítási eljárásokat.

ALC_DEL.1-2 Az értékelőnek meg kell vizsgálnia a szállítási folyamat különböző oldalait annak megállapítása érdekében, hogy alkalmazzák-e a szállítási eljárásokat.

Az értékelő megközelítési módszere a szállítás alkalmazásának ellenőrzésével kapcsolatban a TOE jellegétől és magától a szállítási folyamattól függ. Az eljárások vizsgálatán túl az értékelőnek valamilyen szinten meg kell győződnie arról, hogy a szabályokat a gyakorlatban is betartják. Lehetséges megközelítési módok az alábbiak:

a) látogatás a szétosztási hely(ek)en, ahol megfigyelhető az eljárások gyakorlati alkalmazása;
b) a TOE átvizsgálása a szállítás valamelyik fázisában vagy a felhasználó telephelyén (például a hamisítás ellen védő pecsétek ellenőrzése);
c) a szállítási folyamat alkalmazásának megfigyelése a gyakorlatban, amikor az értékelő a TOE-t szabályos csatornákon keresztül szerzi be;
d) a végfelhasználók megkérdezése a TOE szállítás folyamatáról.

A helyszíni szemlékre útmutató található a 7.2.3 pontban.

Egy újonnan fejlesztett TOE esetén előfordulhat, hogy a TOE szállítási eljárásait még nem vezették be a gyakorlatban. Ekkor az értékelőnek meg kell elégednie azzal, hogy a megfelelő eljárásokat és eszközöket kialakították a jövőbeli szállításokra, és minden érintett alkalmazott tisztában van a felelősségével. Az értékelő kérheti a szállítás egy "száraztesztjét", amennyiben ez célszerűnek tűnik. Amennyiben a fejlesztő már korábban létrehozott hasonló terméket, akkor az ott bevezetett eljárások vizsgálata is segíthet az aktuális termékkel kapcsolatos garancia megállapításában.

6.2.3.4. A Tesztelés garanciaosztály (ATE) értékelése

Ennek a tevékenységnek a célja annak megállapítása, hogy a TOE olyan módon viselkedik-e, ahogyan azt az ST-ben leírták és (az ADV osztályban leírt) értékelési bizonyítékban specifikálták. Ezt a megállapítást a TSF fejlesztő általi funkcionális tesztelése (ATE_FUN) és a TSF értékelő általi független tesztelése (ATE_IND) bizonyos kombinációján keresztül lehet megtenni. További garancia nyerhető azzal, hogy a fejlesztőt növekvő mértékben bevonják a tesztelésbe és a TOE-ra vonatkozó kiegészítő információk nyújtásába, valamint azzal, hogy az értékelő növeli a független tesztelési tevékenységeket.

6.2.3.4.1. Alkalmazási megjegyzések

A TSF tesztelését részben az értékelő, illetve a legtöbb esetben a fejlesztő hajtja végre. Az értékelő tesztelési törekvései nemcsak eredeti tesztek létrehozásából és végrehajtásából állnak, hanem a fejlesztői tesztek megfelelőségének felméréséből és ezek egy részhalmazának újra lefuttatásából is.

Az értékelő megvizsgálja a fejlesztői teszteket annak meghatározása érdekében, hogy azok milyen mértékben elegendőek annak bizonyításához, hogy a TSFI a specifikáltaknak (lásd ADV_FSP) megfelelően működik, és hogy megértse a fejlesztő tesztelési megközelítés módját. Hasonlóan, az értékelő megvizsgálja a fejlesztői teszteket annak meghatározása érdekében, hogy azok milyen mértékben elegendőek a TSF belső viselkedésének és tulajdonságainak a bemutatásához.

Az értékelő végrehajtja a fejlesztői tesztek egy részhalmazát is, ahogyan azokat dokumentálták, abból a célból, hogy megbizonyosodjon a fejlesztői teszteredményekről: az értékelő ennek a vizsgálatnak az eredményeit bemenetként fogja felhasználni a TSF egy részhalmazának független teszteléséhez. Erre a részhalmazra az értékelő egy olyan tesztelési megközelítési módot alkalmaz, amely eltér a fejlesztőétől, különösen akkor, ha a fejlesztői tesztek hiányosak.

A fejlesztői tesztelési dokumentáció helyességének értékeléséhez, illetve új tesztek készítéséhez az értékelőnek meg kell értenie a TSF elvárt, tervezett működését – mind belülről, mind a TSFI-n keresztül látható módon - azon SFR-ek összefüggésében, melyek kielégítésére létrehozták ezeket. Az értékelő választhatja azt az utat, hogy a TSF-et és a TSFI-t alrendszerekre bontja az ST funkcionális területei alapján (napló alrendszer, naplózással kapcsolatos TSFI, hitelesítő modul, hitelesítéssel kapcsolatos TSFI, stb.) ha az ST ezt nem bontotta már fel így, majd egyszerre csak egy alrendszerre összpontosít. Minden alrendszerre megvizsgálja az ST követelményt és a fejlesztői és az útmutató dokumentáció vonatkozó részeit, hogy megértse azt, milyen működést várnak el a TOE-tól. A fejlesztői dokumentációra épülő bizalom aláhúzza a tesztelés lefedettségének (ATE_COV) és mélységének (ATE_DPT) függőségét a fejlesztés (ADV) garanciaosztálytól. (Az alap garanciaszint még nem tartalmaz a tesztelés mélységére vonatkozó követelményeket.)

A CC a családok összetevőinek alkalmazásakor elkülöníti a tesztelés lefedettségét és mélységét a funkcionális teszteléstől, a rugalmasság fokozása érdekében. A családok követelményeit azonban együtt kell alkalmazni annak biztosítása érdekében, hogy a TSF a specifikációjának megfelelően működik. A családok e szoros összefonódása az értékelői munka megduplázódásához vezet a különböző altevékenységek között. Az alábbi alkalmazási megjegyzések az altevékenységek közötti szöveg ismétléseket minimalizálják.

6.2.3.4.1.2. A TOE elvárt működésének megértése

A tesztelési dokumentáció helyességének értékelése, illetve új tesztek készítése előtt az értékelőnek meg kell értenie a biztonsági funkciók elvárt, tervezett működését azon követelmények összefüggésében, melyek kielégítésére létrehozták ezeket.

Mint ahogyan korábban említésre került, az értékelő választhatja a TSF és a TSFI alrendszerekre bontását az ST-ben szereplő SFR-ek (naplózás, hitelesítés, stb.) szerint, majd egyszerre csak egy alrendszerre összpontosíthat. Az értékelő vizsgáljon meg minden ST követelményt, valamint a funkcionális specifikáció és az útmutató dokumentáció vonatkozó részeit, hogy megértse azt, milyen működést várnak el az érintett TSFI-től. Hasonlóan, az értékelő vizsgálja meg a TOE terv és a biztonsági szerkezet dokumentáció vonatkozó részeit, hogy megértse azt, milyen működést várnak el a TSF érintett alrendszereitől és moduljaitól.

A tervezett működés megértése után az értékelő vizsgálja meg a tesztelési tervet, hogy áttekintést kapjon a tesztelés módszeréről. A legtöbb esetben a tesztelési módszer egy TSFI kiváltása, majd a válaszok megfigyelése. A kívülről látható funkcionalitások közvetlenül tesztelhetők, amikor viszont a funkcionalitás a TOE-n kívülről nem látható (például a maradvány információ védelmi funkcionalitás), akkor más eszközöket kell alkalmazni.

A tesztelés, illetve egyéb módszerek a funkcionalitás elvárt működésének ellenőrzésére

Azon esetekben, melyekben nem célszerű, vagy nem lehetséges a tesztelés (amikor nincs kívülről látható TSFI), a tesztelési tervnek alternatívát kell adnia a tervezett viselkedés, működés ellenőrzésére. Az értékelő felelőssége az alternatív módszer alkalmasságának megítélése. A következőket azonban ajánlott figyelembe venni az egyéb módszerek alkalmasságának megállapításakor:

a) elfogadható alternatív módszer a megvalósítási reprezentáció elemzése annak megállapítása érdekében, hogy a megkívánt működést mutatja-e a TOE. Ez jelenthet kód vizsgálatot egy szoftver TOE, vagy chip-maszk vizsgálatot egy hardver TOE esetén.
b) elfogadható a fejlesztő integrációs vagy modul tesztelése által kapott bizonyíték felhasználása is, még ha az értékelési garanciaszint nincs is arányban a TOE modulok alacsony szintű leírásával (ADV_TDS.3 értékelési altevékenység), vagy a megvalósítás leírásával (ADV_IMP.1 értékelési altevékenység). Amennyiben a fejlesztő integrációs vagy modul tesztelését használják egy biztonsági funkcionalitás elvárt működésének ellenőrzése során, akkor meg kell arról győződni, hogy a tesztelési bizonyíték a TOE aktuális megvalósítását tükrözi-e. Amennyiben az alrendszer vagy a modulok változtak a tesztelés óta, akkor bizonyítékra van szükség arról, hogy a változtatásokat nyomon követték és elemezték, vagy ilyen esetekben általában további teszteket kell elvégezni.

Hangsúlyozni kell, hogy a tesztelési munka kiegészítése alternatív módszerekkel csak akkor járható út, ha mind a fejlesztő, mind az értékelő úgy ítéli meg, hogy nincs más praktikus lehetőség egy biztonsági funkció tervezett működésének tesztelésére.

A tesztek megfelelőségének ellenőrzése

A tesztelés által megkövetelt kezdeti feltételek kialakításához szükség van a tesztelés előfeltételeire. Ezek kifejezhetők beállítandó paraméterekkel, vagy a tesztelés sorrendjének kialakításával, olyan esetekben, amikor az egyik teszt befejezése teremti meg egy másik teszt szükséges előfeltételeit. Az értékelőnek meg kell állapítania, hogy az előfeltételek teljesek és alkalmasak-e, nehogy a megfigyelt teszteredmények az elvárt eredmény irányába befolyásolják a folyamatot.

A tesztelési lépések és várt eredmények meghatározzák a TSFI-re alkalmazandó feladatokat és paramétereket, valamint, hogy a várt eredményeket milyen módon kell ellenőrizni és mik ezek az eredmények. Az értékelőnek meg kell állapítania, hogy a tesztelési lépések és várt eredmények összhangban vannak-e a funkcionális specifikáció TSFI leírásával. Ez azt jelenti, hogy a TSFI működés funkcionális specifikációban közvetlenül leírt minden jellemzőjéhez tartoznia kell tesztnek és várt eredménynek az adott működés ellenőrzése érdekében.

A tesztelési tevékenység fő célja annak megállapítása, hogy minden alrendszert, modult és TSFI-t kellőképpen leteszteltek a funkcionális specifikációban, TOE tervben és a biztonsági szerkezet leírásban megfogalmazott üzemeltetési elvárások szerint. Az alap garanciaszinten a tesztelés még nem tartalmaz terhelés teszteket és negatív teszteket. A tesztelési eljárások betekintést nyújtanak abba, hogy a fejlesztő a tesztelés során hogyan aktivizálta a TSFI-ket, modulokat és alrendszereket. Az értékelő ezt az információt felhasználja, amikor kiegészítő teszteket dolgoz ki a TSF független teszteléséhez.

6.2.3.4.2. Funkcionális tesztek: Az ATE_FUN.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztő vajon helyesen hajtotta végre és dokumentálta a tesztelési dokumentációban leírt teszteket.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) teszt dokumentáció.

Annak mértéke, hogy a tesztelési dokumentáció mennyire fedje le TSF-t, függ a lefedettség garanciális összetevőjétől.

A rendelkezésre bocsátott fejlesztői tesztekre az értékelőnek meg kell állapítania a tesztek megismételhetőségét, valamint azt, hogy a fejlesztői tesztek milyen mértékben használhatók az értékelő független teszteléséhez. Az értékelőnek minden olyan TSFI-t, amelyekre a fejlesztői teszt eredmények azt mutatják, hogy esetleg nem a specifikáltnak megfelelően hajtódnak végre, a megfelelőség vagy meg nem felelősség megállapítása érdekében független tesztelés alá kell vetnie.

6.2.3.4.2.1. Az ATE_FUN.1.1E értékelői akció

ATE_FUN.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ATE_FUN.1.1C A tesztelési dokumentációnak tartalmaznia kell a tesztelési terveket, az elvárt teszteredményeket és a tényleges teszteredményeket.

ATE_FUN.1-1 Az értékelőnek ellenőriznie kell, hogy a tesztelési dokumentáció tartalmazza-e a tesztelési terveket, az elvárt eredményeket és a tényleges teszt eredményeket.

Az értékelő ellenőrizze, hogy a tesztelési terveket, az elvárt eredményeket és a tényleges teszt eredményeket belefoglalták-e a tesztelési dokumentációba.

ATE_FUN.1.2C A tesztelési terveknek azonosítaniuk kell a végrehajtandó teszteket, és le kell írniuk minden teszt végrehajtásának forgatókönyvét. Ezen forgatókönyveknek tartalmazniuk kell a más tesztek eredményeitől való minden sorrendbeli függést.

ATE_FUN.1-2 Az értékelőnek ellenőriznie kell, hogy a tesztelési terv leírja-e minden teszt végrehajtásának forgatókönyvét.

Az értékelőnek meg kell állapítania, hogy a teszterv nyújt-e információkat a használt tesztkonfigurációra vonatkozóan: mind a TOE konfigurációra, mind pedig minden használt tesztberendezésre vonatkozóan. Ennek az információnak a tesztkonfiguráció reprodukálhatóságának biztosításához kellően részletesnek kell lennie.

Az értékelőnek azt is meg kell állapítania, hogy a teszterv nyújt-e információt arról, hogy hogyan kell végrehajtani a tesztet: az összes szükséges automatizált indítási eljárásról (és hogy ezek igényelnek-e futási jogosultságot), az alkalmazandó bemenetekről és ezek alkalmazásáról, hogyan lehet megkapni a kimenetet, valamennyi automatikus törlési eljárásról (és hogy ezek igényelnek-e futási jogosultságot), stb. Ennek az információnak a teszt reprodukálhatóságának biztosításához kellően részletesnek kell lennie.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ATE_FUN.1-3 Az értékelőnek meg kell vizsgálnia a tesztelési tervet annak megállapítása érdekében, hogy a TOE teszt konfigurációja megegyezik-e az ST-ben az értékelésre megadott konfigurációval.

A tesztelési tervben ugyanazt az egyedi hivatkozást kell alkalmazni a TOE-ra, mint amit a Konfiguráció kezelési képességek (ALC_CMC) altevékenységekben fektettek le, illetve amit az ST bevezetőjében azonosítottak.

Az ST egynél több konfigurációt is meghatározhat az értékeléshez. Az értékelő ellenőrizze, hogy a fejlesztő által a tesztelési dokumentációban azonosított összes teszt konfiguráció megfelel-e az ST-nek. Például az ST olyan kötelezően beállítandó konfigurációs lehetőségeket határozhat meg, amelyek befolyásolják, hogy a TOE milyen részekből álljon, belefoglalva vagy kizárva egyes részeket. Az értékelő ellenőrizze, hogy a TOE összes ilyen változatát figyelembe vették.

Az értékelő vegye figyelembe azokat az ST-ben leírt, a TOE üzemeltetési környezetére vonatkozó biztonsági céljait, amelyek a teszt környezetre alkalmazhatók. Lehet hogy néhány cél nem alkalmazható a teszt környezetre. Például egy a felhasználói engedélyekkel kapcsolatos cél nem alkalmazható, míg a „csatlakozás a hálózathoz egyetlen ponton” alkalmazható.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ATE_FUN.1-4 Az értékelőnek meg kell vizsgálnia a tesztelési tervet annak megállapítása érdekében, hogy az elegendő utasítást tartalmaz-e a sorrendi függőségekre.

Bizonyos lépések végrehajtására szükség lehet a kezdeti feltételek kialakítása érdekében. Például a felhasználói fiókokat fel kell venni, mielőtt azokat törölni lehet. Egy példa a sorrendiségi függőségre: először azokat a tevékenységeket kell végrehajtani, melyek naplóbejegyzéseket állítanak elő, s csak ezt követően lehet a naplóbejegyzéseket kereső és rendező tesztekkel foglakozni. Másik példa a sorrendiségi függőségre: egyik teszteset állítja elő azt az adatállományt, amely egy másik teszt eset számára bemenetként szolgál.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ATE_FUN.1.3C Az elvárt teszteredményeknek be kell mutatniuk a tesztek sikeres végrehajtásából keletkező várható kimeneteket.

ATE_FUN.1-5 Az értékelőnek meg kell vizsgálnia a tesztelési dokumentációt annak megállapítása érdekében, hogy az tartalmazza-e az összes várt teszteredményt.

Az elvárt teszteredmények annak megállapításához szükségek, hogy egy tesztet sikeresen végrehajtottak-e vagy sem. Az elvárt teszteredmények akkor tekinthetők kielégítőnek, ha egyértelműek, és megfelelnek az adott tesztelési módszer alapján várt működésnek.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ATE_FUN.1.4C A tényleges teszteredményeknek összhangban kell állniuk az elvárt teszteredményekkel.

ATE_FUN.1-6 Az értékelőnek ellenőriznie kell, hogy a tesztelési dokumentációban szereplő várt teszteredmények összhangban állnak-e a tényleges teszteredményekkel.

A fejlesztő által átadott tényleges és várt teszteredmények összehasonlítása felfedi a két eredményhalmaz közötti különbségeket. Lehet, hogy a tényleges teszteredmények közvetlen összehasonlítása nem történhet meg bizonyos adatok egyszerűsítése vagy összevonása előtt. Ilyenkor a fejlesztői tesztelési dokumentációban ismertetni kell a tényleges adatokat egyszerűsítő vagy összevonó eljárásokat.

Például a fejlesztőnek tesztelnie kell egy üzenettár tartalmát egy hálózati kapcsolat után, az üzenettár tartalmának megállapítása érdekében. Az üzenettár egy bináris számot tartalmaz, amelyet valamilyen más adatmegjelenítési formába kell átalakítani az értelmezhetőség érdekében. A fejlesztőnek tehát le kell írnia az adat magas szintű ábrázolási formába történő átalakításának módját, hogy az értékelő is végre tudja azt hajtani (szinkron vagy aszinkron átvitel, stop bitek száma, paritás, stb.).

Megjegyzendő, hogy a tényleges adatok egyszerűsítő vagy összevonó folyamatának leírását az értékelő nem a szükséges módosítások tényleges elvégzésére használja, hanem a folyamat megfelelőségének értékelésére. A fejlesztő feladata az elvárt teszteredmények átalakítása olyan formára, amely könnyen összehasonlítható a tényleges teszteredményekkel.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ATE_FUN.1-7 Az értékelőnek jelentést kell készítenie a fejlesztő tesztelési munkájáról, áttekintést adva a tesztelési módszerről, konfigurációról, mélységről és eredményekről.

Az értékelési jelentésben rögzített fejlesztői tesztelésről szóló információ lehetővé teszi az értékelő számára, hogy bemutassa az általános tesztelési módszert és a fejlesztő által a TOE tesztelésébe fektetett munkát. A cél a fejlesztő tesztelési munkájának érdemi áttekintése. Nem cél, hogy az értékelési jelentésben a fejlesztői teszteléssel kapcsolatos információk a specifikus tesztlépések vagy egyedi tesztek eredményeinek pontos megismétlése legyenek. A cél elegendő részletesség biztosítása más értékelők és a tanúsító szervezet számára ahhoz, hogy betekintést kapjanak a fejlesztő tesztelési módszerébe, a végrehajtott tesztek nagyságrendjébe, a TOE teszt konfigurációjába és a fejlesztői tesztelés általános eredményébe.

Az értékelési jelentés fejlesztői tesztekről szóló részében általában az alábbi információk találhatók:

a) TOE teszt konfigurációk. A ténylegesen tesztelt TOE konfigurációk, köztük az, hogy a teszt felállítása vagy a tesztet követő rendteremtés igényelt-e külön jogosultságú kódot.
b) Tesztelési módszer. Az alkalmazott fejlesztői tesztelési stratégia áttekintése.
c) Tesztelési eredmények. A fejlesztői tesztelés eredményének áttekintő leírása.

E lista korántsem teljes, csupán megmutat néhány területet, melyeknek a fejlesztői teszteléssel kapcsolatosan az értékelési jelentésben szerepelni kell.

6.2.3.4.3. Lefedettség: Az ATE_COV.2 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztő letesztelte-e az összes TSFI-t, és hogy a fejlesztő teszt lefedettség elemzése szemlélteti-e a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikációban leírt TSFI-k közötti megfelelést.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) teszt dokumentáció,
d) tesz lefedettség elemzés.

6.2.3.4.3.1. Az ATE_COV.2.1E értékelői akció

ATE_COV.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ATE_COV.2.1C A teszt lefedettség elemzésének szemléltetnie kell a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikációban leírt TSFI-k közötti megfelelést.

ATE_COV.2-1 Az értékelőnek meg kell vizsgálnia a teszt lefedettség elemzését annak megállapítása érdekében, hogy a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikációban leírt interfészek közötti megfeleltetés pontos-e.
A megfeleltetés bemutatására egy egyszerű kereszt-táblázat is elegendő lehet. A teszt lefedettség elemzésben szereplő teszteket és interfészeket egyértelműen kell azonosítani.
Emlékeztetjük az értékelőt arra, hogy nem kell a tesztelési dokumentáció valamennyi tesztjét leképezni a funkcionális specifikációban leírt interfészekre.

ATE_COV.2-2 Az értékelőnek meg kell vizsgálnia a tesztelési tervet annak megállapítása érdekében, hogy a tesztelési módszer minden interfész esetén szemlélteti-e az adott interfész elvárt működését.

Ehhez a munkaegységhez útmutató található az alábbi alkalmazási megjegyzésekben:

a) 6.2.5.4.1.1, A TOE elvárt működésének megértése
b) 6.2.5.4.1.2, A tesztelés, illetve egyéb módszerek a funkcionalitás elvárt működésének ellenőrzésére

ATE_COV.2-3 Az értékelőnek meg kell vizsgálnia a teszt eljárásokat annak megállapítása érdekében, hogy a teszt előfeltételek, a tesztelési lépések és az elvárt eredmény(ek) megfelelően tesztelnek-e minden interfészt.

Ehhez a funkcionális specifikációra vonatkozó munkaegységhez útmutató található az alábbi alkalmazási megjegyzésben:

a) 6.2.5.4.1.3, A tesztek megfelelőségének ellenőrzése.

ATE_COV.2.2C A teszt lefedettség elemzésének szemléltetnie kell, hogy a funkcionális specifikációban leírt összes TSFI-t letesztelték.

ATE_COV.2-4 Az értékelőnek meg kell vizsgálnia a teszt lefedettség elemzését annak megállapítása érdekében, hogy a funkcionális specifikációban leírt interfészek és a tesztelési dokumentációban azonosított tesztek közötti megfeleltetés teljes-e.

A funkcionális specifikációban szereplő valamennyi TSFI-nek meg kell jelennie a teszt lefedettség elemzésében, és ezeket le kell képezni a tesztekre a teljesség kimutatása érdekében, az interfészek teljes körű specifikáció tesztelése ugyanakkor nem követelmény. Nyilvánvalóan hiányos a lefedettség, ha a funkcionális specifikációban azonosított egyik interfészhez nem rendeltek tesztet.

Emlékeztetjük az értékelőt arra, hogy nem kell a tesztelési dokumentáció valamennyi tesztjét leképezni a funkcionális specifikációban leírt interfészekre.

6.2.3.4.4. Független tesztelés: Az ATE_IND.2 altevékenység értékelése

Ennek az altevékenységnek a célja a TSFI egy részhalmazának független tesztelésével annak megállapítása, hogy a TOE a terv dokumentációban előírt módon működik-e, valamint a fejlesztői tesztek megbízhatóságának ellenőrzése egy azokból vett minta végrehajtásával.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) TOE terv,
d) üzemeltetési felhasználói útmutató,
e) előkészítő felhasználói útmutató,
f) konfiguráció kezelés dokumentáció,
g) tesztelési dokumentáció,
h) a tesztelésre alkalmas TOE.

6.2.3.4.4.1. Az ATE_IND.2.1E értékelői akció

ATE_IND.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ATE_IND.2.1C A TOE-nek tesztelésre alkalmas állapotban kell lennie.

ATE_IND.2-1 Az értékelőnek meg kell vizsgálnia a TOE-t annak megállapítása érdekében, hogy a teszt konfiguráció megegyezik-e az ST-ben meghatározott, értékelés alatt álló konfigurációval.

A fejlesztő által biztosított és a teszt tervben azonosított TOE-nek ugyanazt az egyedi hivatkozást kell alkalmaznia, mint amit a „Konfiguráció kezelés képességei” (ALC_CMC) altevékenységekben fektettek le, illetve amit az ST bevezetőjében azonosítottak.

Az ST meghatározhat egynél több konfigurációt is az értékeléshez. A TOE több különálló hardver és szoftver elemből állhat, melyeket az ST-nek megfelelően kell tesztelni. Az értékelő ellenőrizze, hogy valamennyi teszt konfiguráció ellentmondás mentes-e az ST-vel.

Az értékelő vegye figyelembe azokat az ST-ben leírt, a TOE üzemeltetési környezetére vonatkozó biztonsági célokat, amelyek a teszt környezetre alkalmazhatók. Lehet hogy néhány cél nem alkalmazható a teszt környezetre. Például egy a felhasználói engedélyekkel kapcsolatos cél nem alkalmazható, míg a „csatlakozás a hálózathoz egyetlen ponton” alkalmazható.

Bármilyen tesztelési erőforrás (mérőműszer, elemző készülék) használatakor az értékelő felelőssége annak biztosítása, hogy ezek az erőforrások megfelelően hitelesítve legyenek.

ATE_IND.2-2 Az értékelőnek meg kell vizsgálnia a TOE-t annak megállapítása érdekében, hogy azt megfelelően telepítették-e, és ismert állapotban van-e.

Az értékelő a TOE állapotát többféle módon is megállapíthatja. Például az AGD_PRE.1 altevékenység értékelésének előzetes sikeres befejezése teljesíti ezt a munkaegységet, ha az értékelő még bizonyos abban, hogy a tesztelésre használt TOE-t megfelelően telepítették és ismert állapotban van. Amennyiben nem ez a helyzet, akkor az értékelőnek a fejlesztő eljárásait kell követnie a TOE telepítéséhez és indításához, kizárólag a rendelkezésére bocsátott útmutatókra támaszkodva.

Amennyiben az értékelőnek végre kell hajtania a telepítési lépéseket, mert a TOE ismeretlen állapotban van, akkor e munkaegység sikeres befejezése kielégítheti az AGD_PRE.1-5 munkaegységet is.

ATE_IND.2.2C A fejlesztőnek biztosítania kell a TSF fejlesztői funkcionális tesztelése során használt erőforrás-készlettel azonos eszközkészletet.

ATE_IND.2-3 Az értékelőnek meg kell vizsgálnia a fejlesztő által rendelkezésére bocsátott erőforrás-készletet annak megállapítása érdekében, hogy az azonos-e a TSF fejlesztői funkcionális tesztelése során alkalmazott erőforrásokkal.

A fejlesztő által használt erőforrás-készletet a fejlesztői tesztelési terv dokumentálja, az ATE_FUN funkcionális tesztelés családban meggondolt módon. Az erőforrás-készlet többek között felölelhet laboratóriumi hozzáférést és speciális teszt berendezéseket is. Azokat az erőforrásokat, melyek nem egyeznek meg a fejlesztő által használtakkal, azonossá kell tenni a teszteredményekre gyakorolt lehetséges hatásuk szerint.

6.2.3.4.4.2. Az ATE_IND.2.2E értékelői akció

ATE_IND.2.2E Az értékelőnek végre kell hajtania a tesztelési dokumentációban szereplő tesztek valamely részhalmazát (mintáját) a fejlesztői teszt eredmények ellenőrzése érdekében.

ATE_IND.2-4 Az értékelőnek el kell végeznie a tesztelést a fejlesztői tesztelési tervben és eljárásokban található tesztekből vett mintára.

E munkaegység célja, hogy az értékelő elegendő számú fejlesztői teszt végrehajtásával meggyőződjön a fejlesztői teszteredmények érvényességéről. A minta nagyságáról, és a mintát alkotó fejlesztői tesztekről az értékelő dönt (lásd 7.2.1).

Minden fejlesztői teszt visszavezethető speciális interfészekre. Ezért a mintát alkotó tesztek kiválasztásakor figyelembe vett tényezők hasonlóak az ATE_IND.2-6 munkaegységnél leírtakhoz. Ezen kívül az értékelő alkalmazhat véletlenszerű mintavételezési módszert is a fejlesztői tesztek kiválasztásához, mintába vételéhez.

ATE_IND.2-5 Az értékelőnek ellenőriznie kell, hogy a tényleges teszteredmények összhangban állnak-e az elvárt teszteredményekkel.

A tényleges és az elvárt teszteredmények közti különbségek az ellentmondás feloldására késztetik az értékelőt. Az értékelő által feltárt ellentmondást a fejlesztő is feloldhatja kielégítő magyarázattal vagy az eltérések feloldásával.

Amennyiben nincs kielégítő magyarázat vagy feloldás, akkor az értékelő kevésbé megbízhatónak ítélheti a fejlesztői tesztelést, és növelheti a tesztelési minta nagyságát. Annak megerősítése érdekében, hogy az ATE_IND.2-4 munkaegységben azonosított mintát megfelelően tesztelték, a fejlesztői tesztelésben talált hiányosságokat meg kell szüntetni, akár a fejlesztői tesztelés kijavításával, akár az értékelő által végzett új tesztekkel.

6.2.3.4.4.3. Az ATE_IND.2.3E értékelői akció

ATE_IND.2.3E Az értékelőnek tesztelnie kell a TSF interfészeinek egy részét annak megerősítése érdekében, hogy a TSF a specifikáltaknak megfelelően működik.

ATE_IND.2-6 Az értékelőnek meg kell terveznie egy tesztkészletet.

Az értékelő válassza ki a TOE-nek megfelelő tesztkészletet és tesztelési stratégiát. Egy lehetséges szélsőséges tesztelési stratégia szerint a tesztkészlet annyi interfészt tartalmaz, amennyi csak tesztelhető kevés szigorral. Egy másik lehetséges tesztelési stratégia, hogy a teszt néhány interfészre terjed ki azok fontossága szerint és ezeket igen alapos ellenőrzésnek vetik alá.

Az értékelő által követett tesztelési módszer általában e két szélsőséges eset közé esik. Az értékelőnek ajánlott az interfészek nagy részére legalább egy tesztet végrehajtania, de a tesztelésnek nem kell teljes körű specifikáció-tesztelésnek lennie.

Az értékelőnek a tesztelendő interfész részhalmaz kiválasztásakor az alábbi tényezőket kell figyelembe vennie:

a) A fejlesztői tesztelés bizonyítékai. Ez a következőkből áll: tesztelési dokumentáció, teszt lefedettség elemzés, teszt mélység elemzés. A fejlesztői teszt bizonyíték betekintést nyújt abba, hogy a fejlesztő a tesztelés során hogyan aktivizálta a biztonsági funkciókat. Az értékelő ezt az információt felhasználja a TOE független teszteléséhez szükséges új tesztek tervezésékor. Fokozottan át kell gondolnia a következőket:
   aa) Az interfészekre vonatkozó fejlesztői tesztelés bővítése. Az értékelő végrehajthat ugyanolyan típusú teszteket változó paraméterekkel az interfész szigorúbb tesztelése céljából.
   ab) Az interfészekre vonatkozó fejlesztői tesztelési stratégia kiegészítése. Az értékelő módosíthatja egy adott interfészeknél alkalmazott tesztelési módszert egy új tesztelési stratégiát alkalmazva.
b) Azon interfészek száma, melyekből a tesztkészlet készül. Amennyiben a TOE csak kis számú, viszonylag egyszerű interfészt tartalmaz, célszerű lehet az összes szigorú tesztelése. Más esetekben ez nem költség-hatékony módszer, ekkor mintavételezésre van szükség.
c) Az értékelési tevékenységek egyensúlyának fenntartása. A tesztelésbe fektetett értékelői munka álljon arányban a többi értékelési feladatba fektetett munkával.

Az értékelő válassza ki az interfészek részhalmazát. Ez a kiválasztás több tényezőtől függ, és e tényezők is hatást gyakorolnak a tesztkészlet méretére:

a) Az interfészek fejlesztői tesztelésének szigora. Azokat az interfészeket, melyekre az értékelő további tesztelés szükségességét állapítja meg, ajánlott a tesztkészletbe bevenni.
b) A fejlesztői teszteredmények. Amennyiben a fejlesztői teszteredmény kétséget támaszt az értékelőben egy interfész megfelelő megvalósításával kapcsolatban, az adott interfészt ajánlott a tesztkészletbe bevenni.
c) Az interfészek fontossága. Azokat az interfészeket, amelyek a többieknél fontosabbak, ajánlott a tesztkészletbe bevenni. A „fontosság” egyik jelentős tényezője a biztonsági jelentőség (az SFR-t érvényre juttató interfészek fontosabbak az SFR-t támogató interfészeknél, ezek pedig fontosabbak az SFR-be nem beavatkozó interfészeknél, lásd 6.2.3.1.2 ADV_FSP.2 alfejezet). A „fontosság” másik jelentős tényezője az adott interfészre képezhető SFR-ek száma (ahogyan azt az ADV-beli absztrakciós szintek közötti megfelelés azonosításakor meghatározzák).

d) Az interfészek bonyolultsága. A bonyolult megvalósítást igénylő interfészek bonyolult teszteket követelhetnek meg a fejlesztőktől és az értékelőktől, melyek súlyos, a költség-hatékonysággal ellentétes követelmények. Ugyanakkor a bonyolult interfészeknél nagyobb a hibákra bukkanás valószínűsége, így jó jelöltek lehetnek a tesztkészletbe. Az értékelőnek a fenti két ellentétes szempontot kell mérlegelnie.
e) Közvetett tesztelés. Egyes interfészek tesztelése gyakran más interfészek közvetett tesztelésével is jár, így ezek tesztkészletbe vétele maximalizálja a tesztelt interfészek számát (még ha csak közvetett módon is). Egyes interfészeket általában széleskörű biztonsági funkcionalitásra használnak, így egy hatékony tesztelési megközelítés ezeket megcélozza.
f) Az interfészek típusai (pl. programozott, parancs-soros, protokoll). Az értékelőnek a TOE által támogatott minden TOE által támogatott interfész típusból ajánlott bevennie teszteket.
g) Új vagy szokatlan megoldásokat használó interfészek. Amennyiben a TOE újszerű vagy szokatlan tulajdonságokat tartalmaz, melyek erős üzleti hangsúlyt kaphatnak, az ezeknek megfelelő interfészek is erős jelöltek a tesztelésre.

A fenti útmutató kiemeli a megfelelő tesztkészlet kiválasztási folyamata során figyelembe veendő tényezőket, de semmiképpen nem tekinthető teljesnek.

ATE_IND.2-7 Az értékelőnek el kell készítenie a tesztkészlethez a tesztelési dokumentációt, amely kellőképpen részletes a tesztek megismételhetősége érdekében.

A TSF elvárt működésének az ST-ből, a funkcionális specifikációból és a TOE tervből történő megértése után az értékelőnek meg kell határoznia az interfész tesztelésére leginkább alkalmas módot. Az értékelő különösen az alábbiakat vegye figyelembe:

a) a használni kívánt módszer, például egy külső vagy egy belső interfészt tesztelnek, esetleg egy alternatív teszt módszert (pl. különleges esetben kód vizsgálatot) alkalmaznak,
b) az interfész(ek), melye(ke)t a tesztelésnél és a válaszok megfigyelésénél használnak,
c) a teszteléshez szükséges kezdeti feltételek (például bármely szükséges különleges objektum vagy szubjektum, a szükséges biztonsági tulajdonságokkal),
d) a teszteléshez szükséges speciális berendezések, mely vagy egy interfész aktivizálásához (pl. csomag generátorok), vagy egy interfész megfigyeléséhez (pl. hálózati analizátorok) szükségesek.

Az értékelő tesztelhet úgy is minden interfészt, hogy teszt-esetek sorozatát használja, ahol az egyes teszt-eset az adott interfészt elvárt működésének egy különleges szempontját vizsgálja.

Az értékelő tesztelési dokumentációjában ajánlott meghatározni a teszt származtatásokat, visszavezetve azokat az érintett interfész(ek)re.

ATE_IND.2-8 Az értékelőnek végre kell hajtani a tesztelést.

Az értékelő az elkészített tesztelési dokumentációt alapként használja a TOE tesztelésének végrehajtásához. Bár a végrehajtandó tesztelés alapja a tesztelési dokumentáció, az értékelő ad hoc is végezhet teszteket. A tesztelés során feltárt TOE viselkedés alapján az értékelő új teszteket is készíthet. Az új teszteket is le kell írni a dokumentációban.

ATE_IND.2-9 Az értékelőnek jelentésbe kell foglalnia a tesztkészletben szereplő tesztekről az alábbi információkat:

a) a tesztelendő interfész azonosítása;
b) a tesztekhez szükséges berendezések összekapcsolásához és beállításához tartozó utasítások;
c) a teszt előfeltételek kialakítására vonatkozó utasítások;
d) az interfész kiváltására (aktivizálására) vonatkozó utasítások;
e) az interfész működésének megfigyelésére vonatkozó utasítások;
f) az összes elvárt eredmény leírása, valamint a megfigyelt viselkedés és az elvárt eredmények összehasonlításához szükséges elemzések;
g) a tesztek lezárására és a TOE tesztelés utáni állapotának kialakítására vonatkozó utasítások;
h) tényleges teszteredmények.

A leírásnak olyan részletességűnek kell lennie, hogy egy másik értékelő képes legyen megismételni a teszteket és azonos eredményt kapjon. Míg a teszteredmények bizonyos részei eltérhetnek egymástól (pl. naplórekordok dátum és időbejegyzései), az általános eredménynek meg kell egyezni.

Lehetnek olyan esetek, amikor szükségtelen e munkaegységben minden információt megadni (például egy teszt tényleges eredménye nem követeli meg az elemzést, mielőtt az elvárt eredmények összehasonlítása nem történik meg). Ennek eldöntése és a döntés indoklása az értékelő hatásköre.

ATE_IND.2-10 Az értékelőnek ellenőriznie kell, hogy a tényleges teszteredmények megegyeznek-e az elvárt eredményekkel.

Bármilyen különbözőség az elvárt és tényleges eredmények között a TOE helytelen működését vagy a dokumentáció hibáját jelezheti. A nem várt tényleges eredmény a TOE vagy a tesztelési dokumentáció javítását, esetleg a tesztek összeállításának módosítását, bizonyos tesztek megismétlését igényelheti. Ennek eldöntése és a döntés indoklása az értékelő hatásköre.

ATE_IND.2-11 Az értékelőnek az értékelési jelentésben le kell írnia az értékelői tesztelési munkát, áttekintést adva a tesztelési módszerről, konfigurációról, mélységről és eredményekről.

Az értékelési jelentésben rögzített értékelői tesztelésről szóló információ lehetővé teszi az értékelő számára, hogy bemutassa az általános tesztelési módszert és a tesztelésbe fektetett munkát. A cél a tesztelési munka érdemi áttekintése. Nem cél, hogy az értékelési jelentésben a teszteléssel kapcsolatos információk a specifikus tesztlépések vagy egyedi tesztek eredményeinek pontos megismétlése legyenek. A cél elegendő részletesség biztosítása más értékelők és a tanúsító szervezet számára ahhoz, hogy betekintést kapjanak a választott tesztelési módszerbe, az értékelő által végrehajtott tesztek nagyságrendjébe, a fejlesztő által végrehajtott tesztek nagyságrendjébe, a TOE teszt konfigurációjába és a tesztelés általános eredményébe.

Az értékelési jelentés értékelői tesztekről szóló részében általában az alábbi információk találhatók meg:

a) TOE teszt konfigurációk. A ténylegesen tesztelt TOE konfigurációk.
b) A kiválasztott tesztelési készlet (részhalmaz) nagysága. Az értékelés során tesztelt interfészek mennyisége és ennek indoklása.
c) A részhalmazt alkotó interfészek kiválasztásának szempontjai. Rövid állítások azokról a tényezőkről, melyeket figyelembe vettek az interfészek készletbe választása során.
d) A tesztelt interfészek. Rövid felsorolása a készletbe került interfészeknek.
e) A végrehajtott fejlesztői tesztek. Ezek mennyisége és a kiválasztásukhoz használt szempontok rövid leírása.
f) A tevékenység alapján hozott határozat. Az értékelés során végzett tesztelés eredményének általános elbírálása.

E lista korántsem teljes, csupán megmutat néhány területet, melyeket az értékelői teszteléssel kapcsolatosan az értékelési jelentésben ajánlott szerepeltetni.

6.2.3.5. A Sebezhetőség felmérés garanciaosztály (AVA) értékelése

A sebezhetőség felmérés tevékenység célja a TOE üzemeltetési környezetében lévő hibák vagy gyengeségek kihasználhatóságának megállapítása. Ez a megállapítás az értékelési bizonyíték vizsgálatán, valamint az értékelő által a nyilvánosan elérhető anyagokban való keresésen alapul, és az értékelő áthatolás tesztelése támogatja ezt.

A 7.3 melléklet részletes útmutatót biztosít a sebezhetőség vizsgálat általános fogalmairól és megközelítés módjáról.

6.2.3.5.1. Sebezhetőségi elemzés: Az AVA_VAN.2 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a TOE üzemeltetési környezetében vannak-e alap támadó képességgel rendelkező támadók által kihasználható sebezhetőségek.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) TOE tervek,
d) biztonsági szerkezet leírása,
e) útmutató dokumentáció,
f) tesztelésre alkalmas TOE,
g) nyilvánosan elérhető információk a lehetséges sebezhetőségek azonosításának támogatására.

Egyéb bemenet ehhez az altevékenységhez:

a) a lehetséges sebezhetőségekre és támadásokra vonatkozó aktuális, nyilvánosan elérhető információk (pl. egy tanúsító szervezettől).

Az értékelő vegye figyelembe azokat a kiegészítő teszteket is, melyek az értékelés egyéb részeinél felmerült lehetséges sebezhetőségek eredményeként születtek.

6.2.3.5.1.1. Az AVA_VAN.2.1E értékelői akció

AVA_VAN.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

AVA_VAN.2.1C A TOE-nak alkalmasnak kell lennie tesztelésre.

AVA_VAN.2-1 Az értékelőnek meg kell vizsgálnia a TOE-t annak megállapítása érdekében, hogy a teszt konfiguráció megegyezik-e az ST-ben meghatározott, értékelés alatt álló konfigurációval.

A fejlesztő által biztosított és a teszt tervben azonosított TOE-nek ugyanazt az egyedi hivatkozást kell alkalmaznia, mint amit a „Konfiguráció kezelés képességei” (ALC_CMC) altevékenységekben fektettek le, illetve amit az ST bevezetőjében azonosítottak.

Az ST meghatározhat egynél több konfigurációt is az értékeléshez. A TOE több különálló hardver és szoftver elemből állhat, melyeket az ST-nek megfelelően kell tesztelni. Az értékelő ellenőrizze, hogy valamennyi teszt konfiguráció ellentmondás mentes-e az ST-vel.

Az értékelő vegye figyelembe azokat az ST-ben leírt, a TOE üzemeltetési környezetére vonatkozó biztonsági célokat, amelyek a teszt környezetre alkalmazhatók. Lehet hogy néhány cél nem alkalmazható a teszt környezetre. Például egy a felhasználói engedélyekkel kapcsolatos cél nem alkalmazható, míg a „csatlakozás a hálózathoz egyetlen ponton” alkalmazható.

Bármilyen tesztelési erőforrás (mérőműszer, elemző készülék) használatakor az értékelő felelőssége annak biztosítása, hogy ezek az erőforrások megfelelően hitelesítve legyenek.
AVA_VAN.2-2 Az értékelőnek meg kell vizsgálnia a TOE-t annak megállapítása érdekében, hogy azt megfelelően telepítették-e, és ismert állapotban van-e.

Az értékelő a TOE állapotát többféle módon is megállapíthatja. Például az AGD_PRE.1 altevékenység értékelésének előzetes sikeres befejezése teljesíti ezt a munkaegységet, ha az értékelő még bizonyos abban, hogy a tesztelésre használt TOE-t megfelelően telepítették és ismert állapotban van. Amennyiben nem ez a helyzet, akkor az értékelőnek a fejlesztő eljárásait kell követnie a TOE telepítéséhez és indításához, kizárólag a rendelkezésére bocsátott útmutatókra támaszkodva.

Amennyiben az értékelőnek végre kell hajtania a telepítési lépéseket, mert a TOE ismeretlen állapotban van, akkor e munkaegység sikeres befejezése kielégítheti az AGD_PRE.1-5 munkaegységet is.

6.2.3.5.1.2. Az AVA_VAN.2.2E értékelői akció

AVA_VAN.2.2E Az értékelőnek egy keresést kell végrehajtania nyilvános forrásokban a TOE lehetséges sebezhetőségeinek azonosítása érdekében.

AVA_VAN.2-3 Az értékelőnek tanulmányoznia kell a nyilvánosan rendelkezésre álló információ forrásokat a TOE lehetséges sebezhetőségeinek a meghatározása céljából.

Az értékelő tanulmányozza a nyilvánosan rendelkezésre álló információ forrásokat, amelyek rendelkezésre állnak a TOE lehetséges sebezhetőségei meghatározásainak elősegítéséhez. Sokféle nyilvánosan rendelkezésre álló információ forrás létezik, amelyeket az értékelőnek ajánlatos figyelembe vennie, felhasználva a világhálón elérhető anyagokat, beleértve a következőket:

a) szakértői publikációk (folyóiratok, könyvek);
b) tanulmányok.

Az értékelő ne korlátozza az általa figyelembevett nyilvánosan rendelkezésre álló információkat a fentiekre, hanem vegyen figyelembe bármely egyéb vonatkozó rendelkezésre álló információt.

Az értékelő az átadott bizonyítékok vizsgálata közben használja fel a nyilvános információkat abból a célból, hogy további vizsgálatokat végezzen lehetséges sebezhetőségek felkutatására. Ha az értékelő problémás területeket határozott meg, vegye figyelembe azokat a nyilvánosan rendelkezésre álló információkat, amelyek az adott problémás területre vonatkoznak.

Az olyan információk elérhetősége, amely azonnal rendelkezésre állhat egy támadó számára, s amely elősegíti támadások meghatározását és megkönnyíti a támadások hatékony végrehajtását, jelentősen megnövelheti egy adott támadó támadási lehetőségeit. A sebezhetőségi információk és kifinomult támadó eszközök hozzáférhetősége az Interneten nagyon valószínűvé teszi, hogy ezeket megpróbálják felhasználni a TOE lehetséges sebezhetőségeinek meghatározására és kihasználására. A modern kereső eszközök az ilyen információkat könnyen elérhetővé teszik az értékelő számára, és a publikált lehetséges sebezhetőségekkel, valamint a jól ismert általános támadásokkal szembeni ellenállóképesség költséghatékony módon meghatározható.

A nyilvánosan rendelkezésre álló információ keresése célirányosan azokra a forrásokra irányuljon, amelyek a TOE alapját képező termékre vonatkoznak. Az ilyen keresés terjedelme vegye figyelembe a következő tényezőket: a TOE típusa, az értékelő tapasztalatai ezzel a TOE típussal, a feltételezett támadó képesség és a rendelkezésre álló ADV bizonyíték szintje.

A meghatározási folyamat iteratív, ahol egy lehetséges sebezhetőség meghatározása egy másik problémás terület meghatározásához vezethet, amely további vizsgálatokat igényel.

Az értékelőnek jelentést kell készítenie arról, hogy mit tett a bizonyítékokban található lehetséges sebezhetőségek meghatározására. Az ilyen típusú keresésre azonban lehet, hogy az értékelő nem tudja a vizsgálat megkezdése előtt leírni a lehetséges sebezhetőségek meghatározására teendő lépéseket, mivel lehetséges, hogy a módszert a keresés során találtak alakítják.

Az értékelőnek jelentést kell készíteni a megvizsgált bizonyítékokról a lehetséges sebezhetőségekre irányuló keresés befejezésekor. A bizonyítékok kiválasztása származhat az értékelő által meghatározott olyan problémás területekből, amely a támadó által is feltehetően elérhető bizonyítékhoz kapcsolódik, vagy megfelelhet az értékelő által adott valamilyen más magyarázatnak.

6.2.3.5.1.3. Az AVA_VAN.2.3E értékelői akció

AVA_VAN.2.3E Az értékelőnek egy független sebezhetőség vizsgálatot kell végrehajtania a TOE-ra, az útmutató dokumentációt, funkcionális specifikációt, TOE tervet, és a biztonsági szerkezet leírást használva, a TOE lehetséges sebezhetőségeinek azonosítása érdekében.

AVA_VAN.2-4 Az értékelőnek egy keresést kell folytatnia az ST-re, az útmutató dokumentációra, a funkcionális specifikációra, a TOE tervre és a biztonsági szerkezet leírásra vonatkozóan abból a célból, hogy meghatározza a TOE-ban esetlegesen előforduló lehetséges sebezhetőségeket.

A bizonyítékokban való keresést a TOE-ra vonatkozó tervek és dokumentációk vizsgálata során kell teljesíteni, majd pedig feltételezéseket vagy találgatásokat kell tenni a TOE lehetséges sebezhetőségeit illetően. Ezután a feltételezett lehetséges sebezhetőségeket fontossági sorrendbe kell állítani az alábbiak alapján: a sebezhetőség fennállásának becsült valószínűsége, a kiaknázásához szükséges támadó képesség (feltételezve, hogy fennáll a sebezhetőség), az általa elérhető felügyelet vagy veszélyeztetés mértéke.

A biztonsági szerkezet leírás szolgáltatja a fejlesztő sebezhetőség vizsgálatát, minthogy ez dokumentálja, hogy a TSF hogyan védi saját magát a nem-megbízható szubjektumokkal szemben, és hogyan akadályozza meg a biztonságot érvényre juttató funkcionalitás megkerülését. Ennélfogva az értékelő a TSF lehetséges aláaknázási módszerei keresésének alapjaként használja ezt a leírást a TSF védelméről.

Azoktól az SFR-ektől függően, amelyeket a TOE-nak teljesítenie kell az üzemeltetési környezetben, az értékelő független sebezhetőség vizsgálata vegye tekintetbe az általános lehetséges sebezhetőségeket az alábbi fejezetcímek mindegyike alatt:

a) az értékelés alatt álló TOE típusára vonatkozó általános lehetséges sebezhetőségek, amint ilyeneket a tanúsító szervezet szolgáltathat;
b) megkerülés;
c) hamisítás;
d) közvetlen támadások;
e) megfigyelés;
f) helytelen használat/visszaélés.

A b) - f) tételeket részletesen magyarázza a 7.3 melléklet.

A biztonsági szerkezet leírást a fenti általános lehetséges sebezhetőségek szem előtt tartása mellett kell mérlegelni. Minden lehetséges sebezhetőséget mérlegelni kell azon lehetséges módok felkutatására, amelyekkel a TSF védelmet hatálytalanítani, a TSF-et aláaknázni lehet.

AVA_VAN.2-5 Az értékelőnek az ETR-ben rögzítenie kell a meghatározott lehetséges sebezhetőségeket, amelyek tesztelhetők, és a TOE üzemeltetési környezetében szóba jöhetnek.

Nem szükséges a lehetséges sebezhetőségek további mérlegelése, ha az értékelő azt állapítja meg, hogy az üzemeltetési környezetben meglévő IT vagy nem-IT intézkedések meggátolják a lehetséges sebezhetőségek kiaknázását az adott üzemeltetési környezetben. Például, ha a TOE-hoz való fizikai hozzáférés kizárólag a jogosult felhasználókra van korlátozva, akkor ez a hamisítás lehetséges sebezhetőségét eredményesen nem kihasználhatóvá teheti.

Az értékelőnek minden okot rögzítenie kell a lehetséges sebezhetőségek további mérlegelésből való kizárására, ha azt állapítja meg, hogy a lehetséges sebezhetőség nem kerülhet szóba az üzemeltetési környezetben. Egyéb esetekben az értékelőnek a lehetséges sebezhetőséget további mérlegelésre rögzítenie kell.

Az értékelőnek az ETR-ben meg kell adnia a TOE-val kapcsolatos, annak üzemeltetési környezetében felmerülő lehetséges sebezhetőségek listáját, mely az áthatolás tesztelési tevékenység bemeneteként használható.

6.2.3.5.1.4. Az AVA_VAN.2.4E értékelői akció

AVA_VAN.2.4E Az értékelőnek az azonosított lehetséges sebezhetőségek alapján áthatolás tesztelést kell végrehajtania, annak megállapítása érdekében, hogy a TOE ellenáll egy alap támadó képességgel bíró támadó által végrehajtott támadásnak.

AVA_VAN.2-6 Az értékelőnek a lehetséges sebezhetőségekre irányuló független keresés alapján meg kell terveznie az áthatolás teszteket.

Az értékelőnek kellően fel kell készülnie az áthatolás tesztelésre annak megállapítása érdekében, hogy a TOE üzemeltetési környezetében mennyire érzékeny azokra a lehetséges sebezhetőségekre, melyeket a nyilvánosan elérhető információ forrásokban való keresés során azonosított. Az értékelőnek figyelembe kell vennie bármely harmadik féltől (pl. tanúsító szervezet) kapott, ismert lehetséges sebezhetőségre vonatkozó aktuális információt, valamint a más értékelői tevékenységek eredményeként talált lehetséges sebezhetőségeket is.

Az értékelőnek szem előtt kell tartania, hogy ugyanúgy, mint a biztonsági szerkezet leírás mérlegelése esetében a sebezhetőségek felkutatásánál (ahogyan az AVA_VAN.2-3-ben részletezve van), tesztelést kell végrehajtania a szerkezeti tulajdonságok megerősítésére. Ez valószínűleg negatív teszteket igényel, amelyek a biztonsági szerkezet tulajdonságainak megcáfolását kísérlik meg. Az áthatolás tesztelés stratégiájának kialakításakor az értékelőnek garantálnia kell, hogy a biztonsági szerkezet leírás minden főbb jellegzetessége tesztelésre kerüljön vagy a funkcionális tesztelésnél, vagy az értékelői áthatolás tesztelésnél.

Az áthatolás tesztelést az értékelő valószínűleg tesztesetek sorozatával találja célszerűnek elvégezni, ahol az egyes tesztesetek egy-egy adott lehetséges sebezhetőséget próbálnak ki.

Az értékelőre nézve nem elvárás, hogy teszteket végezzen azokon a lehetséges sebezhetőségeken (beleértve a nyilvánosan ismerteket is) túlmutatóan, melyek

kihasználásához alap támadó képesség szükséges. Egyes esetekben azonban még a kihasználhatóság meghatározása előtt szükség lehet egy teszt végrehajtására. Amennyiben értékelői tapasztalata segítségével az értékelő egy alap támadó képesség felett álló kihasználható sebezhetőséget tár fel, ezt az értékelési jelentésében maradvány sebezhetőségként szerepeltetnie kell.

Egy adott lehetséges sebezhetőség kihasználásához szükséges támadó képesség meghatározásához útmutató található a 7.3.4 pontban.

Az olyan lehetséges sebezhetőségek, melyek feltételezhetően csak megemelt-alap, közepes vagy magas támadó képességgel kihasználhatók, nem eredményeznek „nem felelt meg" eredményt erre az értékelői tevékenységre. Amennyiben vizsgálat támogatja a fenti feltételezést, az érintett lehetséges sebezhetőséget a továbbiakban nem szükséges az áthatolás tesztelés bemeneteként kezelni. Ugyanakkor az ilyen sebezhetőséget az értékelési jelentésben maradvány sebezhetőségként szerepeltetni kell.

Az olyan lehetséges sebezhetőségeket, melyek feltételezhetően alap támadó képességgel kihasználhatók, és a biztonsági célok megsértését eredményezik, a legnagyobb elsőbbséggel ajánlott a lehetséges sebezhetőségek azon listájára felvenni, mely alapján a TOE közvetlen áthatolás tesztelését végzik.

AVA_VAN.2-7 Az értékelőnek a lehetséges sebezhetőségek listáján alapulva el kell készítenie az áthatolás tesztelési dokumentációt, a tesztek megismételhetőségét lehetővé tévő részletességgel. A tesztelési dokumentációnak tartalmaznia kell az alábbiakat:

a) a lehetséges sebezhetőség azonosítását, melyre a TOE-t tesztelik;
b) az áthatolás teszteléshez szükséges minden tesztberendezés csatlakoztatását és beállítását előíró utasítást;
c) az áthatolás tesztelés összes kezdeti előfeltételét kialakító utasításokat;
d) a TSF működését kiváltó utasításokat;
e) a TSF viselkedése megfigyeléséhez szükséges utasításokat;
f) minden várható eredmény leírását, valamint a várható eredményekkel való összehasonlításhoz végrehajtandó, megfigyelt működésre vonatkozó elemzéseket;
g) a tesztek befejezéséhez szükséges és a TOE tesztelés utáni állapotát biztosító utasításokat.

Az értékelőnek a lehetséges sebezhetőségek listáján alapulva el kell készítenie az áthatolás tesztelési dokumentációt, a tesztek megismételhetőségét lehetővé tévő részletességgel.

Az értékelőre nézve nem elvárás, hogy meghatározza a kihasználhatóságát azon lehetséges sebezhetőségeknek, melyek hatásos támadásához alap feletti támadó képesség szükséges. Ugyanakkor értékelői tapasztalata segítségével az értékelő feltárhat olyan lehetséges sebezhetőséget, melyet csak olyan támadó használhat ki, aki magasabb mint alap támadó képességgel rendelkezik. Az ilyen sebezhetőségeket az értékelési jelentésében maradvány sebezhetőségként szerepeltetni kell.

A lehetséges sebezhetőség ismeretében az értékelő határozza meg a leginkább megfelelő módot a TOE érzékenységének kimutatásához. Az értékelő különösen az alábbiakat vegye tekintetbe:

a) a TSFI és más TOE interfészeket, melyeket a TSF kiváltására és a válaszok megfigyelésére használnak (Lehet, hogy az értékelőnek egy TSFI-n kívüli TOE interfészt szükséges használnia a TOE azon tulajdonságainak demonstrálására, melyeket (az ADV_ARC által megkövetelt) biztonsági szerkezet leírás ír le. Megjegyzendő, hogy bár ezek a TOE interfészek lehetőséget adnak a TSF tulajdonságok tesztelésére, nem képezik tárgyát a tesztelésnek);
b) azokat a kezdeti feltételeket, melyek a tesztekhez szükségesek (azaz bármilyen szükséges objektum vagy szubjektum, illetve ezek szükséges biztonsági tulajdonságai);
c) speciális tesztberendezések, amelyek egy TSFI kiváltásához vagy megfigyeléséhez szükségesek (bár nem valószínű, hogy egy alap támadó képességet feltételező lehetséges sebezhetőség speciális tesztberendezést igényel);
d) bár elméleti vizsgálat helyettesítheti a fizikai tesztelést, különösen fontos eset, amikor egy kezdeti teszt eredményeként előre jelezhető, hogy egy támadás adott számú megismétlése valószínűleg sikeres lesz.

Az értékelő az áthatolás tesztelést valószínűleg tesztesetek sorozatával találja célszerűnek elvégezni, ahol az egyes tesztesetek egy-egy adott lehetséges sebezhetőséget próbálnak ki.

A tesztelési dokumentáció ilyen szintű részletessége azt hivatott biztosítani, hogy más értékelők is meg tudják ismételni a teszteket, és azonos eredményre juthassanak.

AVA_VAN.2-8 Az értékelőnek végre kell hajtania az áthatolás tesztelést.

Az értékelő az AVA_VAN.2-6 munkaegység eredményeképpen létrejött áthatolás tesztelési dokumentációt a TOE áthatolás tesztelésének alapjaként használja, de ez nem zárja ki, hogy más, ad hoc áthatolás tesztelést ne végezhessen el. Amennyiben szükséges, az értékelő ad hoc teszteket is elvégezhet az áthatolás tesztelés során tapasztaltak következtében, melyeket – ha az értékelő elvégzi azokat - az áthatolás tesztelési dokumentációban rögzítenie kell. E tesztekkel szemben követelmény lehet, hogy a nem várt eredményeket vagy megfigyeléseket ellenőrizzék, vagy hogy a tesztelés előkészítési szakaszában az értékelőnek javasolt lehetséges sebezhetőségeket megvizsgálják.

Amennyiben az áthatolás tesztelés azt mutatja, hogy egy feltételezett lehetséges sebezhetőség nem létezik, az értékelőnek ajánlott megállapítania, hogy a saját elemzése volt téves, vagy az értékelésre átadandók voltak hibásak, hiányosak.

Az értékelőre nézve nem elvárás, hogy teszteket végezzen azokon a lehetséges sebezhetőségeken (beleértve a nyilvánosan ismerteket is) túlmutatóan, melyek kihasználásához alap támadó képesség szükséges. Egyes esetekben azonban még a kihasználhatóság meghatározása előtt szükség lehet egy teszt végrehajtására. Amennyiben értékelői tapasztalata segítségével az értékelő egy alap támadó képesség felett álló kihasználható sebezhetőséget tár fel, ezt az értékelési jelentésében maradvány sebezhetőségként szerepeltetnie kell.

AVA_VAN.2-9 Az értékelőnek rögzítenie kell az áthatolás tesztek tényleges eredményeit.

A tényleges eredmények bizonyos részletei különbözhetnek a várható értékektől (pl. idő és dátummezők a naplóban), de az összeredménynek meg kell egyeznie. Javasolt minden váratlan teszteredményt kivizsgálni, valamint ezek értékelésre gyakorolt hatását kimondani és igazolni.

AVA_VAN.2-10 Az értékelőnek az értékelési jelentés keretén belül jelentést kell írnia az értékelői áthatolás tesztelésről, leírván a tesztelési módszert, konfigurációt, mélységet és eredményeket.

Az értékelési jelentésben rögzített áthatolás tesztelésről szóló információ lehetővé teszi az értékelő számára, hogy bemutassa az általános tesztelési módszert és az ezen tevékenység végrehajtásába fektetett munkát. A cél az értékelő áthatolás tesztelési munkájának érdemi áttekintése. Nem cél, hogy az értékelési jelentésben az áthatolás teszteléssel kapcsolatos információk a specifikus tesztlépések vagy egyedi áthatolás tesztek eredményeinek pontos megismétlése legyenek. A cél elegendő részletesség biztosítása más értékelők és a tanúsító szervezet számára ahhoz, hogy betekintést kapjanak a választott áthatolás tesztelési módszerbe, a végrehajtott áthatolás tesztek nagyságrendjébe, a TOE teszt konfigurációjába és az áthatolás tesztelési tevékenység általános eredményébe.

Az értékelési jelentés értékelői áthatolás tesztelésről szóló része általában az alábbi információkat tartalmazza:

a) TOE tesztkonfigurációk; az áthatolás tesztelésnél használt konkrét TOE konfigurációk.
b) Az áthatolás teszt során tesztelt TSFI-k. Az áthatolás tesztelés középpontjában álló TSFI-k és egyéb TOE interfészek rövid felsorolása.
c) Az altevékenység alapján született határozat. Az áthatolás tesztelés eredményeinek általános megítélése.

E lista korántsem teljes, csupán felvillant néhány szempontot, melyeknek az értékelő áthatolás tesztelésével kapcsolatosan az értékelési jelentésben ajánlott szerepelniük.
AVA_VAN.2-11 Az értékelőnek meg kell vizsgálnia az összes áthatolás teszt eredményét annak megállapítása érdekében, hogy a TOE üzemeltetési környezetében ellenáll-e egy alap támadó képességgel rendelkező támadónak.

Amennyiben az eredmények azt mutatják, hogy a TOE üzemeltetési környezetében kihasználható sebezhetőségeket tartalmaz alap támadó képességgel rendelkező támadók számára, akkor ez az értékelői akció "Nem felelt meg" határozatot eredményez.

A 7.3.4 mellékletet kell használni egy adott sebezhetőség kihasználásához szükséges támadó képesség meghatározásához, illetve annak eldöntésére, hogy a sebezhetőség a tervezett üzemeltetési környezetben kihasználható-e. Nem feltétlenül kell minden esetben kiszámolni a támadó képességet, csak ha felmerül annak lehetősége, hogy egy alap támadó képességgel rendelkező támadó kihasználhatja a sebezhetőséget.

AVA_VLA.2-12 Az értékelőnek az értékelési jelentés keretén belül jelentést kell írnia az összes kihasználható sebezhetőségről és maradvány sebezhetőségről, az alábbi adatokkal:

a) forrás (pl. azon CEM tevékenység, melynek végrehajtása során észlelték, az értékelő ismerte, szakirodalomban olvasott róla);

b) a nem kielégített SFR(-ek);
c) leírás;
d) kihasználható-e vagy sem az üzemeltetési környezetben (vagyis kihasználható vagy maradvány sebezhetőségről van szó);
e) az azonosított sebezhetőség kihasználáshoz szükséges felhasznált idő, szakértelem, TOE ismeret, hozzáférési lehetőség, eszköz, valamint az ezekhez rendelt értékek a 7.3.4 melléklet 8. és 9. táblázata alapján.

6.2.4. Termék értékelés fokozott garanciaszinten

6.2.4.1. A Fejlesztés garanciaosztály (ADV) értékelése

A fejlesztési tevékenységnek az a célja, hogy a terv dokumentációt felmérje abból a szempontból, hogy az megfelelő-e annak megértéséhez, hogy a TSF hogyan teljesíti az SFR-eket, és hogy az SFR-ek megvalósítását nem lehet meghamisítani vagy megkerülni. Ezt a megértést a TSF terv dokumentációhoz tartozó egyre részletesebb leírások vizsgálatán keresztül lehet elérni. A terv dokumentáció a funkcionális specifikációból (ami a TSF interfészeit írja le), a TOE tervből (ami a TSF szerkezetét írja le abból a szempontból, hogy az hogyan működik a megkívánt SFR-ekhez kapcsolódó funkciók végrehajtása érdekében) és egy megvalósítási leírásból (forráskód szintű leírás) áll. (A fokozott garanciaszint nem tartalmaz megvalósításra vonatkozó követelményeket.) Ezenfelül létezik egy biztonsági szerkezet leírás, amely a TSF szerkezeti tulajdonságait ismerteti annak kifejtése céljából, hogy ennek biztonsági szempontú érvényre jutását nem lehet meghamisítani vagy megkerülni.

A terv dokumentációra vonatkozó CC követelmények szintjei aszerint különböznek, hogy mennyi és milyen részletes információt kell biztosítani, milyen mértékű formalizmussal. Az alacsonyabb szinteken a TSF biztonság szempontból legkritikusabb részeit a legnagyobb részletességgel kell ismertetni, míg a biztonság szempontjából kevésbé fontos részeket csak összegezni kell; további garancia nyerhető azáltal, ha növelik a TSF biztonság szempontból legkritikusabb részeire vonatkozó információk mennyiségét, és ha növelik a kevésbé fontos részekre vonatkozó részleteket. A legnagyobb garancia akkor érhető el, ha minden részre vonatkozóan mélyreható részleteket és információkat adnak meg.

A CC a dokumentumok formalizmusának a mértékét (vagyis azt, hogy a dokumentum informális-e vagy félformális) hierarchikusnak tekinti. Informális az a dokumentum, amelyet természetes nyelven fejeztek ki. A módszertan nem ír elő kötelezően használandó meghatározott nyelvet; ez a kérdés a sémára van hagyva. A következő fejezetek a különböző informális dokumentumok tartalmát ismertetik.

Egy funkcionális specifikáció leírást nyújt a TSF-hez kapcsolódó interfészek rendeltetéséről és használati módjáról. Például, ha egy operációs rendszer eszközt biztosít a felhasználó számára az ön-azonosításra, fájlok létrehozására, fájlok módosítására vagy törlésére, olyan engedélyek beállítására, amelyek meghatározzák, hogy mely egyéb felhasználók férhetnek hozzá fájlokhoz, és eszközt biztosít a távoli gépekkel való kommunikációra, akkor az operációs rendszer funkcionális specifikációjának tartalmaznia kell mindezeknek az ismertetését, és azt, hogy ezeket hogyan valósítják meg a TSF-hez csatlakozó kívülről látható interfészeken keresztüli kölcsönhatások. Ha létezik egy naplózási funkcionalitás is, amely

észleli és rögzíti az ilyen események előfordulásait, akkor az is elvárás, hogy ez a naplózási funkcionalitás része legyen a funkcionális specifikációnak; és bár ezt a funkcionalitást technikailag nem közvetlenül a felhasználó idézi elő a külső interfészen, biztosan kihat erre az, ami a felhasználói külső interfészen történik.

A terv leírást logikai alkotóelemek (alrendszerek vagy modulok) szerint fejezik ki, amelyek mindegyike egy érthető szolgáltatást vagy funkciót biztosít. Például egy tűzfal állhat olyan alrendszerekből, amelyek csomagszűréssel, távoli adminisztrációval, naplózással és kapcsolat-szintű szűréssel foglalkoznak. A tűzfal terv leírásnak ekkor ismertetnie kell, hogy az egyes alrendszerek milyen tevékenységeket hajtanak végre, amikor egy bejövő csomag megérkezik a tűzfalhoz.

6.2.4.1.1. Biztonsági szerkezet: Az ADV_ARC.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak a megállapítása, hogy a TSF olyan módon van-e megszerkesztve, hogy azt nem lehet meghamisítani vagy megkerülni, és hogy a biztonsági tartományokat biztosító TSF-ek a szóbanforgó tartományokat elkülönítik-e egymástól.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) TOE terv,
d) biztonsági szerkezet leírás,
e) üzemeltetési felhasználói útmutató.

Az önvédelem, a tartomány szétválasztás és a nem-megkerülhetőség elveit elkülönítik attól a biztonsági funkcionalitástól, melyet a CC 2. részbeli SFR-ek fejeznek ki, minthogy az önvédelem és nem-megkerülhetőség egyáltalán nem rendelkezik közvetlenül megfigyelhető interfésszel a TSF-en. Ezek inkább olyan tulajdonságai a TSF-nek, amelyeket a TOE és TSF tervezésén keresztül valósítanak meg, és amelyeket a szóbanforgó terv helyes megvalósításával juttatnak érvényre. Ezenfelül ezen tulajdonságok értékelése kevésbé célirányos, mint a mechanizmusok értékelése; egy funkcionalitásnak a hiányát sokkal nehezebb ellenőrizni, mint a meglétét. Annak a megállapítása azonban, hogy ezek a tulajdonságok teljesülnek, éppen olyan kritikus, mint annak a megállapítása, hogy egy mechanizmust helyesen valósítottak meg.

Az általánosan alkalmazott megközelítési mód szerint a fejlesztő biztosítja a fent említett tulajdonságokat teljesítő TSF-et, és bizonyítékot is átad (dokumentáció formájában), amelyet megvizsgálásával belátható, hogy a tulajdonságok valóban teljesülnek. Az értékelő felelőssége, hogy megtekintse a bizonyítékot, a TOE-hoz és TSF-hez átadott egyéb bizonyítékokkal társítva, és megállapítsa, hogy a tulajdonságok megvalósulnak-e. A munkaegységek jellemezhetők úgy, hogy vannak olyanok, amelyek azzal foglalkoznak, hogy milyen információt kell átadni, és vannak olyanok, amelyek az értékelő által végrehajtott tényleges vizsgálatokkal foglalkoznak.

A biztonsági szerkezet leírás ismerteti, hogy a biztonsági tartományokat hogyan definiálták, és a TSF hogyan tartja fenn ezek elkülönülését. Ismerteti, hogy mi gátolja meg a nem-megbízható eljárásokat abban, hogy hozzájussanak a TSF-hez és módosítsák azt. Ismerteti,

hogy mi garantálja azt, hogy a TSF ellenőrzése alá tartozó minden erőforrás megfelelő módon védve van, és hogy minden SFR-vonatkozású tevékenységet a TSF közvetít. Megmagyaráz minden szerepet, amit a környezet tölt be ezek valamelyikénél (pl. hogyan történik a biztonsági funkcionalitás aktivizálása, feltételezve, hogy a tevékenységet az alátámasztó környezet helyesen aktivizálja?). Röviden, megmagyarázza, hogy a TOE az elgondolások szerint hogyan fog valamilyen biztonsági szolgáltatást nyújtani.

Az értékelők által végrehajtott vizsgálatokat a TOE-hoz átadott minden fejlesztői bizonyítékkal kapcsolatban olyan részletesen kell elvégezni, ahogyan az adott bizonyítékot szolgáltatták. A fokozott garanciaszinten nem lehet elvárás, hogy a TSF önvédelmet teljesen megvizsgálják, minthogy csak magas szintű terv reprezentációk állnak rendelkezésre. Az értékelőnek minden bizonnyal vizsgálatai egyéb részeiből nyert információk felhasználására is szüksége lesz (pl. a TOE terv vizsgálata), amikor a következő munkaegységeknél vizsgálandó tulajdonságok felbecsülését végzi.

6.2.4.1.1.1. Az ADV_ARC.1.1E értékelői akció

ADV_ARC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ADV_ARC.1.1C A biztonsági szerkezet leírást olyan szinten kell részletezni, amely összemérhető a TOE terv dokumentációban ismertetett, SFR-t érvényre juttató absztrakciók leírásával.

ADV_ARC.1-1 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy az ebben biztosított információk részletessége összemérhető-e a TOE terv dokumentációban és a funkcionális specifikációban ismertetett, SFR-t érvényre juttató absztrakciók leírásával.

A funkcionális specifikáció vonatkozásában az értékelő győződjön meg arról, hogy az ismertetett önvédelmi funkcionalitás lefedi-e azokat a hatásokat, amelyek nyilvánvalóak a TSFI-n. Egy ilyen leírás magában foglalhatja a TSF futtatható formáira, illetve az objektumokra (pl. TSF által használt fájlok) elhelyezett védelmet. Az értékelő győződjön meg arról, hogy a TSFI-n keresztül aktivizálható funkcionalitást leírták.

Az értékelő győződjön meg arról, hogy a biztonsági szerkezet leírása tartalmaz-e információt a TSF tartomány elkülönítéshez hozzájáruló egyes alrendszerei működésmódjáról.

Az ehhez a munkaegységhez kapcsolódó értékelői akció kapjon „nem felelt meg” határozatot, ha a biztonsági szerkezet leírás megemlít bármilyen olyan modult, alrendszert vagy interfészt, amelyet a funkcionális specifikáció vagy a TOE terv dokumentum nem ismertet.

ADV_ARC.1.2C A biztonsági szerkezet leírásnak ismertetnie kell a TSF által kezelt biztonsági tartományokat, összhangban az SFR-ekkel.

ADV_ARC.1-2 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy az ismerteti-e a TSF által kezelt biztonsági tartományokat.

A biztonsági tartományok olyan környezetekre vonatkoznak, amelyeket a TSF nyújt potenciálisan kárt-okozó egyedek általi használatra; például, egy tipikus biztonságos operációs rendszer számos erőforrást nyújt olyan eljárások számára, amelyek korlátozott hozzáférési jogokkal és biztonsági tulajdonságokkal rendelkeznek. Az értékelő állapítsa meg, hogy a biztonsági tartományok fejlesztői leírása minden olyan SFR-t figyelembe vesz, amit a TOE megkíván.

Bizonyos TOE-k esetében nem léteznek ilyen tartományok, mivel a felhasználók számára rendelkezésre álló minden kölcsönhatást szigorúan a TSF tartalmaz. Ilyen TOE-ra példa egy csomag-szűrő tűzfal. A LAN-on vagy WAN-on lévő felhasználók nem lépnek kölcsönhatásba a TOE-val, így nincsen szükség biztonsági tartományokra; csak a TSF által kezelt adat-struktúrák szolgálnak arra, hogy a felhasználói csomagokat elkülönítetten tartsák. Az értékelő győződjön meg arról, hogy minden olyan állítás, hogy nincsen biztonsági tartomány, alá van támasztva bizonyítékkal, és győződjön meg arról is, hogy ilyen tartományok valóban nem állnak rendelkezésre.

ADV_ARC.1.3C A biztonsági szerkezet leírásnak ismertetnie kell, hogy a TSF inicializálási eljárása milyen mértékben biztonságos.

ADV_ARC.1-3 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy a TSF inicializálási eljárása megőrzi a biztonságot.

A TSF inicializálására vonatkozó, a biztonsági szerkezet leírásban megadott információ azokra a TOE összetevőkre irányul, amelyek közreműködnek abban, hogy a TSF-et egy kezdeti biztonságos állapotba hozzák (vagyis amikor a TSF-nek már minden része működőképes), bekapcsoláskor vagy reset esetén. A biztonsági szerkezet leírásban ez a fejtegetés sorolja fel azokat a rendszer-inicializálási összetevőket és feldolgozásokat, amelyek érintve vannak a „kikapcsolt” állapotból a kezdeti biztonságos állapotba való átmenet során.

Gyakran fordul elő az az eset, hogy az inicializálási funkciót ellátó összetevők a biztonságos állapot elérése után már nem állnak rendelkezésre; ebben az esetben a biztonsági szerkezet leírás határozza meg ezeket az összetevőket, és magyarázza meg, hogy milyen mértékben igaz az, hogy nem-megbízható egyedek nem tudják elérni ezeket a TSF felállása után. Ebben a vonatkozásban az a tulajdonság, amelyet fenn kell tartani, az, hogy 1) a biztonságos állapot elérése után nem-megbízható egyedek nem férhetnek hozzá ezekhez az összetevőkhöz, vagy pedig 2) ha ezek az összetevők nyújtanak is interfészeket nem-megbízható egyedek számára, akkor ezek a TSFI-k nem használhatók a TSF működésébe történő hamisításra.

A TSF inicializálásához kapcsolódó TOE összetevők a TSF inicializálását követően a TSF részeként kezelik magukat, és ebből a nézőpontból vizsgálandók. Meg kell jegyezni, hogy még ha ezeket a TSF részeként is kezelik, valószínűleg megindokolható, hogy ezeknek nem kell teljesíteni az ADV_INT belső szerkezeti követelményeket (ahogyan az ADV_INT erre lehetőséget nyújt).

ADV_ARC.1.4C A biztonsági szerkezet leírásnak szemléltetnie kell, hogy a TSF megvédi magát a hamisítással szemben.

ADV_ARC.1-4 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy az kellő információt biztosít annak megállapításához, hogy a TSF képes megvédi magát a nem-megbízható aktív egyedek hamisításával szemben.

Az „önvédelem” a TSF-nek arra a képességére utal, hogy meg tudja védeni saját magát a külső egyedek olyan manipulációival szemben, amelyek a TSF megváltoztatásaihoz vezethetnek. A más IT egyedektől függő TOE-k esetében gyakran előfordul, hogy a TOE olyan szolgáltatást használ fel funkciói végrehajtásához, amelyeket más IT egyedek szolgáltatnak. Az ilyen esetekben a TSF önmagában nem tudja megvédeni saját magát, mivel más IT egyedektől függ az, hogy valamilyen védelmet tud biztosítani. A biztonsági szerkezet leírás szempontjából az önvédelem elve csak azokra a szolgáltatásokra vonatkozik, amelyeket a TSF nyújt a TSFI-ken keresztül, és nem vonatkozik azokra a szolgáltatásokra, amelyeket az általa használt támogató IT egyedek szolgáltatnak.

Az önvédelem általában számos eszközzel elérhető, a TOE-hoz való hozzáférés fizikai és logikai korlátozásától kezdődően a hardver-alapú (pl. memóriakezelési funkcionalitás) és szoftver-alapú (pl. bemenetek korlát-érték ellenőrzései egy megbízható szerveren) eszközökig. Az értékelő állapítsa meg, hogy minden ilyen mechanizmus ismertetve lett.

Az értékelő állapítsa meg, hogy a terv leírás lefedi azt, hogy a TSF hogyan kezeli a felhasználói bemenetet abból a szempontból, hogy az ne ronthassa le a TSF-et. Például a TSF megvalósíthatja a privilégium elvét és megvédheti magát azzal, hogy privilegizált-módban futó rutinokat alkalmaz a felhasználói bemenetek kezelésére. A TSF hasznosíthatja az olyan processzor-alapú elkülönítési mechanizmusokat, mint amilyenek a privilégium szintek vagy gyűrűk. A TSF megvalósíthat olyan szoftver védelmi szerkezeteket vagy kódolási konvenciókat, amelyek hozzájárulnak a szoftver tartományok elkülönítésének megvalósításához, feltehetően azzal, hogy a felhasználói címteret elhatárolják a rendszer címtértől. Ezenfelül a TSF bízhat abban, hogy a környezet biztosít bizonyos védelmet.

A tartomány elválasztási funkciókhoz hozzájáruló összes mechanizmust le kell írni. Az értékelő mindazokat az ismereteket, amelyeket más bizonyítékokból (fokozott garanciaszinten: funkcionális specifikáció, TOE terv és a biztonsági szerkezet egyéb részeinek leírása) szerzett meg, használja fel annak megállapításánál, hogy az önvédelemhez hozzájáruló minden olyan funkcionalitást is ismertettek, amely a biztonsági szerkezet leírásban nem szerepel.

Az önvédelmi mechanizmusok leírásának helyessége az a tulajdonság, hogy a leírás hitelt érdemlően ismerteti, hogy mit valósítottak meg. Az értékelő használjon fel egyéb bizonyítékokat (fokozott garanciaszinten: funkcionális specifikáció, TOE terv és a biztonsági szerkezet egyéb részeinek leírása) annak megállapításához, hogy az önvédelmi mechanizmus leírásai ellentmondanak-e egymásnak. Ha egy értékelő nem látja át, hogy egy meghatározott önvédelmi mechanizmus hogyan működik, vagy hogyan működne a rendszer architektúrában, lehetséges, hogy ez egy olyan eset, amikor a leírás nem helyes.

ADV_ARC.1.5C A biztonsági szerkezet leírásnak szemléltetnie kell, hogy a TSF meggátolja az SFR-t érvényre juttató funkcionalitás megkerülését.

ADV_ARC.1-5 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy az bemutat-e olyan vizsgálatot, ami megfelelő módon ismerteti, hogy az SFR-t érvényre juttató mechanizmusokat milyen mértékben nem lehet megkerülni.

A nem-megkerülhetőség egy olyan tulajdonság, hogy a TSF biztonsági funkcionalitása (ahogyan azt az SFR-ek specifikálják) mindig működésbe lép. Például, ha a fájlokhoz való hozzáférés a TSF-nek az egyik, SFR-en keresztül specifikált tulajdonsága, akkor nem szabad előfordulnia olyan interfésznek, amin keresztül a fájlokhoz hozzá lehet férni a TSF hozzáférés ellenőrzési mechanizmusa aktivizálása nélkül (vagyis nem szabad előfordulnia például olyan interfésznek, amelyen keresztül közvetlenül hozzá lehet férni egy diszkhez).

Annak leírása, hogy a TSF mechanizmusokat miért nem lehet megkerülni, általában módszeres indoklást igényel a TSF-en és a TSFI-ken alapulva. Annak leírása, hogy a TSF hogyan működik (amit a terv lebontási bizonyítékok, vagyis a funkcionális specifikáció és TOE terv dokumentáció tartalmaznak) – a TSS-ben foglalt információ mellett – biztosítja a szükséges hátteret ahhoz, hogy az értékelő megértse, hogy mely erőforrásokat kell védeni, és milyen biztonsági funkciókat kell biztosítani. A funkcionális specifikáció adja meg a TSFI-k ismertetését, amelyeken keresztül az erőforrások/funkciók hozzáférhetők.

Az értékelő becsülje fel az átadott leírásokat (és a fejlesztő által biztosított egyéb információkat, mint például a funkcionális specifikáció), hogy meggyőződjön arról, hogy nem áll rendelkezésre olyan interfész, amelyet a TSF megkerülésére lehetne használni. Ez azt jelenti, hogy az egyes interfészeknek vagy nem szabad kapcsolatban állniuk az ST-ben előírt SFR-ekkel (és nem szabad kölcsönhatásban lenniük semmi olyannal sem, amit felhasználnak az SFR-ek kielégítésére), vagy a más fejlesztői bizonyítékokban leírt biztonsági funkcionalitást az ismertetett módon kell használniuk. Például egy játék valószínűleg nem áll kapcsolatban az SFR-ekkel, így meg kell magyarázni, hogy miért nem befolyásolja a biztonságot. A felhasználói adatokhoz való hozzáférés azonban feltehetően kapcsolatban áll hozzáférés ellenőrzési SFR-ekkel, így a magyarázatnak ismertetnie kell azt, hogy a biztonsági funkcionalitás hogyan működik, amikor az adathozzáférési interfészeken keresztül aktivizálódik. Ilyen leírás szükséges minden elérhető interfészre.

Leírásra példa a következő. Tegyük fel, hogy a TSF fájlvédelmet biztosít. Tegyük fel továbbá, hogy bár a „hagyományos” TSFI megnyitási, olvasási és írási rendszerhívások aktivizálják a TOE tervben ismertetett fájlvédelmi mechanizmusokat, létezik egy TSFI, amely hozzáférést biztosít egy batch job lehetőséghez (batch job-ok létrehozása, job-ok törlése, nem végrehajtott job-ok módosítása). Az értékelőnek a megbízó által biztosított leírásból dönteni kell tudnia arról, hogy a szóbanforgó TSFI ugyanazt a védelmi mechanizmust aktivizálja-e, mint a „hagyományos” interfészek. Ez elérhető például a TOE terv megfelelő részeire való hivatkozással, amely azt tárgyalja, hogy a batch job lehetőséggel rendelkező TSFI hogyan valósítja meg biztonsági céljait.

Ugyanezen példát használva tételezzük fel, hogy létezik egy TSFI, amelynek az egyetlen célja, hogy kijelezze az időpontot. Az értékelő állapítsa meg, hogy a leírás megfelelő módon bizonyítja, hogy ez a TSFI nem képes egyetlen védett erőforrás manipulálására sem, és nem aktivizálhat egyetlen biztonsági funkcionalitást sem.

A megkerülésre egy másik példa az, amikor feltételezik, hogy a TSF megőrzi egy kriptográfiai kulcs bizalmasságát (ami felhasználható kriptográfiai műveletekhez, de amit nem szabad írni és olvasni). Ha egy támadó közvetlenül fizikailag hozzáfér az eszközhöz, képes lehet arra, hogy oldal-csatornákat vizsgáljon -mint például az eszköz áramfelvételét, az eszköz pontos időzítését, vagy az eszköz valamilyen elektromágneses kisugárzását-, és ebből következtessen a kulcsra.

Ha létezhetnek ilyen oldal-csatornák, a szemléltetés vegye tekintetbe azokat a mechanizmusokat, amelyek meggátolják ezeknek az oldal-csatornáknak a bekövetkezését, mint például véletlen belső órák, két-utas technológia stb. A szóbanforgó mechanizmusok ellenőrizhetők a tisztán terv-alapú érvelések és a tesztelések kombinációjával.

Utolsó példaként arra, hogy biztonsági funkcionalitást használnak védett erőforrás helyett, tételezzünk fel egy olyan ST-t, amely tartalmazza az „Az eredet kikényszerített bizonyítása” (FCO_NRO_2) biztonsági követelményt, amely megkívánja, hogy a TSF bizonyítékot nyújtson az ST-ben specifikált információ-típusok eredetére vonatkozóan. Tételezzük fel, hogy az „információ-típusok” magukban foglalnak minden információt, amelyet a TOE felhasználásával küldenek e-mailen keresztül. Ebben az esetben az értékelő vizsgálja meg a leírást, hogy meggyőződjön arról, hogy minden TSFI részletezve van, amely aktivizálható e-mail küldése céljából, és ezek végrehajtják az „Az eredet kikényszerített bizonyítása” funkciót. A leírás utalhat az üzemeltetési felhasználói útmutatóra, hogy minden helyet bemutasson, ahonnan e-mail származhat (pl. levelező program, scriptektől/batch-job-októl származó értesítések), és hogy bemutassa, hogy mindezek a helyek hogyan aktivizálják az eredet előállítása funkciót.

Az értékelő győződjön meg arról is, hogy a leírás átfogó, amelyben minden interfészt megvizsgálnak a megkívánt SFR-ek teljes összessége szerint. Ez megkívánhatja az értékelőtől, hogy vizsgálja meg az alátámasztó információkat (funkcionális specifikáció, TOE terv, a biztonsági szerkezet leírás egyéb részei, az üzemeltetési felhasználói útmutató) annak megállapítása érdekében, hogy a leírás helyesen ragadta-e meg az egyes interfésznek minden vonatkozását. Az értékelő gondolja át, hogy az egyes TSFI-k mely SFR-ekre lehetnek befolyással (a TSFI leírásból és ennek megvalósításából az alátámasztó dokumentációban), és ezután vizsgálja meg a leírást annak megállapítása érdekében, hogy az lefedi-e a szóbanforgó vonatkozást.

6.2.4.1.2. Funkcionális specifikáció: Az ADV_FSP.3 altevékenység értékelése

Ennek az altevékenységnek a célja annak a megállapítása, hogy a fejlesztő leírta-e a TSFI-t, a rendeltetés, használati mód és a paraméterek szempontjából. Ezen kívül minden TSFI-re a tevékenységeket, eredményeket és hibaüzeneteket is kellőképpen le kell írni, hogy megállapíthatóak legyenek az SFR-t érvényre juttató TSFI-k. Az SFR-t érvényre juttató TSFI-ket részletesebben kell leírni, mint a többi TSFI-t.

Az ehhez az altevékenységhez a munkaegységek által megkövetelt értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) TOE terv.

Az ehhez az altevékenységhez felhasznált egyéb értékelési bizonyíték:

a) biztonsági szerkezet leírása,
b) üzemeltetési felhasználói útmutató.

6.2.4.1.2.1. Az ADV_FSP.3.1E értékelői akció

ADV_FSP.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ADV_FSP.3.1C A funkcionális specifikációnak teljes mértékben be kell mutatnia a TSF-et.

ADV_FSP.3-1 Az értékelőnek meg kell vizsgálnia a funkcionális specifikációt annak megállapítása érdekében, hogy az teljes mértékben bemutatja-e a TSF-t.

Ennél az altevékenységnél a TSFI azonosítása szükséges előfeltétel minden egyéb tevékenységhez. A TSFI azonosítása érdekében azonosítani kell a TSF-t (a „TOE terv" (ADV_TDS) munkaegységei részeként). Ez a tevékenység végrehajtható magas szinten, annak biztosításával, hogy az interfészek nagy csoportjai (hálózati protokollok, hardver interfészek, konfigurációs fájlok) nem maradtak ki, vagy alacsony szinten, ahogy a funkcionális specifikáció értékelése előrehalad.

Ezen munkaegység értékelésekor az értékelő állapítsa meg, hogy a TSF minden részét figyelembe vették-e a funkcionális specifikációban felsorolt interfészek szerint. A TSF minden részéhez tartozzon egy interfész leírás, vagy ha a TSF valamely részéhez nem tartozik interfész, az értékelő állapítsa meg, hogy ez elfogadható.

ADV_FSP.3.2C A funkcionális specifikációnak le kell írnia minden TSFI rendeltetését és használati módját.

ADV_FSP.3-2 Az értékelőnek meg kell vizsgálnia a funkcionális specifikációt annak megállapítása érdekében, hogy az meghatározza-e minden TSFI rendeltetését.

Egy TSFI rendeltetése egy olyan általános kijelentés, amely összegzi az interfész által nyújtott funkcionalitást. Az interfészhez kapcsolódó minden tevékenység és eredmény teljes megfogalmazása nem szükséges, de a felhasználót segítenie kell annak általános megértésében, hogy az interfészt mire szánták. Az értékelő ne csak a rendeltetés létezését állapítsa meg, hanem azt is, hogy ez helyesen tükrözi a TSFI-t, figyelembe véve az interfészre vonatkozó egyéb információkat is, mint például a tevékenységek leírása és a hibaüzenetek.

ADV_FSP.3-3 Az értékelőnek meg kell vizsgálnia a funkcionális specifikációt annak megállapítása érdekében, hogy az meghatározza-e minden TSFI használati módját.

Egy TSFI használati módja összegzi, hogy az interfészt hogyan kell kezelni a TSFI-vel kapcsolatos tevékenységek kiváltása és az eredmények megszerzése érdekében. Az értékelő állapítsa meg a funkcionális specifikációban megadott anyagból, hogy hogyan kell használni az interfészt. Ez nem feltétlenül jelenti azt, hogy minden egyes TSFI-hez léteznie kell egy külön használati módnak, például valószínűleg általánosan leírható a kernel-hívások

aktivizálási módja, majd megadható minden olyan interfész, ami ezt az általános módszert használja. A különböző típusú interfészek eltérő használási mód meghatározást kívánnak. Az API-k, a hálózati protokoll interfészek, a rendszer konfigurációs paraméterek és hardver busz interfészek mindegyikéhez eltérő használati mód tartozik, és ezt a fejlesztőnek figyelembe kell vennie, amikor a funkcionális specifikációt kialakítja, ahogy az értékelőnek is figyelembe kell vennie, amikor a funkcionális specifikáció értékeli.

Az olyan adminisztrációs interfészek esetében, amelyek funkcionalitását úgy dokumentálták, hogy ahhoz nem-megbízható felhasználó nem férhet hozzá, az értékelőnek meg kell győződnie arról, hogy a funkcionális specifikáció leírja azt a módszert, amellyel a funkciót hozzáférhetetlenné teszik. Meg kell jegyezni, hogy a hozzáférhetetlenséget a fejlesztőnek tesztelnie kell tesztkészletében.

Az értékelőnek nemcsak a használati mód leírások létezését kell megállapítania, hanem azt is, hogy ezek pontosan lefednek minden TSFI-t.

ADV_FSP.3.3C A funkcionális specifikációnak azonosítania kell és le kell írnia minden TSFI-hez kapcsolódó összes paramétert.

ADV_FSP.3-4 Az értékelőnek meg kell vizsgálnia a TSFI bemutatását annak megállapítása érdekében, hogy az teljes mértékben azonosít-e minden TSFI-hez kacsolódó összes paramétert.

Az értékelő vizsgálja át a funkcionális specifikációt, hogy meggyőződjön arról, hogy minden egyes TSFI-hez kapcsolódó összes paramétert leírtak. A paraméterek olyan közvetlen bemenetei vagy kimenetei egy interfésznek, amelyek a szóbanforgó interfész működését irányítják. Például paraméterek az API-knak átadott argumentumok; a különféle mezők egy meghatározott hálózati protokoll csomagjaiban; a Windows Registry-ben lévő egyedi kulcs értékek; egy chip érintkezői közötti jelek; stb.

Annak megállapítása érdekében, hogy minden paraméter megvan-e a TSFI-ben, az értékelő vizsgálja át az interfész leírás további részeit is (tevékenységeket, hibaüzeneteket, stb.), hogy megállapítsa, vajon az interfész leírások figyelembe vették-e a paraméterek leírásait. Az értékelő ellenőrizze az értékeléshez átadott egyéb bizonyítékokat is (pl. TOE terv, biztonsági szerkezet leírás, üzemeltetési felhasználói dokumentáció), hogy észrevegye, ha ezek leírnak egy olyan működést meghatározó vagy kiegészítő paramétert, amit a funkcionális specifikáció nem tartalmaz.

ADV_FSP.3-5 Az értékelőnek meg kell vizsgálnia a TSFI bemutatását annak megállapítása érdekében, hogy az teljesen és pontosan leír-e minden TSFI-hez kacsolódó összes paramétert.
Az összes paraméter azonosítása után az értékelőnek meg kell győződnie arról, hogy ezeket helyesen és teljesen írták le. Egy paraméter leírása azt közli valamilyen érthető módon, hogy mi is a paraméter. Például a foo(i) interfész leírható úgy, hogy tartozik hozzá egy „i paraméter, ami egy egész”; ez azonban nem egy elfogadható paraméter leírás. Sokkal inkább elfogadható egy olyan leírás, hogy „az i paraméter egy egész szám, amely jelzi a rendszerbe jelenleg bejelentkezett felhasználók számát”.

Annak megállapítása érdekében, hogy minden paraméter leírása teljes, az értékelő vizsgálja át az interfész leírások további részeit is (rendeltetés, felhasználási mód, tevékenységek, hibaüzenetek, stb.), hogy megállapítsa, vajon az interfész leírások figyelembe vették-e a paraméterek leírásait. Az értékelő ellenőrizze az értékeléshez átadott egyéb bizonyítékokat is (pl. TOE terv, biztonsági szerkezet leírás, üzemeltetési felhasználói dokumentáció), hogy észrevegye, ha ezek leírnak egy olyan működést meghatározó vagy kiegészítő paramétert, amit a funkcionális specifikáció nem tartalmaz.

ADV_FSP.3.4C Az SFR-t érvényre juttató TSFI-kre, a funkcionális specifikációnak le kell írnia a TSFI-hez kapcsolódó, SFR-t érvényre juttató tevékenységeket.

ADV_FSP.3-6 Az értékelőnek meg kell vizsgálnia a TSFI bemutatását annak megállapítása érdekében, hogy az teljesen és helyesen leír-e az SFR-t érvényre juttató TSFI-khez kapcsolódó minden SFR-t érvényre juttató tevékenységet.

Ha egy interfészen keresztül elérhető tevékenység szerepet játszik a TOE valamelyik biztonsági szabályzatának az érvényre juttatásában (vagyis ha az interfészen keresztül hozzáférhető tevékenységek egyike visszavezethető a TSF-től elvárt SFR-ek egyikére), akkor a szóbanforgó interfész SFR-t érvényre juttató. Az ilyen szabályzatok nem korlátozódnak a hozzáférés ellenőrzési szabályzatokra, hanem minden olyan funkcionalitásra vonatkoznak, amelyet az ST-ben megadott SFR-ek valamelyike specifikál. Meg kell jegyezni, hogy egy interfészhez számos tevékenység tartozhat, következésképpen ezek közül egyesek lehetnek SFR-t érvényre juttatók, míg mások nem.

A fejlesztőnek nem kell „felcímkéznie” az interfészeket SFR-t érvényre juttatóként, és ugyanígy nincs megkövetelve, hogy egy interfészen keresztül hozzáférhető tevékenységet SFR-t érvényre juttatóként azonosítson. Az értékelő felelőssége hogy megvizsgálja a fejlesztő által nyújtott bizonyítékokat, és megállapítsa a kívánt információ meglétét. Abban az esetben, amikor a fejlesztő beazonosította az SFR-t érvényre juttató TSFI-t és az ezen az interfészen keresztül rendelkezésre álló, SFR-t érvényre juttató tevékenységeket, az értékelőnek feltétlenül meg kell ítélnie a teljességet és pontosságot az értékeléshez átadott egyéb információk alapján (pl. TOE terv, biztonsági szerkezet leírás, üzemeltetési felhasználói útmutató), és az interfészhez bemutatott egyéb információk alapján (paraméterek és paraméter leírások, hibaüzenetek, stb.).

Ebben az esetben (amikor a fejlesztő csak SFR-t érvényre juttató információkat adott meg az SFR-t érvényre juttató TSFI-re), az értékelő győződjön meg arról is, hogy nincsenek rosszul kategorizált interfészek. Ez elvégezhető az értékeléshez átadott egyéb információk vizsgálatával (pl. TOE terv, biztonsági szerkezet leírás, üzemeltetési felhasználói útmutató), valamint az interfészhez bemutatott olyan egyéb információk vizsgálatával (például paraméterek és paraméter leírások), amelyek nincsenek SFR-t érvényre juttatóként kategorizálva. Ehhez a megállapításhoz az ADV_FSP.3-7 és ADV_FSP.3-8 munkaegységeket is fel kell használni.

Abban az esetben, amikor a fejlesztő ugyanolyan szintű információt nyújt minden interfészre, az értékelő hajtsa végre az előző bekezdésben megemlített típusú vizsgálatot. Az értékelő állapítsa meg, hogy mely interfészek SFR-t érvényre juttatók, és melyek nem, majd ezt követően győződjön meg arról, hogy az SFR-t érvényre juttató tevékenységek SFR-t érvényre

juttató vonatkozásait megfelelően leírták-e. Meg kell jegyezni, hogy az értékelőnek végre kell tudni hajtania az ADV_FSP.3-8 munkaegységhez kapcsolódó munkák zömét ezen SFR-t érvényre juttató jelleg vizsgálata során.

Az SFR-t érvényre juttató tevékenységek azok, amelyek valamelyik külső interfészen láthatók, és az elvárt SFR-k érvényre juttatására szolgálnak. Például, ha vannak naplózási követelmények az ST-ben, akkor a naplózással kapcsolatos tevékenységek SFR-t érvényre juttatók, ennélfogva kötelező leírni ezeket, még akkor is, ha ezen tevékenységek eredménye általában nem látható az érintett interfészen (minthogy a naplózással kapcsolatban egy interfészen kiváltott felhasználói tevékenység gyakran egy másik interfészen látható napló-bejegyzést idéz elő).

A leírás megkívánt szintje olyan, ami elegendő az olvasó számára annak megértéséhez, hogy a TSFI tevékenységek milyen szerepet játszanak az SFR vonatkozásában. Az értékelő tartsa szem előtt, hogy a leírásnak elegendően részletesnek kell lennie ahhoz, hogy támogassa a teszt-esetek előállítását (és kiértékelését) a szóbanforgó interfész vonatkozásában. Ha a leírás nem világos, vagy nem eléggé részletes a TSFI értelmes teszteléséhez, akkor valószínű, hogy a leírás nem megfelelő.

ADV_FSP.3.5C Az SFR-t érvényre juttató TSFI-kre, a funkcionális specifikációnak le kell írnia a biztonságot érvényre juttató hatásokból származó közvetlen hibaüzeneteket, valamint a TSFI meghívásához kapcsolódó kivételeket.

ADV_FSP.3-7 Az értékelőnek meg kell vizsgálnia a TSFI bemutatását annak megállapítása érdekében, hogy az teljesen és helyesen leírja-e az összes SFR-t érvényre juttató TSFI aktivizálásának eredményeként kapható hibaüzeneteket.

Ezt a munkaegységet vagy az ADV_FSP.3-6 munkaegységgel összekapcsolva, vagy utána kell végrehajtani, hogy biztosított legyen az SFR-t érvényre juttató TSFI helyes azonosítása. Az értékelő tartsa szem előtt, hogy a követelmény és az ehhez kapcsolódó munkaegység feltétlenül elvárja minden olyan közvetlen hibaüzenet leírását, amely egy SFR-t érvényre juttató TSFI-hez, azon belül pedig egy SFR-t érvényre juttató tevékenységhez kapcsolódik. Ennek az az oka, hogy ezen a garanciaszinten fel kell használni a hibaüzenet leírások által nyújtott „extra” információt annak megállapításához, hogy egy interfész minden SFR-t érvényre juttató vonatkozását megfelelően leírták-e. Például, ha egy TSFI-hez kapcsolódó hibaüzenet (pl. „hozzáférés megtagadva”) jelzi, hogy egy SFR-t érvényre juttató döntés vagy tevékenység történt, de az SFR-t érvényre juttató tevékenységek leírásában semmilyen említés nem történik a szóbanforgó konkrét SFR-t érvényre juttató mechanizmusról, akkor lehetséges, hogy a leírás nem teljes.

A hibák sokféle formát ölthetnek, a leírandó interfésztől függően. Egy API esetében maga az interfész visszaadhat hibakódot; beállíthat egy globális hibafeltételt; vagy beállíthat egy hibakóddal kapcsolatos meghatározott paramétert. Egy konfigurációs fájl esetében egy helytelenül beállított paraméter kiválthat egy naplófájlban rögzítendő hibaüzenetet. Egy hardver PCI kártya esetében egy hibafeltétel egy jelet válthat ki a buszon, vagy egy CPU-hoz kapcsolódó kivétel feltételt idézhet elő.

Hibák (és a kapcsolódó hibaüzenetek) egy interfész aktivizálásán keresztül következnek be. Az interfész aktivizálására adott válaszként jelentkező feldolgozás hiba körülményekkel találhatja szemben magát, ami egy hibaüzenet előállítását váltja ki (egy megvalósítás-specifikus mechanizmuson keresztül). Bizonyos esetekben ez lehet egy visszatérési érték magától az interfésztől; más esetekben lehetséges, hogy egy globális értéket állítanak be, és az interfész aktivizálása után ezt ellenőrzik. Valószínű, hogy a TOE számos olyan alacsony-szintű hibaüzenettel rendelkezik, amelyek alapvető erőforrás körülményekből erednek, mint például „a diszk megtelt", vagy „erőforrás lock-olva van". Bár az ilyen hibaüzenetek számos TSFI-hez hozzárendelhetők, felhasználhatók az olyan esetek felismerésére, amikor egy interfész leírás kimaradt. Például egy olyan TSFI, amely „a diszk megtelt" üzenetet állít elő, de amihez a tevékenységek ismertetésénél nem tartozik kézzelfogható leírás arról, hogy a TSFI miért idéz elő diszk hozzáférést, arra ösztönözheti az értékelőt, hogy a szóbanforgó TSFI-vel kapcsolatos egyéb bizonyítékokat is megvizsgálja (biztonsági szerkezet (ADV_ARC), TOE terv (ADV_TDS)), annak megállapítása érdekében, hogy a leírás teljes és helyes-e.

Annak megállapítása érdekében, hogy egy TSFI aktivizálása következtében fellépő hibaüzenet leírása pontos és teljes-e, az értékelő mérje össze az interfész leírásokat az értékeléshez átadott egyéb bizonyítékokkal (pl. TOE terv, biztonsági szerkezet leírás, üzemeltetési felhasználói dokumentáció), valamint az adott TSFI-hez szolgáltatott egyéb bizonyítékokkal (az SFR-t érvényre juttató tevékenységek leírása, a TSF-t támogató és a TSF-be nem beavatkozó tevékenységek és eredmények összegzése) is.

ADV_FSP.3.6C A funkcionális specifikációnak minden TSFI-re összegeznie kell az SFR-t támogató és az SFR-be nem beavatkozó tevékenységeket.

ADV_FSP.3-8 Az értékelőnek meg kell vizsgálnia a TSFI bemutatását annak megállapítása érdekében, hogy az minden TSFI-re összegzi-e az SFR-t támogató és az SFR-be nem beavatkozó tevékenységeket.

Ennek a munkaegységnek a célja az SFR-t érvényre juttató tevékenységekre vonatkozó részletek (amelyeket az ADV_FSP.3-6 munkaegységben kell megadni) kiegészítése a többi (nem SFR-t érvényre juttató) tevékenység összegzésével. Ez az összegzés lefed minden SFR-t támogató és SFR-be nem beavatkozó tevékenységet, akár SFR-t érvényre juttató TSFI-n, akár pedig SFR-t támogató vagy SFR-be nem beavatkozó interfészen keresztül aktivizálhatók. Egy ilyen összegzés az összes SFR-t támogató és SFR-be nem beavatkozó tevékenység vonatkozásában segíti az értékelőt egy teljes kép kialakításában a TSF által nyújtott funkciókról, valamint annak megállapításában, hogy egy tevékenységet vagy TSFI-t nem kategorizáltak-e esetleg helytelenül.

Az elvárt információ absztraktabb, mint amit az SFR-t érvényre juttató tevékenységekre megkövetelnek. Bár ennek is elég részletesnek kell lennie ahhoz, hogy az olvasó megérthesse a tevékenység által elvégzetteket, de annyira nem kell részletesnek lennie, hogy elegendő legyen például a tevékenység tesztelésének a megalapozásához. Az értékelő szempontjából az a fontos, hogy az információnak feltétlenül elegendőnek kell lennie ahhoz, hogy határozottan el tudja dönteni, hogy a tevékenység SFR-t támogató vagy SFR-be nem beavatkozó. Ha ilyen szintű információ hiányzik, akkor az összegzés nem elegendő, több információra van szükség.

ADV_FSP.3.7C A visszavezetésnek szemléltetnie kell az SFR-ek visszavezetését a funkcionális specifikáció TSFI-eire.

ADV_FSP.3-9 Az értékelőnek ellenőriznie kell, hogy a visszavezetés összekapcsolja-e az SFR-eket a megfelelő TSFI-kkel.

A visszavezetés a fejlesztőnek kell megadnia abból a célból, hogy útmutatóként szolgáljon ahhoz, hogy mely SFR-ek, mely TSFI-kkel állnak kapcsolatban. Ez a visszavezetés lehet olyan egyszerű, mint például egy táblázat; ez bemenetként szolgál az értékelő számára a következő munkaegységekben való felhasználáshoz, amelyekben az értékelő ellenőrzi ennek helyességét és teljességét.

6.2.4.1.2.2. Az ADV_FSP.3.2E értékelői akció

ADV_FSP.3.2E Az értékelőnek meg kell állapítania, hogy a funkcionális specifikáció az SFR-ek pontos és teljes megjelenítése-e.

ADV_FSP.3-10 Az értékelőnek meg kell vizsgálnia a funkcionális specifikációt annak megállapítása érdekében, hogy az az SFR-ek teljes megjelenítése-e.

Az értékelő építhet a fejlesztő visszavezetésére (lásd ADV_FSP.3-9), ami egy megfeleltetés a TOE biztonsági funkcionális követelmények és a TSFI között, hogy meggyőződjön arról, hogy a funkcionális specifikáció és a teszt lefedettség vizsgálat minden SFR-t lefed. Meg kell jegyezni, hogy a szóbanforgó megfeleltetés részletezettségi szintje lehet alacsonyabb, mint a követelmények összetevő-, sőt elem szintje, a funkcionális követelményeken végrehajtott műveletek miatt (értékadások, pontosítások és kiválasztások), amit az ST szerzője végez el.

Például az FDP_ACC.l komponens tartalmazhat egy értékadásokkal rendelkező elemet. Ha az ST például tíz szabályt tartalmaz az FDP_ACC.l értékadásban, és ezt a tíz szabályt esetleg három különböző TSFI fedi le, az értékelő számára nem lenne elegendő az FDP_ACC.l-hoz hozzárendelni a TSFI A, B és C-t, és kijelenteni, hogy ezzel teljesítetve van a munkaegység. Ehelyett az értékelő feltehetően hozzárendeli az FDP ACC.l (1-es szabály) –t a TSFI A-hoz; az FDP ACC.l (2-es szabály) –t a TSFI B-hez; stb. Lehetséges az az eset is, hogy az interfész egy gyűjtő interfész (pl. IOCTL), amikor a megfeleltetést az adott interfész bizonyos paraméterkészletére kell megadni.

Az értékelőnek fel kell ismernie, hogy az olyan követelményekre vonatkozóan, amelyek kevéssé vagy egyáltalán nem öltenek testet a TSF határán (pl. FDP_RIP), nincsen elvárva, hogy ezeket teljes mértékben megfeleltessék a TSFI-nek. A szóbanforgó követelmények vizsgálatát a TOE terv vizsgálatakor fogják elvégezni (ADV_TDS), ha ez benne van az ST-ben. Fontos megjegyezni azt is, hogy mivel a TSFI-hez kapcsolódó paramétereket, tevékenységeket és hibaüzeneteket teljes mértékben specifikálni kell, az értékelőnek képesnek kell lennie annak megállapítására, hogy egy SFR minden vonatkozásáról látszik-e, hogy azt interfész szinten valósították meg.

ADV_FSP.3-11 Az értékelőnek meg kell vizsgálnia a funkcionális specifikációt annak megállapítása érdekében, hogy az az SFR-ek helyes megjelenítése-e.

Az ST-ben lévő minden olyan funkcionális követelmény esetében, amely a TSF határán látható hatásokban nyilvánul meg, a követelményhez kapcsolódó TSFI-hez megadott információ specifikálja a követelmény által leírt megkívánt funkcionalitást. Ha például az ST hozzáférés ellenőrzési listákra vonatkozó követelményt tartalmaz, és ennek a követelménynek egyetlen olyan TSFI-t feleltettek meg, amely Unix-fajtájú védelmi bitekre specifikál funkcionalitást, akkor a funkcionális specifikáció az adott követelmény szempontjából helytelen.

Az értékelőnek tudnia kell, hogy az olyan követelményekre vonatkozóan, amelyek kevéssé vagy egyáltalán nem öltenek testet a TSF határán (pl. FDP_RIP), nem várják el, hogy teljes mértékben megfeleltessék a TSFI-nek. A szóbanforgó követelmények vizsgálatát a TOE terv vizsgálatakor fogják elvégezni (ADV_TDS), ha ez benne van az ST-ben.

6.2.4.1.3. TOE tervezés: Az ADV_TDS.2 altevékenység értékelése

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) a funkcionális specifikáció,
c) a biztonsági szerkezet leírás,
d) a TOE terv.

6.2.4.1.3.1. Az ADV_TDS.2.1E értékelői akció

ADV_TDS.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ADV_TDS.2.1C A tervnek le kell írnia a TOE szerkezetét alrendszerek szerint.

ADV_TDS.2-1 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy a teljes TOE szerkezetet leírták-e alrendszerek szerint.

Az értékelő győződjön meg arról, hogy a TOE minden alrendszerét azonosították. Ez a TOE leírás bemenetként szolgál az ADV_TDS.3-2 munkaegységhez, ahol a TOE TSF-et alkotó részeit azonosítják. Vagyis ez a követelmény a teljes TOE-ra vonatkozik, nem csak a TSF-re.
A TOE (és a TSF) leírható az absztrakció több szintjén (vagyis alrendszerek és modulok szintjén). A TOE bonyolultságától függően a terv leírható alrendszerek és modulok szerint. Ezen a garanciaszinten a felbontást csak az alrendszerekig szükséges elvégezni.

E tevékenység végrehajtásakor az értékelő vizsgáljon meg a TOE-hoz bemutatott egyéb bizonyítékot is (pl. ST, üzemeltetési felhasználói útmutató) annak megállapítása érdekében, hogy a TOE leírása ezekben a bizonyítékokban összhangban áll-e a TOE tervben leírtakkal.

ADV_TDS.2.2C A tervnek azonosítania kell a TSF minden alrendszerét.

ADV_TDS.2-2 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy az a TSF minden alrendszerét azonosítja-e.

Az ADV_TDS.2-1 munkaegységben a TOE valamennyi alrendszere legyen azonosítva, és állapítsák meg, hogy a nem-TSF alrendszereket helyesen jellemezték-e. Erre a munkára alapozva, pontosan azonosítani kell azokat az alrendszereket, melyeket nem jellemeztek nem-TSF alrendszerként. Az értékelő állapítsa meg az „Előkészítő eljárások” (AGD_PRE) útmutatónak megfelelően installált hardverről és szoftverről, hogy minden alrendszert figyelembe vettek, akár része a TSF-nek, akár nem.

ADV_TDS.2.3C A tervnek le kell írnia a TSF minden SFR-be be nem avatkozó alrendszerének működésmódját, kellő részletességgel annak megállapításához, hogy az SFR-be be nem avatkozó.

ADV_TDS.2-3 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy a TSF minden SFR-be be nem avatkozó alrendszerét leírták-e úgy, hogy az értékelő megállapíthassa, hogy ezek az alrendszerek valóban SFR-be be nem avatkozóak.

ADV_TDS.2.4C A tervnek le kell írnia az SFR-t érvényre juttató alrendszerek SFR-t érvényre juttató működésmódját.

ADV_TDS.2-4 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy az biztosít-e egy teljes, pontos és részletes leírást az SFR-t érvényre juttató alrendszerek SFR-t érvényre juttató működésmódjáról.

A fejlesztő megjelölheti az alrendszereket SFR-t érvényre juttatóként, SFR-t támogatóként, és SFR-be nem beavatkozóként, bár ezek a „megjelölések” csak annak jelzésére szolgálnak, hogy a fejlesztőnek milyen mennyiségű és típusú információt kell szolgáltatnia, és felhasználható azon információ mennyiségének korlátozására, amelyet a fejlesztőnek kell kidolgoznia, ha az előkészítési munkálatok nem állítják elő a megkívánt dokumentációt. Akár kategorizálta az alrendszereket a fejlesztő, akár nem, az értékelő felelőssége annak megállapítása, hogy az alrendszerek rendelkeznek-e megfelelő információval a TOE-beli szerepüket illetően (SFR-t érvényre juttató, stb.), és a megfelelő információ megszerzése a fejlesztőtől, ha a fejlesztő elmulasztotta biztosítani a megkívánt információt egy meghatározott alrendszer esetében.

Az SFR-et érvényre juttató tulajdonság arra utal, hogy egy alrendszer hogyan biztosítja az SFR-et megvalósító funkcionalitást. Ennek a tulajdonságnak a részletes ismertetése, bár nem algoritmikus leírás szinten, általában azt tárgyalja, hogy a funkcionalitás hogyan lett biztosítva abból a szempontból, hogy milyen kulcs-adatok és adatstruktúrák léteznek, milyenek a szabályozási összefüggések egy alrendszeren belül, és hogy ezek az elemek hogyan működnek együtt az SFR-t érvényre juttató tulajdonság biztosítása céljából. Egy ilyen leírás hivatkozik az SFR-et támogató tulajdonságra, amelyet az értékelőnek az elkövetkező munkaegységek végrehajtása közben kell megfontolnia.

Az értékelő a teljesség és pontosság megállapítás céljából egyéb rendelkezésre álló információkat is vizsgáljon meg (pl. funkcionális specifikáció, biztonsági szerkezet leírás). E dokumentumok funkcionalitásra vonatkozó leírásainak összhangban kell lenniük a munkaegységhez biztosított bizonyítékkal.

ADV_TDS.2.5C A tervnek összegeznie kell az SFR-t érvényre juttató alrendszerek SFR-t támogató és SFR-be nem beavatkozó működésmódját.

ADV_TDS.2-5 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy az biztosít-e egy teljes és pontos magas szintű leírást az SFR-t érvényre juttató alrendszerek SFR-be nem beavatkozó működésmódjáról.

A fejlesztő megjelölheti az alrendszereket SFR-t érvényre juttatóként, SFR-t támogatóként, és SFR-be nem beavatkozóként, bár ezek a „megjelölések" csak annak jelzésére szolgálnak, hogy a fejlesztőnek milyen mennyiségű és típusú információt kell szolgáltatnia, és felhasználható azon információ mennyiségének korlátozására, amelyet a fejlesztőnek kell kidolgoznia, ha az előkészítési munkálatok nem állítják elő a megkívánt dokumentációt. Akár kategorizálta az alrendszereket a fejlesztő, akár nem, az értékelő felelőssége annak megállapítása, hogy az alrendszerek rendelkeznek-e megfelelő információval a TOE-beli szerepüket illetően (SFR-t érvényre juttató, stb.), és a megfelelő információ megszerzése a fejlesztőtől, ha a fejlesztő elmulasztotta biztosítani a megkívánt információt egy meghatározott alrendszer esetében.

Az előző munkaegységgel ellentétben ez a munkaegység azt írja elő az értékelő számára, hogy mérje fel az SFR-t érvényre juttató alrendszerekhez átadott olyan információkat, amelyek SFR-be nem beavatkozó alrendszerekre vonatkoznak. Ennek a felmérésnek a célja kettős. Először is az, hogy nyújtson az értékelőnek szélesebb ismereteket az egyes alrendszerek üzemeltetési módjáról. Másodszor, hogy az értékelő állapítsa meg, hogy minden SFR-t érvényre juttató tulajdonságot leírtak, amelyet egy alrendszer felmutat. Az előző munkaegységgel ellentétben az SFR-be nem beavatkozó viselkedésmódra vonatkozó információknak nem kell olyan részleteseknek lenni, mint az SFR-t érvényre juttató tulajdonságra megadottaknak. Például az olyan adat-struktúrákat vagy adat-tételeket, amelyek nincsenek kapcsolatban SFR-t érvényre juttató funkcionalitással, feltehetően nem kell részletesen ismertetni, ha egyáltalán le kell írni. Az értékelő döntésén múlik azonban, hogy egy meghatározott TOE esetében mit jelent a „magas-szint", és hogy elegendő információt kapott-e a fejlesztőtől ahhoz, hogy megbízható határozatot hozhasson erre a munkaegységre (még akkor is, ha az derül ki, hogy az információ ugyanolyan részletezettségű, mint az SFR-t érvényre juttató alrendszerek részére megadottak).

Figyelmeztetjük az értékelőt, hogy a „tökéletes" garancia nem cél, és nem is követeli meg ez a munkaegység, így az ítélőképességét kell igénybe vennie a megkívánt bizonyítékok mennyiségének és összetételének a megállapításakor az erre a munkaegységre vonatkozó határozat meghozatalához.

Az értékelő a teljesség és pontosság megállapítás céljából egyéb rendelkezésre álló információkat is vizsgáljon meg (pl. funkcionális specifikáció, biztonsági szerkezet leírás). E dokumentumok funkcionalitásra vonatkozó leírásainak összhangban kell lenniük a munkaegységhez biztosított bizonyítékkal. Különösen a funkcionális specifikációt használják annak megállapításához, hogy a funkcionális specifikáció által ismertetett, TSF interfészek megvalósításához megkövetelt viselkedést teljes mértékben leírták-e az alrendszerre, minthogy a viselkedés vagy SFR-t érvényre juttató, vagy SFR-t támogató vagy pedig SFR-be nem beavatkozó lesz.

ADV_TDS.2.6C A tervnek összegeznie kell az SFR-t támogató alrendszerek működésmódját.

ADV_TDS.2-6 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy az biztosít-e egy teljes és pontos magas szintű leírást az SFR-t támogató alrendszerek működésmódjáról.

A fejlesztő megjelölheti az alrendszereket SFR-t érvényre juttatóként, SFR-t támogatóként, és SFR-be nem beavatkozóként, bár ezek a „megjelölések" csak annak jelzésére szolgálnak, hogy a fejlesztőnek milyen mennyiségű és típusú információt kell szolgáltatnia, és felhasználható azon információ mennyiségének korlátozására, amelyet a fejlesztőnek kell kidolgoznia, ha az előkészítési munkálatok nem állítják elő a megkívánt dokumentációt. Akár kategorizálta az alrendszereket a fejlesztő, akár nem, az értékelő felelőssége annak megállapítása, hogy az alrendszerek rendelkeznek-e megfelelő információval a TOE-beli szerepüket illetően (SFR-t érvényre juttató, stb.), és a megfelelő információ megszerzése a fejlesztőtől, ha a fejlesztő elmulasztotta biztosítani a megkívánt információt egy meghatározott alrendszer esetében.

Az előző két munkaegységgel ellentétben ez a munkaegység azt kívánja meg a fejlesztőtől, hogy az SFR-t támogató alrendszerekről biztosítson információkat (és az értékelő mérje fel ezeket). Az ilyen alrendszerek legyenek megemlítve az SFR-t érvényre juttató alrendszerek ismertetésekor, és a kölcsönhatások ismertetésénél is az ADV_TDS.2-7 munkaegységben. Az értékelői felmérés célja, az előző munkaegységhez hasonlóan, kettős. Először is, hogy nyújtson az értékelőnek ismereteket az egyes alrendszerek üzemeltetési módjáról. Másodszor, hogy az értékelő állapítsa meg, hogy a szóbanforgó működés elegendő részletességgel van-e leírva ahhoz, hogy az a mód, ahogyan az alrendszer támogatja az SFR-t érvényre juttató működést, világos legyen, és az értékelő eldönthesse, hogy ez a működés maga nem SFR-t érvényre juttató-e. Az SFR-t támogató alrendszerek működésére vonatkozó információknak nem kell olyan részleteseknek lenni, mint az SFR-t érvényre juttató tulajdonságra megadottaknak. Például az olyan adat-struktúrákat vagy adat-tételeket, amelyek nincsenek kapcsolatban SFR-et érvényre juttató funkcionalitással, feltehetően nem kell részletesen ismertetni, ha egyáltalán le kell írni. Az értékelő döntésén múlik azonban, hogy egy meghatározott TOE esetében mit jelent a „magas-szint", és hogy elegendő információt kapott-e a fejlesztőtől ahhoz, hogy megbízható határozatot hozhasson erre a munkaegységre (még akkor is, ha az derül ki, hogy az információ ugyanolyan részletezettségű, mint az SFR-t érvényre juttató alrendszerek részére megadottak).

Figyelmeztetjük az értékelőt, hogy a „tökéletes" garancia nem cél, és nem is követeli meg ez a munkaegység, így az ítélőképességét kell igénybe vennie a megkívánt bizonyítékok mennyiségének és összetételének a megállapításakor az erre a munkaegységre vonatkozó határozat meghozatalához.

Az értékelő a teljesség és pontosság megállapítás céljából egyéb rendelkezésre álló információkat is vizsgáljon meg (pl. funkcionális specifikáció, biztonsági szerkezet leírás). E dokumentumok funkcionalitásra vonatkozó leírásainak összhangban kell lenniük a munkaegységhez biztosított bizonyítékkal. Különösen a funkcionális specifikációt használják annak megállapításához, hogy a funkcionális specifikáció által ismertetett, TSF interfészek megvalósításához megkövetelt viselkedést teljes mértékben leírták-e az alrendszerre,

minthogy a viselkedés vagy SFR-t érvényre juttató, vagy SFR-t támogató vagy pedig SFR-be nem beavatkozó lesz.

ADV_TDS.2.7C A tervnek le kell írnia a TSF összes alrendszere közötti kölcsönhatásokat.

ADV_TDS.2-7 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy az leírja-e a TSF alrendszerei közötti kölcsönhatásokat.

Az alrendszerek közötti kölcsönhatások leírásának az a célja, hogy segítse az olvasót annak jobb megértésében, hogy a TSF hogyan hajtja végre a funkcióit. Ezeket a kölcsönhatásokat nem szükséges megvalósítási szinten jellemezni (pl. egy alrendszer valamelyik rutinjából paramétereknek az átadása egy másik alrendszerhez tartozó rutin számára; globális változók; hardver jelzések (pl. megszakítások) az egyik hardver alrendszertől egy megszakítás-kezelő alrendszer felé), de ebben a fejtegetésben legyenek lefedve azok az adatelemek, amelyeket egy speciális alrendszerhez úgy határoztak meg, hogy ezeket egy másik alrendszerben való felhasználásra szántak. Az alrendszerek közötti minden felügyeleti kapcsolatot is ismertetni kell (pl. az egyik alrendszer felelős egy tűzfal rendszer szabályzat-bázisának konfigurálásáért és a másik alrendszer megvalósítja a szóbanforgó szabályokat).

Meg kell jegyezni, hogy bár a fejlesztőnek jellemeznie kell az alrendszerek közötti összes kölcsönhatást, az értékelőnek magának kell megítélnie a leírás teljességét. Ha egy kölcsönhatás oka nem világos, vagy ha vannak olyan SFR-vonzatú kölcsönhatások, amelyekről úgy tűnik, hogy nincsenek ismertetve, az értékelő gondoskodjon arról, hogy ezt az információt a fejlesztő átadja. Ha azonban az értékelő azt állapítja meg, hogy bizonyos alrendszerek közötti kölcsönhatásokat ugyan nem ismertetett teljes mértékben a fejlesztő, de a teljes leírás nem járulna hozzá sem az általános funkcionalitás, sem a TSF által nyújtott biztonsági funkcionalitás megértéséhez, akkor az értékelő dönthet úgy, hogy a leírást elegendőnek tekinti, és nem kívánja meg a teljességet csak önmagáért.

ADV_TDS.2.8C A megfeleltetésnek szemléltetnie kell, hogy a TOE tervben ismertetett minden működésmódot megfeleltették az ezt aktivizáló TSFI-nek.

ADV_TDS.2-8 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy az tartalmaz-e teljes és helyes megfeleltetést a funkcionális specifikációban leírt TSFI és a TOE tervben leírt TSF modulok között.

A TOE tervben leírt alrendszerek a TSF működését ismertetik, a TSF SFR-t érvényre juttató részeit részletesen, az egyéb részeit pedig magas szinten. A TSFI azt ismerteti, hogy a megvalósítás hogyan használható. A fejlesztőtől származó bizonyíték azonosítja azt az alrendszert, ami először aktivizálódik, mikor műveletet kérnek a TSFI-től, valamint azonosítja a funkcionalitás megvalósításáért elsődlegesen felelős alrendszereket. A teljes hívási fa nem szükséges minden egyes TSFI-hez ennél a munkaegységnél.

Az értékelő mérje fel a megfeleltetés teljességét meggyőződve arról, hogy minden TSFI-hez legalább egy alrendszert hozzárendeltek. A helyesség ellenőrzése bonyolultabb.

A helyességre vonatkozó első szempont az, hogy minden egyes TSFI legyen megfeleltetve egy alrendszernek a TSF határánál. Ennek megállapítása megtehető az alrendszerek és

kölcsönhatások ismertetésének áttekintésével, majd ezek helyének a meghatározásával az architektúrában a szóbanforgó információk alapján. A helyességre vonatkozó következő szempont az, hogy ennek a megfeleltetésnek van-e értelme. Például egy hozzáférés ellenőrzéssel foglalkozó TSFI-nek a hozzárendelése egy olyan alrendszerhez, amely jelszókat ellenőriz, nem helyes. Az értékelőnek itt is az ítélőképességét kell igénybe vennie ennek a megállapításnak a meghozatalakor. A cél az, hogy ez az információ segítse az értékelőt abban, hogy megértse a rendszert és az SFR-ek megvalósítását, valamint azt a módot, ahogyan az entitások a TSF határán kölcsönhatásba tudnak lépni a TSF-fel. Annak felmérését, hogy az SFR-eket pontosan írták-e le alrendszerek szerint, nagyrészt a többi munkaegységben hajtják végre.

6.2.4.1.3.2. Az ADV_TDS.2.2E értékelői akció

ADV_TDS.2.2E Az értékelőnek meg kell erősítenie, hogy a terv az összes funkcionális biztonsági követelmény (SFR) pontos és teljes megjelenítése.

ADV_TDS.2-9 Az értékelőnek meg kell vizsgálnia a TOE biztonsági funkcionális követelményeket és a TOE tervet annak megállapítása érdekében, hogy a TOE terv az ST minden funkcionális biztonsági követelményét (SFR) lefedi-e.

Az értékelő összeállíthat egy megfeleltetést a TOE funkcionális biztonsági követelményei és a TOE terv között. Ez a megfeleltetés feltehetően egy SFR-től az alrendszerek egy halmazáig fog vezetni. Meg kell jegyezni, hogy a szóbanforgó megfeleltetés részletezettségi szintje lehet alacsonyabb, mint a követelmények összetevő-, sőt elem szintje, az ST szerzője által az SFR-eken végrehajtott műveletek (értékadások, pontosítások és kiválasztások) miatt.

Például a „Részleges hozzáférés ellenőrzés” (FDP_ACC.l) összetevő tartalmazhat egy értékadásokkal rendelkező elemet. Ha az ST például tíz szabályt tartalmaz a „Részleges hozzáférés ellenőrzés” (FDP_ACC.l) értékadásában, és ezt a tíz szabályt tizenöt modulon belüli megadott helyeken valósították meg, nem lenne elegendő, ha az értékelő a „Részleges hozzáférés ellenőrzés”-t (FDP_ACC.l) egy alrendszerhez rendelné hozzá, majd kijelentené, hogy a munkaegység teljesítve lett. Ehelyett, az értékelő rendelje hozzá a „Részleges hozzáférés ellenőrzés” (FDP_ACC.l) (1-es szabály)-t az A alrendszer x, y, és z moduljaihoz, a „Részleges hozzáférés ellenőrzés” (FDP_ACC.l) (2-es szabály)-t az A alrendszer x, p, és q moduljaihoz, és így tovább.

ADV_TDS.2-10 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy az minden funkcionális biztonsági követelményt helyesen jelenít-e meg.

Az értékelő győződjön meg arról, hogy az ST TOE-ra vonatkozó SFR-eket felsoroló részének minden biztonsági követelményére létezik a TOE tervben egy megfelelő terv leírás, amely pontosan részletezi, hogy a TSF hogyan valósítja meg a szóbanforgó követelményt. Ez megkívánja az értékelőtől, hogy határozzon meg egy alrendszer összetételt, amely felelős egy megadott funkcionális követelmény megvalósításáért, majd vizsgálja meg a szóbanforgó alrendszereket annak megértése érdekében, hogy a követelmény hogyan valósul meg. Végül az értékelő mérje fel, hogy a követelmény helyesen lett-e megvalósítva.

Példaként, ha az ST követelmények szerepkör-alapú hozzáférés ellenőrzési mechanizmust specifikálnak, az értékelő először azonosítsa azokat az alrendszereket, amelyek hozzájárulnak ennek a mechanizmusnak a megvalósításához. Ez megtehető a TOE terv mélyreható ismerete vagy megértése alapján, vagy a megelőző munkaegységben elvégzett munkán keresztül. Meg kell jegyezni, hogy ennek a nyomkövetésnek csak az a célja, hogy azonosítsa az alrendszereket, nem pedig a teljes vizsgálat.

A következő lépés annak megértése, hogy az alrendszerek milyen mechanizmusokat valósítanak meg. Például, ha a terv egy olyan hozzáférés ellenőrzési megvalósítást ír le, amely UNIX-típusú védelmi biteken alapul, a terv nem pontos megvalósulása azoknak a hozzáférés ellenőrzési követelményeknek, amelyeket a fenti ST példa mutat be. Ha az értékelő a részletek hiánya miatt nem tudja megállapítani, hogy pontosan milyen mechanizmusokat valósítottak meg, becsülje fel, hogy minden SFR-t érvényre juttató alrendszert azonosítottak-e, vagy hogy a szóbanforgó alrendszerekről elegendő részleteket nyújtottak-e.

6.2.4.2. Az Útmutató dokumentumok garanciaosztály (AGD) értékelése

Az útmutató dokumentumokhoz kapcsolódó tevékenységnek az a célja, hogy elbírálják annak a dokumentációnak a megfelelőségét, amely ismerteti, hogy a felhasználó hogyan tudja a TOE-t biztonságos módon kezelni. Az ilyenfajta dokumentációnak figyelembe kell vennie a különféle felhasználó típusokat (például azokat, akik befogadják, telepítik, adminisztrálják vagy üzemeltetik a TOE-t), akiknek a helytelen akciói hátrányosan befolyásolhatják a TOE-nak vagy a saját adataiknak a biztonságát.

Az útmutató dokumentumok osztály két családra van osztva, amelyek elsősorban az előkészítő felhasználói dokumentációval foglalkoznak (ami mindazt tartalmazza, amit meg kell tenni annak érdekében, hogy a leszállított TOE-t átalakítsák a környezet értékelt konfigurációjához, ahogyan az az ST-ben le van írva, vagyis ahogyan a TOE-t befogadják és telepítik), másodsorban pedig az üzemeltetői felhasználói dokumentációval (ami mindazt tartalmazza, amit meg kell tenni a TOE üzemeltetése során az értékelt konfigurációban, vagyis az üzemeltetést és adminisztrációt).

Az útmutató dokumentumokhoz kapcsolódó tevékenység azokra a funkciókra és csatlakozási felületekre vonatkozik, amelyek a TOE biztonságához kapcsolódnak. A TOE biztonságos konfigurálása az ST-ben van leírva.

6.2.4.2.1. Üzemeltetési felhasználói útmutató: Az AGD_OPE.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy az üzemeltetési felhasználói útmutató leírja-e minden felhasználói szerepkörre a TSF által nyújtott biztonsági funkcionalitást és interfészeket, tartalmazza-e a TOE biztonságos használatához szükséges utasításokat és útmutatást, lefedi-e az összes üzemeltetési mód biztonságos eljárásait, lehetővé teszi-e a TOE nem biztonságos állapotainak megelőzését és észlelését, egyúttal egyértelmű és megalapozott-e.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) a funkcionális specifikáció,
c) a TOE terv,
d) az üzemeltetési felhasználói útmutató.

6.2.4.2.1.1. Az AGD_OPE.1.1E értékelői akció

AGD_OPE.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

AGD_OPE.1.1C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre le kell írnia azokat a felhasználó által elérhető funkciókat és jogosultságokat (beleértve a megfelelő figyelmeztetéseket is), melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

AGD_OPE.1-1 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót, annak megállapítása érdekében, hogy az leírja-e azokat a felhasználó által elérhető funkciókat és jogosultságokat (beleértve a megfelelő figyelmeztetéseket is), melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

A TOE konfigurálása lehetővé teheti, hogy a különböző felhasználói szerepkörök a TOE különböző funkcióihoz eltérő jogosultságokkal rendelkezzenek. Ezáltal egyes felhasználók számára engedélyezve lesznek olyan funkciók, melyek mások számára nem. Ezeket a funkciókat és jogosultságokat minden felhasználói szerepkörre le kell írni az üzemeltetési felhasználói útmutatóban.

Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre azonosítania kell az ellenőrzés alatt tartandó funkciókat és jogosultságokat, az ezek számára szükséges utasítás típusokat, valamint az utasítások okait. Az üzemeltetési felhasználói útmutatónak figyelmeztetéseket kell tartalmaznia az ellenőrzés alatt tartandó funkciókra és jogosultságokra vonatkozóan. A figyelmeztetéseknek a várt hatásokról, az esetleges mellékhatásokról és a más funkciókkal és jogosultságokkal kapcsolatos lehetséges kapcsolatokról kell szólniuk.

AGD_OPE.1.2C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre le kell írnia, hogy a TOE által biztosított, elérhető interfészeket hogyan kell biztonságos módon használni.

AGD_OPE.1-2 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e a TOE által biztosított, elérhető interfészek biztonságos használatát.
Az üzemeltetési felhasználói útmutatónak javaslatokat kell megfogalmaznia a TSF hatékony használatához (például jelszó kialakítási gyakorlat áttekintése, felhasználói állományok mentésének javasolt gyakorisága, felhasználói hozzáférési jogok megváltoztatása hatásának elemzése).

AGD_OPE.1.3C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre le kell írnia az elérhető funkciókat és interfészeket, különösen a felhasználó ellenőrzése alá

tartozó minden biztonsági szempontból fontos paramétert, jelezve (ahol ez lehetséges) a biztonságos értékeket.

AGD_OPE.1-3 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e az elérhető funkciókat és interfészeket, különösen a felhasználó ellenőrzése alá tartozó minden biztonsági paramétert, jelezve (ahol ez lehetséges) a biztonságos értékeket is.

Az üzemeltetési felhasználói útmutatónak áttekintést kell adnia a felhasználói interfészeken keresztül látható biztonsági funkcionalitásról.

Az üzemeltetési felhasználói útmutatónak azonosítania kell, és le kell írnia a biztonsági funkciók és interfészek célját, működésüket, illetve egymás között kapcsolataikat.

Minden felhasználó által elérhető interfészre az üzemeltetési felhasználói útmutatónak:

a) le kell írnia azokat a módszereket, melyekkel az interfész hívható (pl. parancssor, programozási nyelvi rendszerhívások, menükiválasztás, parancsgombok);
b) le kell írnia a felhasználó által állítandó paramétereket, azok célját, érvényes és alapértelmezett értékeiket, a paraméterek biztonságos és nem biztonságos használatát okozó beállításokat, mindezt egyenként vagy paraméter-kombinációkban;
c) le kell írnia a közvetlen TSF válaszokat, üzeneteket vagy visszaadott kódot.

Az értékelőnek elsősorban a funkcionális specifikációt és az ST-t kell figyelembe vennie annak megállapítása érdekében, hogy az ezekben leírt TSF összhangban áll-e az üzemeltetési felhasználói útmutatóval. Az értékelőnek meg kell győződnie az üzemeltetési felhasználói útmutató teljességéről, vagyis arról, hogy az összes emberi felhasználó számára lehető teszi az elérhető TSFI-k biztonságos használatát. Az értékelő segítségként elkészítheti az útmutató és ezen dokumentumok közötti informális leképezést. Az ebben fellelhető bármilyen hiányosság az útmutató teljességének csorbulását jelezheti.

AGD_OPE.1.4C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre világosan be kell mutatnia a felhasználó által elérhető funkciókkal kapcsolatban végrehajtandó, biztonsági szempontból fontos minden esemény típust, beleértve a TSF ellenőrzése alá eső egyedek biztonsági tulajdonságainak megváltoztatását is.

AGD_OPE.1-4 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e a felhasználói funkciókkal kapcsolatban végrehajtandó, biztonsági szempontból lényeges minden esemény típust, beleértve a TSF ellenőrzése alá tartozó egyedek biztonsági tulajdonságainak megváltoztatását is.

Minden biztonsági szempontból fontos esemény típust részletezni kell minden felhasználói szerepkörre, hogy minden felhasználó tudja, milyen események fordulhatnak elő, és mit kell tennie (ha szükséges) a biztonság fenntartása érdekében. A TOE üzemeltetése során előforduló biztonsági szempontból lényeges eseményeket (például naplótár túlcsordulás; rendszerösszeomlás; felhasználói rekordok felülírása, mint amikor egy felhasználó távozik a

szervezettől, és a fiókját eltörlik) kellően meg kell határozni, hogy a felhasználó beavatkozhasson a biztonságos működés fenntartása érdekében.

AGD_OPE.1.5C Az üzemeltetési felhasználói útmutatónak azonosítani kell a TOE összes lehetséges üzemeltetési módját (beleértve a meghibásodás vagy üzemeltetési hiba utáni műveleteket is), valamint ezek biztonságos üzemeltetésre gyakorolt következményeit és kihatásait.

AGD_OPE.1-5 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót és az egyéb értékeléshez adott bizonyítékot annak megállapítása érdekében, hogy az útmutató azonosítja-e a TOE összes lehetséges üzemmódját (beleértve a meghibásodás vagy üzemeltetési hiba utáni működést is, amennyiben ilyen előfordulhat), valamint ezek következményét és kihatásait a biztonságos üzemelés fenntartására.
Más értékelési bizonyítékot, elsősorban a funkcionális specifikációt az értékelőnek annak megállapításához javasolt használnia, hogy az útmutató megfelelő eligazító leírást tartalmaz-e.

Amennyiben a garanciacsomaghoz tesztdokumentáció van csatolva, akkor az ebben a bizonyítékban nyújtott információ is felhasználható annak eldöntésére, hogy az útmutató elegendő útmutató információt tartalmaz-e. A tesztlépéseknél megadott részletek felhasználhatók annak megerősítésére, hogy a nyújtott útmutató elégséges a TOE használatához és adminisztrálásához.

Az értékelőnek egy időben egy ember számára látható TSFI-t ajánlott vizsgálnia, úgy, hogy összehasonlítja a TSFI biztonságos használatáról szóló útmutatást egyéb bizonyítékokkal, annak kiderítése érdekében, hogy a TSFI-vel kapcsolatos információk valóban jól írják-e le annak biztonságos használatát (azaz megfelelnek-e az SFR-eknek). Az értékelőnek az interfészek közötti kapcsolatokat is át kell néznie, potenciális ellentmondásokat keresve.

AGD_OPE.1.6C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre le kell írnia azokat a betartandó biztonsági intézkedéseket, melyek az ST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célok elérését szolgálják.

AGD_OPE.1-6 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e azokat a betartandó biztonsági intézkedéseket, melyek az ST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célok elérését szolgálják.

Az értékelő elemezze az ST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célokat, majd állapítsa meg, hogy az üzemeltetési felhasználói útmutató minden felhasználói szerepkörre megfelelően leírja-e a fontos biztonsági intézkedéseket.

Az üzemeltetési felhasználói útmutatóban leírt biztonsági intézkedéseknek magukban kell foglalniuk az összes fontos külső eljárásrendi, fizikai, személyzeti és kapcsolódásra vonatkozó intézkedést.

Megjegyzendő, hogy a TOE biztonságos telepítésére vonatkozó intézkedéseket az Előkészítő eljárások (AGD_PRE) vizsgálja.

AGD_OPE.1.7C Az üzemeltetési felhasználói útmutatónak egyértelműnek és megalapozottnak kell lennie.

AGD_OPE.1-7 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az egyértelmű-e.

Az útmutató akkor nem egyértelmű (félrevezető), ha ez alapján egy egy felhasználó indokoltan félreértheti teendőit, és a TOE-ra vagy a TOE által nyújtott biztonságra nézve hátrányos módon alkalmazza a leírtakat.

AGD_OPE.1-8 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az megalapozott-e.

Az útmutató akkor tekinthető megalapozatlannak, ha olyan követelményeket támaszt a TOE használatával vagy üzemeltetési környezetével szemben, melyek nem felelnek meg az ST-nek, vagy indokolatlanul nagy terhet jelentenek a biztonság fenntartásához.

6.2.4.2.2. Előkészítő eljárások: Az AGD_PRE.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a TOE biztonságos előkészületi eljárásait és lépéseit dokumentálták, s hogy ezek biztonságos konfigurációt eredményeznek.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) a TOE, beleértve az előkészítő eljárásait,
c) a fejlesztő szállítási eljárásainak leírása.

Az előkészületi eljárások az összes olyan elfogadási és telepítési eljárást jelentik, melyek ahhoz szükségesek, hogy a TOE-t az ST-ben leírt biztonságos konfiguráció állapotába juttassák.

6.2.4.2.2.1. Az AGD_PRE.1.1E értékelői akció

AGD_PRE.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

AGD_PRE.1.1C Az előkészítő eljárásoknak le kell írniuk a leszállított TOE biztonságos elfogadásához szükséges valamennyi lépést, a fejlesztő szállítási eljárásaival összhangban.

AGD_PRE.1-1 Az értékelőnek ellenőriznie kell, hogy biztosították-e a leszállított TOE biztonságos elfogadásához szükséges eljárásokat.

Amennyiben a fejlesztő szállítási eljárásaival kapcsolatban nem várható elfogadási eljárások alkalmazása, akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

AGD_PRE.1-2 Az értékelőnek meg kell vizsgálnia a biztosított elfogadási eljárásokat annak megállapítása érdekében, hogy azok leírják-e a TOE biztonságos elfogadásához szükséges lépéseket, a fejlesztő szállítási eljárásaival összhangban.

Az elfogadási eljárásoknak legalább az arra vonatkozó felhasználói ellenőrzést tartalmazniuk kell, hogy a TOE valamennyi részét az ST-ben jelzett helyes verziókkal szállították-e le.

Az elfogadási eljárásoknak tükrözniük kell azokat a felhasználó által a leszállított TOE elfogadásához alkalmazott lépéseket, melyek a fejlesztő szállítási eljárásaiból származnak.

Az elfogadási eljárásoknak részletes információt kell szolgáltatniuk az alábbiakhoz, amennyiben azok alkalmazhatók:

a) az arról való meggyőződés, hogy a leszállított TOE a teljes értékelt példány.
b) a leszállított TOE módosításának vagy hamisításának az észlelése.

AGD_PRE.1.2C Az előkészítő eljárásoknak le kell írniuk a TOE biztonságos telepítéséhez, valamint az üzemeltetési környezethez való biztonságos előkészülethez szükséges valamennyi lépést, az ST-ben leírt, üzemeltetési környezetre vonatkozó biztonsági célokkal összhangban.

AGD_PRE.1-3 Az értékelőnek ellenőriznie kell, hogy biztosították-e a TOE biztonságos telepítéséhez szükséges eljárásokat.

Amennyiben a TOE-vel és üzemeltetési környezetével kapcsolatban nem várható telepítési eljárások alkalmazása (mert például a TOE-t már működésre alkalmas állapotban szállították le, s nincsenek a környezetére vonatkozó követelmények), akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

AGD_PRE.1-4 Az értékelőnek meg kell vizsgálnia a biztosított telepítési eljárásokat annak megállapítása érdekében, hogy azok leírják-e a TOE biztonságos telepítéséhez, valamint az üzemeltetési környezet biztonságos előkészítéséhez szükséges lépéseket, az ST biztonsági céljaival összhangban.

Amennyiben nem várható telepítési eljárások alkalmazása (mert például a TOE-t már működésre alkalmas állapotban szállították le, s nincsenek a környezetére vonatkozó követelmények), akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

A telepítési eljárásoknak részletes információt kell szolgáltatniuk az alábbiakról, amennyiben azok alkalmazhatók:

a) a biztonságos telepítéshez szükséges minimális rendszer követelmények,
b) az üzemeltetési környezetre vonatkozó követelmények, az ST-ben meghatározott biztonsági célokkal összhangban,
c) a TSF ellenőrzése alatt álló egyedek telepítés-specifikus biztonsági tulajdonságainak módosítása,
d) kivételek és problémák kezelése.

6.2.4.2.2.2. Az AGD_PRE.1.2E értékelői akció

AGD_PRE.1.2E Az értékelőnek végre kell hajtania az előkészítő eljárásokat annak megerősítése érdekében, hogy a TOE biztonságosan előkészíthető a működésre.

Az előkészítés megköveteli az értékelőtől, hogy a TOE-t egy leszállításra alkalmas állapotból olyan állapotba állítsa át, amelyben a TOE üzemel, beleértve a TOE elfogadását és telepítését, valamint az ST-ben megadott biztonsági célokkal összhangban álló SFR-ek érvényre juttatását.

Az értékelőnek a TOE elfogadására és telepítésére kizárólag a fejlesztői eljárásokat szabad követnie, s csak a vásárlóktól általánosan elvárt tevékenységeket szabad végrehajtania, csak az előkészületi útmutatót használva. A végrehajtás során tapasztalt bármilyen nehézség hiányos, nem egyértelmű vagy megalapozatlan útmutatót jelenthet.

Az értékelő ezt a munkaegységet végrehajthatja a „Független tesztelés – minta” (ATE_IND.2) értékelési altevékenységgel együtt.

6.2.4.3. Az Életciklus támogatás garanciaosztály (ALC) értékelése

Az életciklus támogatáshoz kapcsolódó tevékenységnek az a célja, hogy elbírálja a fejlesztő által a TOE fejlesztése és kezelése során használt biztonsági eljárások megfelelőségét. Ezek az eljárások a fokozott garanciaszinten magukban foglalják a fejlesztő által használt életciklus modellt, a konfiguráció kezelést, a TOE fejlesztése során alkalmazott biztonsági intézkedéseket és a szállítási tevékenységet.

A TOE elégtelenül ellenőrzött fejlesztése és kezelése sebezhetőségekhez vezethet a megvalósításban. Egy definiált életciklus modellnek való megfelelőség elősegítheti az intézkedések javítását ezen a területen. Egy, a TOE-hoz alkalmazott felmérhető életciklus modell megszüntetheti a félreérthetőségeket a TOE fejlesztési eljárásának kiértékelésében.

A konfiguráció kezeléshez kapcsolódó tevékenységnek az a célja, hogy segítséget nyújtson a fogyasztónak az értékelt TOE beazonosításában, hogy biztosítsa a konfiguráció elemek egyedi azonosítását, és biztosítsa a fejlesztő által a TOE-n történt változtatások ellenőrzéséhez és nyomonkövetéséhez használt eljárások megfelelőségét. Ez magában foglalja az arra vonatkozó részleteket, hogy milyen változtatások vannak nyomonkövetve, hogy a lehetséges változtatások hogyan vannak beépítve, és magában foglalja, hogy milyen mértékben használnak automatizálást a hibalehetőségek csökkentésére.

A fejlesztő biztonsági eljárásainak az a célja, hogy védjék a TOE-t és a kapcsolódó tervezési információkat a hamisításokkal vagy felfedésekkel szemben. A fejlesztési folyamatba történő hamisítás lehetővé teheti sebezhetőségek szándékos bevitelét. A tervezési információk felfedése lehetővé teheti a sebezhetőségek könnyebb kiaknázhatóságát. Az eljárások megfelelősége a TOE és a fejlesztési folyamat természetétől függ.

A szállításhoz kapcsolódó tevékenység célja annak az elbírálása, hogy megfelelő azoknak az eljárásoknak a dokumentációja, amelyek biztosítják, hogy a TOE-t változtatás nélkül szállítják ki a fogyasztóhoz.

6.2.4.3.1. Konfiguráció kezelési képességek: Az ALC_CMC.3 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztő használ-e egy konfiguráció kezelés rendszert, mely egyértelműen azonosít minden konfiguráció elemet, valamint hogy megfelelő módon ellenőrzik-e ezen elemek módosíthatóságát.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) a tesztelésre alkalmas TOE,
c) a konfiguráció kezelési dokumentáció.

6.2.4.3.1.1. Az ALC_CMC.3.1E értékelői akció

ALC_CMC.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ALC_CMC.3.1C A TOE-t meg kell jelölni egyedi hivatkozásával.

ALC_CMC.3-1 Az értékelőnek ellenőriznie kell, hogy az értékelésre benyújtott TOE verzióját megjelölték-e hivatkozásával.

Az értékelőnek gondoskodnia kell arról, hogy a TOE tartalmazza az ST-ben megadott egyedi hivatkozást. Ez elérhető megjelölt csomagolással vagy adathordozóval, illetve a működő TOE által megjelenített címkével. Ez biztosítja, hogy a vásárlók is képesek a TOE megfelelő azonosítására (a vásárlás vagy használat időpontjában).

A TOE biztosíthat is egy olyan módszert, mellyel egyszerűen azonosítható. Például egy szoftver TOE induláskor vagy egy parancs-sorra adott válaszként kijelezheti nevét és verziószámát. Egy hardver vagy förmver TOE azonosítható a TOE-ra fizikailag rábélyegzett sorozatszámmal.

ALC_CMC.3-2 Az értékelőnek ellenőriznie kell, hogy az alkalmazott TOE hivatkozások ellentmondás mentesek-e.

Amennyiben a TOE-t egynél több helyen jelölik meg (címkézik), akkor a címkéknek egyezniük kell. Lehetséges például, hogy a TOE részeként biztosított, címkézett útmutató dokumentációkat az értékelt működő TOE-hez kapcsoljuk. Ez biztosítja, hogy a vásárlók biztosak legyenek abban, hogy a TOE értékelt verzióját vették meg, telepítették, és az útmutató dokumentációból is a helyes verzióval rendelkeznek, az ST-nek megfelelő üzemeltetés érdekében.

Az értékelő azt is ellenőrizze, hogy a TOE hivatkozása megegyezik-e az ST-ben szereplővel.

ALC_CMC.3.2C A konfiguráció kezelés dokumentációnak le kell írnia a konfiguráció elemek egyértelmű azonosítására alkalmazott módszert.

ALC_CMC.3-3 Az értékelőnek meg kell vizsgálnia a konfiguráció elemek azonosításához alkalmazott módszert, annak megállapítása érdekében, hogy az leírja-e azt, hogy hogyan azonosítják egyedileg a konfiguráció elemeket.

Eljárások ismertessék, hogy az egyes konfiguráció elemek állapota hogyan követhető nyomon a TOE életciklusa során. Az eljárások részletezve lehetnek a CM tervben vagy különböző CM dokumentumban. A tartalmazott információ ismertesse a következőket:

a) azt a módszert, ahogyan az egyes konfiguráció elemek egyedileg azonosítva lettek, hogy lehetséges legyen ugyanazon konfiguráció elem verzióinak nyomonkövetése;
b) azt a módszert, ahogyan a konfiguráció elemekhez egyedi azonosítókat jelölnek ki, és ahogyan ezek a CM rendszerbe bekerülnek;
c) azt a módszert, amely egy konfiguráció elem kiváltott verzióinak beazonosítására szolgál.

ALC_CMC.3.3C A konfiguráció kezelés rendszernek egyértelműen azonosítania kell minden konfiguráció elemet.

ALC_CMC.3-4 Az értékelőnek meg kell vizsgálnia a konfiguráció elemeket annak megállapítása érdekében, hogy azokat a konfiguráció kezelés rendszernek megfelelő módon azonosították.

Arra vonatkozó garancia, hogy a CM rendszer minden konfiguráció elemet egyedileg azonosít, a konfiguráció elemek azonosítóinak vizsgálatán keresztül nyerhető. Mind a TOE-t alkotó konfiguráció elemekre, mind pedig a fejlesztő által értékelési bizonyítékként átadott konfiguráció elem leírásokra vonatkozóan az értékelőnek meg kell erősítenie, hogy minden konfiguráció elem olyan egyedi azonosítóval rendelkezik, amely összhangban áll a CM dokumentációban ismertetett egyedi azonosítási módszerrel.

ALC_CMC.3.4C A konfiguráció kezelés rendszernek olyan eszközöket kell biztosítania, mely csak jogosult változtatásokat enged végrehajtani a konfiguráció elemekben.

ALC_CMC.3-5 Az értékelőnek meg kell vizsgálnia a konfiguráció kezelési tervben leírt hozzáférés ellenőrzési intézkedéseket annak megállapítása érdekében, hogy azok hatékonyan meggátolják-e a konfiguráció elemekhez való jogosulatlan hozzáféréseket.

Az értékelő többféleképpen is megállapíthatja a konfiguráció kezelés hozzáférés ellenőrzési intézkedéseinek hatékonyságát. Például az értékelő gyakorlati próbával győződhet meg azok kikerülhetetlenségéről. Az értékelő használhatja a konfiguráció kezelés rendszer (ALC_CMC.3.8C által megkövetelt) eljárásainak kimeneteit is. Az értékelő végignézhet egy olyan bemutatót is, mely a hozzáférés ellenőrzési intézkedések hatékony működését szemléltetik.

ALC_CMC.3.5C A konfiguráció kezelés dokumentációnak tartalmaznia kell egy konfiguráció kezelés tervet.

ALC_CMC.3-6 Az értékelőnek ellenőriznie kell, hogy a konfiguráció kezelés rendszer tartalmaz-e konfiguráció kezelés tervet.

A konfiguráció kezelés tervnek nem feltétlenül kell egy összefüggő dokumentumnak lennie, bár ajánlott, hogy legyen egy különálló dokumentum, mely leírja, hogy a konfiguráció kezelés terv különböző részei hol találhatók. Amennyiben a konfiguráció kezelés tervet több dokumentum együtteseként biztosítják, a következő munkaegység útmutatót ad az elvárt tartalomra.

ALC_CMC.3.6C A konfiguráció kezelés tervnek le kell írnia a konfiguráció kezelés rendszer TOE fejlesztéséhez történő használatát.

ALC_CMC.3-7 Az értékelőnek meg kell vizsgálnia a konfiguráció kezelés tervet annak megállapítása érdekében, hogy leírja-e azt, hogyan használják a konfiguráció kezelés rendszert a TOE fejlesztéséhez.

A konfiguráció kezelés terv az alábbiakat tartalmazhatja:

a) a TOE fejlesztői környezetében végrehajtott minden tevékenység, mely a konfiguráció kezelés hatáskörébe esik (pl. egy konfiguráció elem létrehozása, módosítása vagy törlése, adatmentés, archiválás);
b) milyen eszközök elérése szükséges (konfiguráció kezelés eszköz, űrlapok);
c) a konfiguráció kezelés eszközök használata: a konfiguráció kezelés rendszert használóknak szükséges részletek az eszközök helyes használatára, a TOE sértetlenségének biztosítása érdekében;
d) a konfiguráció kezelés hatáskörébe eső egyéb objektumok (fejlesztő komponensek és eszközök, vizsgáló környezetek, stb.);
e) az egyes konfiguráció elemeken a műveleteket végrehajtó szerepkörök és felelősségek (különböző típusú konfiguráció elemekre (pl. tervdokumentáció vagy forráskód) különböző lehet a szerepkör);
f) kik és hogyan határozhatnak a változásokról, interfész módosításról;
g) a változás kezelés leírása;
h) azon eljárások, melyek azt biztosítják, hogy a konfiguráció elemeken csak jogosult egyének végezhessenek módosításokat;
i) azon eljárások, melyek azt biztosítják, hogy segítségükkel a konfiguráció elemeken végzett egyidejű módosítások nem okoznak problémákat;
j) az eljárások alkalmazásának eredményeképp létrejött bizonyíték. Például egy konfiguráció elem változtatása esetén a konfiguráció kezelés rendszer a változtatás nyomon követhetősége érdekében naplózhatja a változtatás leírását, minden érintett konfiguráció elem azonosításával, a változtatás állapotával (felfüggesztett vagy befejezett), dátumával és időpontjával.
k) a verziókövetés és a TOE verziók egyedi hivatkozásához használt módszer (pl. operációs rendszer javítások kibocsátása, ezek alkalmazásának detektálása).

ALC_CMC.3.7C Bizonyítéknak kell kimutatnia, hogy konfiguráció kezelés rendszer minden konfiguráció elemet kezel.

ALC_CMC.3-8 Az értékelőnek ellenőriznie kell, hogy a konfiguráció listában azonosított konfiguráció elemeket a konfiguráció kezelés rendszerben kezelik-e.

A fejlesztő által alkalmazott konfiguráció kezelés rendszernek fenn kell tartania a TOE sértetlenségét. Az értékelő ellenőrizze, hogy minden konfiguráció elem típus (pl. terv

dokumentáció vagy forrás kód modulok) esetén vannak-e a konfiguráció kezelés tervben leírt eljárások szerint generált bizonyíték példák. Ekkor a mintavételezési módszer a konfiguráció kezelés rendszerben használt tagoltság szintjétől függ. Amennyiben például 10.000 forráskód modul szerepel a konfiguráció listában, nyilván más mintavételezési stratégiát szükséges követni, mintha csak 1 vagy 5. A tevékenység célja nem az apró hibák felderítése, hanem annak biztosítása, hogy a konfiguráció kezelés rendszer helyesen működik.

A mintavételezésre útmutató található a 7.2.1 pontban.

ALC_CMC.3.8C Bizonyítéknak kell kimutatnia, hogy a konfiguráció kezelés rendszer a konfiguráció kezelés tervnek megfelelően működik.

ALC_CMC.3-9 Az értékelőnek ellenőriznie kell a konfiguráció kezelés dokumentációt annak kiderítéséhez, hogy tartalmazza-e a konfiguráció kezelés terv által meghatározott konfiguráció kezelés rendszer rekordokat.

A konfiguráció kezelés rendszer kimenetének bizonyítékot kell szolgáltatnia ahhoz, hogy az értékelő meg tudjon győződni arról, hogy a konfiguráció kezelés tervet valóban alkalmazzák-e, valamint a konfiguráció kezelés rendszer minden konfiguráció elemet kezel-e, ahogy azt az ALC_CMC.3.7C megköveteli. Egy példa kimenet tartalmazhat változáskezelési űrlapokat vagy konfiguráció elem hozzáférést jóváhagyó nyomtatványokat.

ALC_CMC.3-10 Az értékelőnek meg kell vizsgálnia a bizonyítékot annak meghatározása érdekében, hogy a konfiguráció kezelés rendszert a konfiguráció kezelés tervben szereplő módon használják.

Az értékelőnek ki kell választania minden konfiguráció kezelés szempontból fontos művelettípusra (pl. létrehozás, módosítás, törlés, korábbi verzióra visszatérés stb.) egy bizonyíték mintát annak megerősítése céljából, hogy a munkát a dokumentált eljárásoknak megfelelően végezték el. Az értékelőnek meg kell erősítenie, hogy a bizonyíték tartalmazza az összes információt, mely a konfiguráció kezelés tervben az adott műveletre elő van írva. A bizonyíték vizsgálata hozzáférést igényelhet a használt konfiguráció kezelés eszközhöz. Az értékelő használhat mintavételezést ehhez a munkához.

A mintavételezésre útmutató található a 7.2.1 pontban.

A fejlesztői csoport kiválasztott tagjaival készült interjú révén kiegészítő bizonyosságot szerezhet az értékelő a konfiguráció kezelés rendszer helyes használatáról, illetve a konfiguráció elemek hatékony kezeléséről. Az ilyen interjúk segítségével az értékelő mélyebb ismereteket szerezhet a konfiguráció kezelés rendszer használatáról, egyúttal megerősítést nyerhet, hogy a konfiguráció kezelés eljárásait valóban a konfiguráció kezelés dokumentációban leírt módon alkalmazzák. Az ilyen interjúk azonban inkább csak kiegészítik, s nem helyettesítik a dokumentációs bizonyítékok vizsgálatát, s nem is szükségesek, ha a dokumentációs bizonyítékok egyedül kielégítik az elvárásokat. Olyan esetben, amikor bizonyos szempontokat (pl. szerepköröket és felelősségeket) a konfiguráció kezelés tervből nem sikerül teljes körűen felderíteni, az interjún alapuló módszer megoldást adhat.

E tevékenység végrehajtása során az értékelőnek várhatóan meg kell látogatnia a fejlesztés helyszínét.

A fejlesztői helyszín meglátogatására útmutató található a melléklet 7.2.3 pontjában.

6.2.4.3.2. Konfiguráció kezelés hatóköre: Az ALC_CMS.3 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a konfiguráció lista tartalmazza-e a TOE-t, a TOE-t alkotó részeket, a TOE megvalósítási reprezentációját, valamint az értékelési bizonyítékokat.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) a konfiguráció lista.

6.2.4.3.2.1. Az ALC_CMS.3.1E értékelői akció

ALC_CMS.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ALC_CMS.3.1C A konfiguráció listának tartalmaznia kell a következőket: maga a TOE; a garanciális biztonsági követelmények (SAR) által megkövetelt értékelési bizonyítékok, a TOE-t alkotó részek és a megvalósítási reprezentáció.

ALC_CMS.3-1 Az értékelőnek ellenőriznie kell, hogy a konfiguráció lista tartalmazza-e az alábbi elem készletet:

a) maga a TOE;
b) a TOE-t alkotó részek;
c) a TOE megvalósítási reprezentációja;
d) az ST garanciális biztonsági követelményei (SAR) által megkövetelt értékelési bizonyítékok.

ALC_CMS.3.2C A konfiguráció listának egyértelműen azonosítania kell a konfiguráció elemeket.

ALC_CMS.3-2 Az értékelőnek meg kell vizsgálnia a konfiguráció listát annak megállapítása érdekében, hogy az egyértelműen azonosít-e minden konfiguráció elemet.

A konfiguráció lista elegendő információt tartalmazzon ahhoz, hogy egyértelműen azonosítja az összes konfiguráció elem használt verzióját (ez tipikusan egy verzió szám). Ezen lista használatával az értékelő ellenőrizheti, hogy az értékelés a helyes konfiguráció elemekre, és mindegyikük helyes verziójára irányul.

ALC_CMS.3.3C A konfiguráció listának a TSF szempontból fontos minden konfiguráció elemre meg kell adni az elem fejlesztőjét.

ALC_CMS.3-3 Az értékelőnek ellenőriznie kell, hogy a konfiguráció lista megadja-e a TSF szempontból fontos összes konfiguráció elem fejlesztőjét.

Amennyiben a TOE fejlesztésében csak egy fejlesztő érintett, akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

6.2.4.3.3. Szállítás: Az ALC_DEL.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a szállítási dokumentáció leírja-e az összes olyan eljárást, amelyet a TOE biztonság fenntartásához használnak a vásárlókhoz történő szállítás során.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) a szállítási dokumentáció.

6.2.4.3.3.1. Az ALC_DEL.1.1E értékelői akció

ALC_DEL.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ALC_DEL.1.1C A szállítási dokumentációnak le kell írnia minden olyan eljárást, amely a TOE verzióinak vásárlókhoz történő szállítása során a biztonság fenntartásához szükséges.

ALC_DEL.1-1 Az értékelőnek meg kell vizsgálnia a szállítási dokumentációt annak megállapítása érdekében, hogy az leírja-e az összes olyan eljárást, amely a TOE vagy részei verzióinak felhasználókhoz történő szállítása során a biztonság fenntartásához szükségesek.

A szállítási eljárások leírják a TOE vagy összetevőinek szállítása során a TOE biztonságának fenntartására, valamint a TOE azonosítására alkalmas eljárásokat.

A szállítási dokumentáció az egész TOE-re vonatkozik, ugyanakkor a TOE különböző részeire különböző eljárások vonatkozhatnak. Az értékelésnek az eljárások összességét figyelembe kell vennie.

A szállítási eljárásokat a szállítás teljes folyamatában, a gyártási környezettől a telepítési környezetig alkalmazni kell (például csomagolás, tárolás és szétosztás). A csomagolás és szállítás szabványos kereskedelmi gyakorlata elfogadható lehet. Ez magában foglalja a zsugorfóliás csomagolást, a biztonsági csíkot vagy egy pecsételt borítékot. A szétosztásra fizikai (pl. nyilvános levelezés vagy magán szolgáltató) vagy elektronikus (pl. elektronikus mail vagy interneten keresztüli letöltés) eljárások alkalmazhatók.

A fejlesztő kriptográfiai ellenőrző összegeket vagy elektronikus aláírást használhat a módosítás vagy a hamisítás észlelhetősége érdekében. A hamisítás ellen védő pecsétek a bizalmasság megsértését is jelzik. Szoftver TOE esetén a bizalmasság titkosítás

alkalmazásával biztosítható. Amennyiben a rendelkezésre állás fontos szempont, megbízható továbbítás követelhető meg.

A "biztonság fenntartásához szükséges" kitétel értelmezésekor figyelembe kell venni az alábbiakat:

- a TOE jellege (pl. szoftver vagy hardver),
- A TOE-ra kinyilvánított általános, a sebezhetőség vizsgálatnál megválasztott biztonsági szint. Amennyiben a TOE-nak üzemeltetési környezetében ellent kell állnia egy bizonyos támadó képességgel rendelkező támadókkal szemben, akkor ez a TOE szállítására is alkalmazandó. Az értékelőnek meg kell állapítania, hogy kiegyensúlyozott megközelítést alkalmaztak-e annak érdekében, hogy a szállítás ne jelentsen gyenge pontot egy egyébként biztonságos fejlesztési folyamatban.
- Az ST által meghatározott biztonsági célok. A szállítási dokumentációknál a hangsúly valószínűleg a sértetlenséggel kapcsolatos intézkedéseken lesz. Ugyanakkor bizonyos TOE-k szállítása esetében a bizalmasság és a rendelkezésre állás is kiemelt fontosságú, ilyenkor ezeket a szempontokat is vizsgálni kell.

Az ALC_DEL.1.2D bizonyítékból származtatott értékelői akció

ALC_DEL.1.2D A fejlesztőnek használnia kell a szállítási eljárásokat.

ALC_DEL.1-2 Az értékelőnek meg kell vizsgálnia a szállítási folyamat különböző oldalait annak megállapítása érdekében, hogy alkalmazzák-e a szállítási eljárásokat.

Az értékelő megközelítési módszere a szállítás alkalmazásának ellenőrzésével kapcsolatban a TOE jellegétől és magától a szállítási folyamattól függ. Az eljárások vizsgálatán túl az értékelőnek valamilyen szinten meg kell győződnie arról, hogy a szabályokat a gyakorlatban is betartják. Lehetséges megközelítési módok az alábbiak:

a) látogatás a szétosztási hely(ek)en, ahol megfigyelhető az eljárások gyakorlati alkalmazása;
b) a TOE átvizsgálása a szállítás valamelyik fázisában vagy a felhasználó telephelyén (például a hamisítás ellen védő pecsétek ellenőrzése);
c) a szállítási folyamat alkalmazásának megfigyelése a gyakorlatban, amikor az értékelő a TOE-t szabályos csatornákon keresztül szerzi be;
d) a végfelhasználók megkérdezése a TOE szállítás folyamatáról.

A helyszíni szemlékre útmutató található a 7.2.3 pontban.

Egy újonnan fejlesztett TOE esetén előfordulhat, hogy a TOE szállítási eljárásait még nem vezették be a gyakorlatban. Ekkor az értékelőnek meg kell elégednie azzal, hogy a megfelelő eljárásokat és eszközöket kialakították a jövőbeli szállításokra, és minden érintett alkalmazott tisztában van a felelősségével. Az értékelő kérheti a szállítás egy “száraztesztjét”, amennyiben ez célszerűnek tűnik. Amennyiben a fejlesztő már korábban létrehozott hasonló terméket, akkor az ott bevezetett eljárások vizsgálata is segíthet az aktuális termékkel kapcsolatos garancia megállapításában.

6.2.4.3.4. Fejlesztés biztonság: Az ALC_DVS.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztő fejlesztési környezetre vonatkozó ellenintézkedései megfelelők-e, alkalmasak-e a TOE tervek és a TOE megvalósítás bizalmasságának és sértetlenségének megvédésére, biztosítva ezzel, hogy a TOE biztonságos működése ne kompromittálódjon.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) a fejlesztés biztonsági dokumentáció.

Az értékelőnek szüksége lehet egyéb értékelői bizonyíték megvizsgálására is annak megállapítása érdekében, hogy a biztonsági intézkedések jól meghatározottak-e, s követik-e ezeket. Speciálisan, az értékelőnek szüksége lehet a fejlesztő (az ALC_CMC.3 és ALC_CMS.3 altevékenységek bemenetét képező) konfiguráció kezelési dokumentációjának megvizsgálására. Az eljárások alkalmazására vonatkozó bizonyítékokat is megkövetelik.

6.2.4.3.4.1. Az ALC_DVS.1.1E értékelői akció

ALC_DVS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ALC_DVS.1.1C A fejlesztés biztonsági dokumentációnak le kell írnia minden olyan fizikai, eljárásbeli, személyi és egyéb biztonsági intézkedést, mely a TOE tervek és TOE megvalósítás bizalmasságának és sértetlenségének a védelméhez szükséges, fejlesztési környezetében.

ALC_DVS.1-1 Az értékelőnek meg kell vizsgálnia a fejlesztői biztonsági dokumentációt annak megállapítása érdekében, hogy az részletezi-e az összes olyan, fejlesztői környezetben használt biztonsági intézkedést, melyek a TOE tervek és a TOE megvalósítás bizalmasságának és sértetlenségének megőrzését szolgálják.
Az értékelő először azt határozza meg, hogy mire van szükség a kellő védelemhez. Ehhez használja az ST információit, különösen a fejlesztési környezetre vonatkozó biztonsági célokat.

Az ST-ből származó közvetlen információ hiányában az értékelőnek kell meghatároznia a szükséges biztonsági mértéket. Olyan esetben, amikor a fejlesztő alulbecsülte a szükséges biztonsági mértéket, egy lehetséges sebezhetőséggel való visszaélésen alapuló világos indoklást kell erre adni.

Az értékelőnek az alábbi típusú biztonsági intézkedéseket kell számba vennie a dokumentáció vizsgálatakor:

a) *fizikai*, például fizikai hozzáférés védelmi intézkedések a TOE fejlesztői környezethez való jogosulatlan hozzáférés megakadályozására (munkaidőben és azon kívül);
b) *eljárásbeli*, például:

ba) a fejlesztői környezethez vagy annak bizonyos elemeihez (pl. fejlesztő berendezésekhez) való hozzáférés biztosítása;
bb) hozzáférési jogok visszavonása, ha egy személy elhagyja a fejlesztői csoportot;
bc) védett anyag továbbítása a fejlesztői környezeten belül, kívülre, illetve (a meghatározott elfogadási eljárásokkal összhangban) a különböző fejlesztői környezetek között ;
bd) látogatók beengedése és kísérése a fejlesztői környezetben;
be) szerepkörök és felelősségek a biztonsági intézkedések folyamatos betartásában, és a biztonsági szabályszegések észlelésében.

c) *személyi*, például egy új fejlesztő megbízhatóságának ellenőrzése;
d) *egyéb biztonsági intézkedések*, például a fejlesztői eszközök logikai védelme.

A fejlesztői biztonsági dokumentációnak azonosítania kell a fejlesztési helyszíneket, valamint le kell írnia a végrehajtott fejlesztés különböző oldalait, az egyes helyszíneken alkalmazott biztonsági intézkedésekkel együtt. A fejlesztésre sor kerülhet például egyetlen épület több helyszínén, egy telephely több épületében, vagy több telephelyen. TOE részek vagy befejezetlen TOE-k szállítása különböző fejlesztési helyszínek között a Fejlesztés biztonság (ALC_DVC), míg a kész TOE vásárlóhoz továbbítása a Szállítás (ALC_DEL) hatáskörébe tartozik.

A fejlesztés magában foglalja a TOE előállítását is.

ALC_DVS.1-2 Az értékelőnek meg kell vizsgálnia a fejlesztés bizalmasságát és sértetlenségét, annak megállapítása érdekében, hogy az alkalmazott biztonsági intézkedések kielégítők-e.

Az alábbi jellegű szabályok tartoznak ide:

a) a TOE fejlesztéssel kapcsolatos milyen információkat kell bizalmasan kezelni, és a fejlesztői csoport mely tagjai férhetnek hozzá ilyen anyagokhoz;
b) milyen anyagokat kell védeni a jogosulatlan módosítástól a TOE sértetlenségének megőrzése érdekében, és a fejlesztők közül kik jogosultak az ilyen anyagok módosítására.

Az értékelőnek meg kell állapítania, hogy a fejlesztői biztonsági dokumentáció tartalmazza-e ezeket a szabályokat, az alkalmazott biztonsági intézkedések megfelelnek-e a szabályoknak, és a szabályok köre teljes-e.

Amíg a „Konfiguráció kezelés képességei” (ALC_CMC) követelményei rögzítettek, a „Fejlesztés biztonsága” (ALC_DVS) csak a szükséges intézkedéseket követeli meg, s ezek függnek a TOE természetétől, s az ST-ben megadott információktól. Például az ST a fejlesztési környezetre meghatározhat egy olyan biztonsági célt, amely megköveteli, hogy a TOE-t olyan fejlesztők dolgozzák ki, akik biztonsági engedéllyel rendelkeznek. Az értékelőnek ekkor ebben az altevékenységben meg kell állapítania, hogy alkalmaztak-e ilyen szabályt.

6.2.4.3.4.2. Az ALC_DVS.1.2E értékelői akció

ALC_DVS.1.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági intézkedéseket betartják.

ALC_DVS.1-3 Az értékelőnek meg kell vizsgálnia a fejlesztési biztonság dokumentációt és az ahhoz kapcsolódó bizonyítékokat annak megállapítása érdekében, hogy a biztonsági intézkedéseket betartották-e.

Ebben a munkaegységben az értékelőnek meg kell állapítania, hogy a fejlesztési biztonság dokumentációban megfogalmazott biztonsági intézkedéseket alkalmazták-e a TOE sértetlenségének és a kapcsolódó dokumentáció bizalmasságának megfelelő védelme érdekében. Ez meghatározható például a dokumentált bizonyítékok vizsgálatával, melyet kiegészíthet a fejlesztői környezetben tett látogatás. A látogatás során az értékelő:

a) megfigyelheti a biztonsági intézkedések alkalmazását (pl. fizikai védelmi intézkedések);
b) megvizsgálhatja az eljárások alkalmazásának dokumentált bizonyítékát;
c) megkérdezheti, ellenőrizheti a fejlesztőket, hogy tisztában vannak-e a fejlesztés biztonsági szabályaival és eljárásaival, valamint saját felelőségükkel.

A fejlesztői helyszín meglátogatása hasznos módszer az alkalmazott intézkedések megbízhatóságának megítélésében. A látogatás elhagyását meg kell beszélni a tanúsító szervezettel.

A fejlesztői helyszín meglátogatására útmutató található a melléklet 7.2.3 pontjában.

6.2.4.3.5. Életciklus meghatározás: Az ALC_LCD.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztő használ-e dokumentált modellt a TOE életciklusára.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) az életciklus meghatározás dokumentáció.

6.2.4.3.5.1. Az ALC_LCD.1.1E értékelői akció

ALC_LCD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ALC_LCD.1.1C Az életciklus modell dokumentációnak le kell írnia a TOE fejlesztéséhez és karbantartásához használt modellt.

ALC_LCD.1-1 Az értékelőnek meg kell vizsgálnia az alkalmazott életciklus modell dokumentált leírását, annak megállapítása érdekében, hogy az lefedi-e a fejlesztési és karbantartási folyamatot.

Az életciklus modell leírásának az alábbiakat kell tartalmaznia:

a) a TOE életciklus fázisaira (fő folyamataira), illetve az egymást követő fázisok közötti átmenetre vonatkozó információk,
b) a fejlesztő által használt eljárásokra, eszközökre és technikákra (pl. a tervezéshez, kódolásra, tesztelésre, hibajavításra) vonatkozó információk,
c) az eljárások alkalmazását felügyelő átfogó menedzsment szerkezet (pl. az életciklus modell által lefedett fejlesztési és karbantartási folyamatban megkövetelt eljárások mindegyikére az egyedi felelősségi körök azonosítása és leírása),
d) arra vonatkozó információ, hogy a TOE mely részét szállítják alvállalkozók (amennyiben alvállalkozók is érintettek a TOE fejlesztésében).

Az ALC_LCD.1 értékelési altevékenység nem követeli meg az alkalmazott modell egyetlen szabványos életciklus modellnek való megfelelését sem.

ALC_LCD.1.2C Az életciklus modellnek biztosítania kell a TOE fejlesztéséhez és karbantartásához szükséges ellenőrzést.

ALC_LCD.1-2 Az értékelőnek meg kell vizsgálnia az életciklus modellt annak megállapítása érdekében, hogy az életciklus modell által leírt eljárások, eszközök és technikák használata pozitív módon hozzájárul-e a TOE fejlesztéséhez és karbantartásához.

Az életciklus modellben szereplő információ az értékelő számára arról ad bizonyosságot, hogy az alkalmazott fejlesztési és karbantartási eljárások a legkisebb szintre csökkentik a biztonsági hibák valószínűségét. Amennyiben az életciklus modellben szerepel például az ellenőrzési (átvizsgálás) folyamat, de a komponensek módosításának rögzítése nem garantált, akkor az értékelő nem tud megfelelő bizalommal lenni afelől, hogy a TOE-ba nem kerül be újabb hiba. Az értékelő további garanciát kaphat azáltal, hogy összehasonlítja a modell leírását a TOE fejlesztéssel kapcsolatos más értékelői tevékenységek (pl. a „Konfiguráció kezelés képességei” (ALC_CMC) által lefedett értékelői akciók) során összegyűjtött, a fejlesztési folyamatról szóló ismeretekkel. Az életciklus modellben talált hiányosságokkal foglalkozni kell, ha azok kimutathatóan növelhetik a TOE-ba bekerülő véletlen vagy szándékos hibák számát.

A CC nem tesz kötelezővé egyetlen fejlesztési módszert sem, és bármelyiket is alkalmazzák, a célszerűség szerint ajánlott azt értékelni. A "spirális", a "gyors-prototípus" vagy a "vízesés" tervezési modellek egyaránt alkalmazhatók egy minőségi TOE létrehozására, amennyiben ellenőrzött környezetben használják ezeket.

6.2.4.4. A Tesztelés garanciaosztály (ATE) értékelése

Ennek a tevékenységnek a célja annak megállapítása, hogy a TOE olyan módon viselkedik-e, ahogyan azt az ST-ben leírták és (az ADV osztályban leírt) értékelési bizonyítékban specifikálták. Ezt a megállapítást a TSF fejlesztő általi funkcionális tesztelése (ATE_FUN) és a TSF értékelő általi független tesztelése (ATE_IND) bizonyos kombinációján keresztül lehet megtenni. További garancia nyerhető azzal, hogy a fejlesztőt növekvő mértékben bevonják a tesztelésbe és a TOE-ra vonatkozó kiegészítő információk nyújtásába, valamint azzal, hogy az értékelő növeli a független tesztelési tevékenységeket.

6.2.4.4.1. Alkalmazási megjegyzések

A TSF tesztelését részben az értékelő, illetve a legtöbb esetben a fejlesztő hajtja végre. Az értékelő tesztelési törekvései nemcsak eredeti tesztek létrehozásából és végrehajtásából állnak, hanem a fejlesztői tesztek megfelelőségének felméréséből és ezek egy részhalmazának újra lefuttatásából is.

Az értékelő megvizsgálja a fejlesztői teszteket annak meghatározása érdekében, hogy azok milyen mértékben elegendőek annak bizonyításához, hogy a TSFI a specifikáltaknak (lásd ADV_FSP) megfelelően működik, és hogy megértse a fejlesztő tesztelési megközelítés módját. Hasonlóan, az értékelő megvizsgálja a fejlesztői teszteket annak meghatározása érdekében, hogy azok milyen mértékben elegendőek a TSF belső viselkedésének és tulajdonságainak a bemutatásához.

Az értékelő végrehajtja a fejlesztői tesztek egy részhalmazát is, ahogyan azokat dokumentálták, abból a célból, hogy megbizonyosodjon a fejlesztői teszteredményekről: az értékelő ennek a vizsgálatnak az eredményeit bemenetként fogja felhasználni a TSF egy részhalmazának független teszteléséhez. Erre a részhalmazra az értékelő egy olyan tesztelési megközelítési módot alkalmaz, amely eltér a fejlesztőétől, különösen akkor, ha a fejlesztői tesztek hiányosak.

A fejlesztői tesztelési dokumentáció helyességének értékeléséhez, illetve új tesztek készítéséhez az értékelőnek meg kell értenie a TSF elvárt, tervezett működését – mind belülről, mind a TSFI-n keresztül látható módon - azon SFR-ek összefüggésében, melyek kielégítésére létrehozták ezeket. Az értékelő választhatja azt az utat, hogy a TSF-et és a TSFI-t alrendszerekre bontja az ST funkcionális területei alapján (napló alrendszer, naplózással kapcsolatos TSFI, hitelesítő modul, hitelesítéssel kapcsolatos TSFI, stb.) ha az ST ezt nem bontotta már fel így, majd egyszerre csak egy alrendszerre összpontosít. Minden alrendszerre megvizsgálja az ST követelményt és a fejlesztői és az útmutató dokumentáció vonatkozó részeit, hogy megértse azt, milyen működést várnak el a TOE-tól. A fejlesztői dokumentációra épülő bizalom aláhúzza a tesztelés lefedettségének (ATE_COV) és mélységének (ATE_DPT) függőségét a fejlesztés (ADV) garanciaosztálytól.

A CC a családok összetevőinek alkalmazásakor elkülöníti a tesztelés lefedettségét és mélységét a funkcionális teszteléstől, a rugalmasság fokozása érdekében. A családok követelményeit azonban együtt kell alkalmazni annak biztosítása érdekében, hogy a TSF a specifikációjának megfelelően működik. A családok e szoros összefonódása az értékelői munka megduplázódásához vezet a különböző altevékenységek között. Az alábbi alkalmazási megjegyzések az altevékenységek közötti szöveg ismétléseket minimalizálják.

A TOE elvárt működésének megértése

A tesztelési dokumentáció helyességének értékelése, illetve új tesztek készítése előtt az értékelőnek meg kell értenie a biztonsági funkciók elvárt, tervezett működését azon követelmények összefüggésében, melyek kielégítésére létrehozták ezeket.

Mint ahogyan korábban említésre került, az értékelő választhatja a TSF és a TSFI alrendszerekre bontását az ST-ben szereplő SFR-ek (naplózás, hitelesítés, stb.) szerint, majd

egyszerre csak egy alrendszerre összpontosíthat. Az értékelő vizsgáljon meg minden ST követelményt, valamint a funkcionális specifikáció és az útmutató dokumentáció vonatkozó részeit, hogy megértse azt, milyen működést várnak el az érintett TSFI-től. Hasonlóan, az értékelő vizsgálja meg a TOE terv és a biztonsági szerkezet dokumentáció vonatkozó részeit, hogy megértse azt, milyen működést várnak el a TSF érintett alrendszereitől és moduljaitól.

A tervezett működés megértése után az értékelő vizsgálja meg a tesztelési tervet, hogy áttekintést kapjon a tesztelés módszeréről. A legtöbb esetben a tesztelési módszer egy TSFI kiváltása, majd a válaszok megfigyelése. A kívülről látható funkcionalitások közvetlenül tesztelhetők, amikor viszont a funkcionalitás a TOE-n kívülről nem látható (például a maradvány információ védelmi funkcionalitás), akkor más eszközöket kell alkalmazni.

A tesztelés, illetve egyéb módszerek a funkcionalitás elvárt működésének ellenőrzésére

Azon esetekben, melyekben nem célszerű, vagy nem lehetséges a tesztelés (amikor nincs kívülről látható TSFI), a tesztelési tervnek alternatívát kell adnia a tervezett viselkedés, működés ellenőrzésére. Az értékelő felelőssége az alternatív módszer alkalmasságának megítélése. A következőket azonban ajánlott figyelembe venni az egyéb módszerek alkalmasságának megállapításakor:

a) elfogadható alternatív módszer a megvalósítási reprezentáció elemzése annak megállapítása érdekében, hogy a megkívánt működést mutatja-e a TOE. Ez jelenthet kód vizsgálatot egy szoftver TOE, vagy chip-maszk vizsgálatot egy hardver TOE esetén.
b) elfogadható a fejlesztő integrációs vagy modul tesztelése által kapott bizonyíték felhasználása is, még ha az értékelési garanciaszint nincs is arányban a megvalósítás leírásával (ADV_IMP.1 értékelési altevékenység). Amennyiben a fejlesztő integrációs vagy modul tesztelését használják egy biztonsági funkcionalitás elvárt működésének ellenőrzése során, akkor meg kell arról győződni, hogy a tesztelési bizonyíték a TOE aktuális megvalósítását tükrözi-e. Amennyiben az alrendszer vagy a modulok változtak a tesztelés óta, akkor bizonyítékra van szükség arról, hogy a változtatásokat nyomon követték és elemezték, vagy ilyen esetekben általában további teszteket kell elvégezni.

Hangsúlyozni kell, hogy a tesztelési munka kiegészítése alternatív módszerekkel csak akkor járható út, ha mind a fejlesztő, mind az értékelő úgy ítéli meg, hogy nincs más praktikus lehetőség egy biztonsági funkció tervezett működésének tesztelésére.

A tesztek megfelelőségének ellenőrzése

A tesztelés által megkövetelt kezdeti feltételek kialakításához szükség van a tesztelés előfeltételeire. Ezek kifejezhetők beállítandó paraméterekkel, vagy a tesztelés sorrendjének kialakításával, olyan esetekben, amikor az egyik teszt befejezése teremti meg egy másik teszt szükséges előfeltételeit. Az értékelőnek meg kell állapítania, hogy az előfeltételek teljesek és alkalmasak-e, nehogy a megfigyelt teszteredmények az elvárt eredmény irányába befolyásolják a folyamatot.

A tesztelési lépések és várt eredmények meghatározzák a TSFI-re alkalmazandó feladatokat és paramétereket, valamint, hogy a várt eredményeket milyen módon kell ellenőrizni és mik

ezek az eredmények. Az értékelőnek meg kell állapítania, hogy a tesztelési lépések és várt eredmények összhangban vannak-e a funkcionális specifikáció TSFI leírásával. Ez azt jelenti, hogy a TSFI működés funkcionális specifikációban közvetlenül leírt minden jellemzőjéhez tartoznia kell tesztnek és várt eredménynek az adott működés ellenőrzése érdekében.

A tesztelési tevékenység fő célja annak megállapítása, hogy minden alrendszert, modult és TSFI-t kellőképpen leteszteltek a funkcionális specifikációban, TOE tervben és a biztonsági szerkezet leírásban megfogalmazott üzemeltetési elvárások szerint. A fokozott garanciaszinten a tesztelés negatív teszteket is tartalmaz. A tesztelési eljárások betekintést nyújtanak abba, hogy a fejlesztő a tesztelés során hogyan aktivizálta a TSFI-ket, modulokat és alrendszereket. Az értékelő ezt az információt felhasználja, amikor kiegészítő teszteket dolgoz ki a TSF független teszteléséhez.

6.2.4.4.2. Funkcionális tesztek: Az ATE_FUN.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztő vajon helyesen hajtotta végre és dokumentálta a tesztelési dokumentációban leírt teszteket.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) teszt dokumentáció.

Annak mértéke, hogy a tesztelési dokumentáció mennyire fedje le TSF-t, függ a lefedettség garanciális összetevőjétől.

A rendelkezésre bocsátott fejlesztői tesztekre az értékelőnek meg kell állapítania a tesztek megismételhetőségét, valamint azt, hogy a fejlesztői tesztek milyen mértékben használhatók az értékelő független teszteléséhez. Az értékelőnek minden olyan TSFI-t, amelyekre a fejlesztői teszt eredmények azt mutatják, hogy esetleg nem a specifikáltnak megfelelően hajtódnak végre, a megfelelőség vagy meg nem felelősség megállapítása érdekében független tesztelés alá kell vetnie.

6.2.4.4.2.1. Az ATE_FUN.1.1E értékelői akció

ATE_FUN.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ATE_FUN.1.1C A tesztelési dokumentációnak tartalmaznia kell a tesztelési terveket, az elvárt teszteredményeket és a tényleges teszteredményeket.

ATE_FUN.1-1 Az értékelőnek ellenőriznie kell, hogy a tesztelési dokumentáció tartalmazza-e a tesztelési terveket, az elvárt eredményeket és a tényleges teszt eredményeket.

Az értékelő ellenőrizze, hogy a tesztelési terveket, az elvárt eredményeket és a tényleges teszt eredményeket belefoglalták-e a tesztelési dokumentációba.

ATE_FUN.1.2C A tesztelési terveknek azonosítaniuk kell a végrehajtandó teszteket, és le kell írniuk minden teszt végrehajtásának forgatókönyvét. Ezen forgatókönyveknek tartalmazniuk kell a más tesztek eredményeitől való minden sorrendbeli függést.

ATE_FUN.1-2 Az értékelőnek ellenőriznie kell, hogy a tesztelési terv leírja-e minden teszt végrehajtásának forgatókönyvét.

Az értékelőnek meg kell állapítania, hogy a tesztterv nyújt-e információkat a használt tesztkonfigurációra vonatkozóan: mind a TOE konfigurációra, mind pedig minden használt tesztberendezésre vonatkozóan. Ennek az információnak a tesztkonfiguráció reprodukálhatóságának biztosításához kellően részletesnek kell lennie.

Az értékelőnek azt is meg kell állapítania, hogy a tesztterv nyújt-e információt arról, hogy hogyan kell végrehajtani a tesztet: az összes szükséges automatizált indítási eljárásról (és hogy ezek igényelnek-e futási jogosultságot), az alkalmazandó bemenetekről és ezek alkalmazásáról, hogyan lehet megkapni a kimenetet, valamennyi automatikus törlési eljárásról (és hogy ezek igényelnek-e futási jogosultságot), stb. Ennek az információnak a teszt reprodukálhatóságának biztosításához kellően részletesnek kell lennie.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ATE_FUN.1-3 Az értékelőnek meg kell vizsgálnia a tesztelési tervet annak megállapítása érdekében, hogy a TOE teszt konfigurációja megegyezik-e az ST-ben az értékelésre megadott konfigurációval.

A tesztelési tervben ugyanazt az egyedi hivatkozást kell alkalmazni a TOE-ra, mint amit a „Konfiguráció kezelési képességek” (ALC_CMC) altevékenységekben fektettek le, illetve amit az ST bevezetőjében azonosítottak.

Az ST egynél több konfigurációt is meghatározhat az értékeléshez. Az értékelő ellenőrizze, hogy a fejlesztő által a tesztelési dokumentációban azonosított összes teszt konfiguráció megfelel-e az ST-nek. Például az ST olyan kötelezően beállítandó konfigurációs lehetőségeket határozhat meg, amelyek befolyásolják, hogy a TOE milyen részekből álljon, belefoglalva vagy kizárva egyes részeket. Az értékelő ellenőrizze, hogy a TOE összes ilyen változatát figyelembe vették.

Az értékelő vegye figyelembe azokat az ST-ben leírt, a TOE üzemeltetési környezetére vonatkozó biztonsági céljait, amelyek a teszt környezetre alkalmazhatók. Lehet hogy néhány cél nem alkalmazható a teszt környezetre. Például egy a felhasználói engedélyekkel kapcsolatos cél nem alkalmazható, míg a „csatlakozás a hálózathoz egyetlen ponton” alkalmazható.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ATE_FUN.1-4 Az értékelőnek meg kell vizsgálnia a tesztelési tervet annak megállapítása érdekében, hogy az elegendő utasítást tartalmaz-e a sorrendi függőségekre.

Bizonyos lépések végrehajtására szükség lehet a kezdeti feltételek kialakítása érdekében. Például a felhasználói fiókokat fel kell venni, mielőtt azokat törölni lehet. Egy példa a sorrendiségi függőségre: először azokat a tevékenységeket kell végrehajtani, melyek naplóbejegyzéseket állítanak elő, s csak ezt követően lehet a naplóbejegyzéseket kereső és rendező tesztekkel foglakozni. Másik példa a sorrendiségi függőségre: egyik teszteset állítja elő azt az adatállományt, amely egy másik teszt eset számára bemenetként szolgál.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ATE_FUN.1.3C Az elvárt teszteredményeknek be kell mutatniuk a tesztek sikeres végrehajtásából keletkező várható kimeneteket.

ATE_FUN.1-5 Az értékelőnek meg kell vizsgálnia a tesztelési dokumentációt annak megállapítása érdekében, hogy az tartalmazza-e az összes várt teszteredményt.

Az elvárt teszteredmények annak megállapításához szükségek, hogy egy tesztet sikeresen végrehajtottak-e vagy sem. Az elvárt teszteredmények akkor tekinthetők kielégítőnek, ha egyértelműek, és megfelelnek az adott tesztelési módszer alapján várt működésnek.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ATE_FUN.1.4C A tényleges teszteredményeknek összhangban kell állniuk az elvárt teszteredményekkel.

ATE_FUN.1-6 Az értékelőnek ellenőriznie kell, hogy a tesztelési dokumentációban szereplő várt teszteredmények összhangban állnak-e a tényleges teszteredményekkel.

A fejlesztő által átadott tényleges és várt teszteredmények összehasonlítása felfedi a két eredményhalmaz közötti különbségeket. Lehet, hogy a tényleges teszteredmények közvetlen összehasonlítása nem történhet meg bizonyos adatok egyszerűsítése vagy összevonása előtt. Ilyenkor a fejlesztői tesztelési dokumentációban ismertetni kell a tényleges adatokat egyszerűsítő vagy összevonó eljárásokat.

Például a fejlesztőnek tesztelnie kell egy üzenettár tartalmát egy hálózati kapcsolat után, az üzenettár tartalmának megállapítása érdekében. Az üzenettár egy bináris számot tartalmaz, amelyet valamilyen más adatmegjelenítési formába kell átalakítani az értelmezhetőség érdekében. A fejlesztőnek tehát le kell írnia az adat magas szintű ábrázolási formába történő átalakításának módját, hogy az értékelő is végre tudja azt hajtani (szinkron vagy aszinkron átvitel, stop bitek száma, paritás, stb.).

Megjegyzendő, hogy a tényleges adatok egyszerűsítő vagy összevonó folyamatának leírását az értékelő nem a szükséges módosítások tényleges elvégzésére használja, hanem a folyamat megfelelőségének értékelésére. A fejlesztő feladata az elvárt teszteredmények átalakítása olyan formára, amely könnyen összehasonlítható a tényleges teszteredményekkel.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ATE_FUN.1-7 Az értékelőnek jelentést kell készítenie a fejlesztő tesztelési munkájáról, áttekintést adva a tesztelési módszerről, konfigurációról, mélységről és eredményekről.

Az értékelési jelentésben rögzített fejlesztői tesztelésről szóló információ lehetővé teszi az értékelő számára, hogy bemutassa az általános tesztelési módszert és a fejlesztő által a TOE tesztelésébe fektetett munkát. A cél a fejlesztő tesztelési munkájának érdemi áttekintése. Nem cél, hogy az értékelési jelentésben a fejlesztői teszteléssel kapcsolatos információk a specifikus tesztlépések vagy egyedi tesztek eredményeinek pontos megismétlése legyenek. A cél elegendő részletesség biztosítása más értékelők és a tanúsító szervezet számára ahhoz, hogy betekintést kapjanak a fejlesztő tesztelési módszerébe, a végrehajtott tesztek nagyságrendjébe, a TOE teszt konfigurációjába és a fejlesztői tesztelés általános eredményébe.

Az értékelési jelentés fejlesztői tesztekről szóló részében általában az alábbi információk találhatók:

a) TOE teszt konfigurációk. A ténylegesen tesztelt TOE konfigurációk, köztük az, hogy a teszt felállítása vagy a tesztet követő rendteremtés igényelt-e külön jogosultságú kódot.
b) Tesztelési módszer. Az alkalmazott fejlesztői tesztelési stratégia áttekintése.
c) Tesztelési eredmények. A fejlesztői tesztelés eredményének áttekintő leírása.

E lista korántsem teljes, csupán megmutat néhány területet, melyeknek a fejlesztői teszteléssel kapcsolatosan az értékelési jelentésben szerepelni kell.

6.2.4.4.3. Lefedettség: Az ATE_COV.2 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztő letesztelte-e az összes TSFI-t, és hogy a fejlesztő teszt lefedettség elemzése szemlélteti-e a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikációban leírt TSFI-k közötti megfelelést.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) teszt dokumentáció,
d) tesz lefedettség elemzés.

6.2.4.4.3.1. Az ATE_COV.2.1E értékelői akció

ATE_COV.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ATE_COV.2.1C A teszt lefedettség elemzésének szemléltetnie kell a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikációban leírt TSFI-k közötti megfelelést.

ATE_COV.2-1 Az értékelőnek meg kell vizsgálnia a teszt lefedettség elemzését annak megállapítása érdekében, hogy a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikációban leírt interfészek közötti megfeleltetés pontos-e.

A megfeleltetés bemutatására egy egyszerű kereszt-táblázat is elegendő lehet. A teszt lefedettség elemzésben szereplő teszteket és interfészeket egyértelműen kell azonosítani.

Emlékeztetjük az értékelőt arra, hogy nem kell a tesztelési dokumentáció valamennyi tesztjét leképezni a funkcionális specifikációban leírt interfészekre.

ATE_COV.2-2 Az értékelőnek meg kell vizsgálnia a tesztelési tervet annak megállapítása érdekében, hogy a tesztelési módszer minden interfész esetén szemlélteti-e az adott interfész elvárt működését.

Ehhez a munkaegységhez útmutató található az alábbi alkalmazási megjegyzésekben:

a) 6.2.5.4.1.1, A TOE elvárt működésének megértése
b) 6.2.5.4.1.2, A tesztelés, illetve egyéb módszerek a funkcionalitás elvárt működésének ellenőrzésére

ATE_COV.2-3 Az értékelőnek meg kell vizsgálnia a teszt eljárásokat annak megállapítása érdekében, hogy a teszt előfeltételek, a tesztelési lépések és az elvárt eredmény(ek) megfelelően tesztelnek-e minden interfészt.

Ehhez a funkcionális specifikációra vonatkozó munkaegységhez útmutató található az alábbi alkalmazási megjegyzésben:

a) 6.2.5.4.1.3, A tesztek megfelelőségének ellenőrzése.

ATE_COV.2.2C A teszt lefedettség elemzésének szemléltetnie kell, hogy a funkcionális specifikációban leírt összes TSFI-t letesztelték.

ATE_COV.2-4 Az értékelőnek meg kell vizsgálnia a teszt lefedettség elemzését annak megállapítása érdekében, hogy a funkcionális specifikációban leírt interfészek és a tesztelési dokumentációban azonosított tesztek közötti megfeleltetés teljes-e.

A funkcionális specifikációban szereplő valamennyi TSFI-nek meg kell jelennie a teszt lefedettség elemzésében, és ezeket le kell képezni a tesztekre a teljesség kimutatása érdekében, az interfészek teljes körű specifikáció tesztelése ugyanakkor nem követelmény. Nyilvánvalóan hiányos a lefedettség, ha a funkcionális specifikációban azonosított egyik interfészhez nem rendeltek tesztet.

Emlékeztetjük az értékelőt arra, hogy nem kell a tesztelési dokumentáció valamennyi tesztjét leképezni a funkcionális specifikációban leírt interfészekre.

6.2.4.4.4. Mélység: Az ATE_DPT.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztő letesztelte-e a TSF alrendszereket a TOE tervnek és a biztonsági szerkezet leírásnak megfelelően.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) TOE terv,
d) biztonsági szerkezet leírása,
e) teszt dokumentáció,
f) tesz mélység elemzés.

6.2.4.4.4.1. Az ATE_DPT.1.1E értékelői akció

ATE_DPT.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ATE_DPT.1.1C A teszt mélység elemzésnek szemléltetnie kell a tesztelési dokumentációban azonosított tesztek és a TOE tervben szereplő TSF alrendszerek közötti megfelelést.

ATE_DPT.1-1 Az értékelőnek meg kell vizsgálnia a teszt mélység elemzését annak megállapítása érdekében, hogy a tesztelési dokumentáció tartalmazza-e a TSF alrendszerek működésének és egymás közötti kapcsolódásaik leírását.

Ez a munkaegység ellenőrzi a tesztek és a TOE terv megfelelését. Amennyiben a TSF architektúrális helyességének leírása (az ADV_ARC biztonsági szerkezet leírás keretén belül) speciális mechanizmusokra hivatkozik, ez a munkaegység ellenőrzi a tesztek és az ilyen mechanizmusok üzemeltetési leírása közötti megfelelést is.

A megfeleltetés bemutatására egy egyszerű kereszt-táblázat is elegendő lehet. A teszt mélység elemzésben szereplő teszteket és a működéseket, kapcsolódásokat egyértelműen kell azonosítani.

Emlékeztetjük az értékelőt arra, hogy nem kell a tesztelési dokumentáció valamennyi tesztjét leképezni a funkcionális specifikációban leírt interfészekre.

ATE_DPT.1-2 Az értékelőnek meg kell vizsgálnia a tesztelési tervet, a teszt előfeltételeket, a tesztelési lépéseket és az elvárt eredmény(eke)t annak megállapítása érdekében, hogy a működés leírás tesztelési módszere szemlélteti-e, hogy az alrendszerek működése megfelel-e a TOE tervben leírtaknak.

Ehhez a munkaegységhez útmutató található az alábbi alkalmazási megjegyzésekben:

a) 6.2.5.4.1.1, A TOE elvárt működésének megértése
b) 6.2.5.4.1.2, A tesztelés, illetve egyéb módszerek a funkcionalitás elvárt működésének ellenőrzésére

Amennyiben leírták a TSF alrendszerek interfészeit, az alrendszerek működésének tesztelése végrehajtható közvetlenül ezeken az interfészeken. Egyébként az alrendszerek működése a TSFI interfészeken tesztelendő. Az előzőek kombinációja is alkalmazható. Bármelyik módszert is választotta, az értékelőnek meg kell fontolnia, hogy az adott módszer alkalmas-e az alrendszerek TOE tervben leírt működésnek a tesztelésére.

ATE_DPT.1-3 Az értékelőnek meg kell vizsgálnia a tesztelési tervet, a teszt előfeltételeket, a tesztelési lépéseket és az elvárt eredmény(eke)t annak megállapítása érdekében, hogy a működés leírás tesztelési módszere szemlélteti-e, hogy az alrendszerek egymásra hatása megfelel-e a TOE tervben leírtaknak.

Amíg az előző munkaegység az alrendszerek működésével foglalkozott, ez a munkaegység az alrendszerek egymásra hatásával (az egymás közötti működéssel) foglalkozik.

Ehhez a munkaegységhez útmutató található az alábbi alkalmazási megjegyzésekben:

a) 6.2.5.4.1.1, A TOE elvárt működésének megértése
b) 6.2.5.4.1.2, A tesztelés, illetve egyéb módszerek a funkcionalitás elvárt működésének ellenőrzésére

Amennyiben leírták a TSF alrendszerek interfészeit, az alrendszerek közötti egymásra hatás tesztelése végrehajtható közvetlenül ezeken az interfészeken. Egyébként az alrendszerek közötti egymásra hatásra a TSFI interfészeken keresztül lehet következtetni. Bármelyik módszert is választotta, az értékelőnek meg kell fontolnia, hogy az adott módszer alkalmas-e az alrendszerek közötti, a TOE tervben leírt egymásra hatás tesztelésére.

ATE_DPT.1.2C A teszt mélység elemzésnek szemléltetnie kell, hogy a TOE tervben szereplő összes TSF alrendszert letesztelték.

ATE_DPT.1-4 Az értékelőnek meg kell vizsgálnia a teszt eljárásokat annak megállapítása érdekében, hogy a TSF alrendszerek működésének és egymásra hatásának minden leírását tesztelték-e.

Ez a munkaegység az ATE_DPT.1-1 munkaegység teljességét ellenőrzi. A TOE tervben szereplő valamennyi alrendszer működésére, illetve valamennyi alrendszerek egymásra hatására vonatkozó leírást tesztelni kell. Nyilvánvalóan hiányos a tesztelés mélysége, ha a TSF tervben azonosított egyik TSF alrendszer működésre, vagy alrendszerek egymásra hatására vonatkozó leíráshoz nem rendeltek tesztet.

Emlékeztetjük az értékelőt arra, hogy nem kell a tesztelési dokumentáció valamennyi tesztjét leképezni a TOE tervben leírt alrendszer interfészekre.

6.2.4.4.5. Független tesztelés: Az ATE_IND.2 altevékenység értékelése

Ennek az altevékenységnek a célja a TSFI egy részhalmazának független tesztelésével annak megállapítása, hogy a TOE a terv dokumentációban előírt módon működik-e, valamint a fejlesztői tesztek megbízhatóságának ellenőrzése egy azokból vett minta végrehajtásával.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) TOE terv,
d) üzemeltetési felhasználói útmutató,
e) előkészítő felhasználói útmutató,

f) konfiguráció kezelés dokumentáció,
g) tesztelési dokumentáció,
h) a tesztelésre alkalmas TOE.

6.2.4.4.5.1. Az ATE_IND.2.1E értékelői akció

ATE_IND.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ATE_IND.2.1C A TOE-nek tesztelésre alkalmas állapotban kell lennie.

ATE_IND.2-1 Az értékelőnek meg kell vizsgálnia a TOE-t annak megállapítása érdekében, hogy a teszt konfiguráció megegyezik-e az ST-ben meghatározott, értékelés alatt álló konfigurációval.

A fejlesztő által biztosított és a teszt tervben azonosított TOE-nek ugyanazt az egyedi hivatkozást kell alkalmaznia, mint amit a „Konfiguráció kezelés képességei” (ALC_CMC) altevékenységekben fektettek le, illetve amit az ST bevezetőjében azonosítottak.

Az ST meghatározhat egynél több konfigurációt is az értékeléshez. A TOE több különálló hardver és szoftver elemből állhat, melyeket az ST-nek megfelelően kell tesztelni. Az értékelő ellenőrizze, hogy valamennyi teszt konfiguráció ellentmondás mentes-e az ST-vel.

Az értékelő vegye figyelembe azokat az ST-ben leírt, a TOE üzemeltetési környezetére vonatkozó biztonsági célokat, amelyek a teszt környezetre alkalmazhatók. Lehet hogy néhány cél nem alkalmazható a teszt környezetre. Például egy a felhasználói engedélyekkel kapcsolatos cél nem alkalmazható, míg a „csatlakozás a hálózathoz egyetlen ponton” alkalmazható.

Bármilyen tesztelési erőforrás (mérőműszer, elemző készülék) használatakor az értékelő felelőssége annak biztosítása, hogy ezek az erőforrások megfelelően hitelesítve legyenek.
ATE_IND.2-2 Az értékelőnek meg kell vizsgálnia a TOE-t annak megállapítása érdekében, hogy azt megfelelően telepítették-e, és ismert állapotban van-e.

Az értékelő a TOE állapotát többféle módon is megállapíthatja. Például az AGD_PRE.1 altevékenység értékelésének előzetes sikeres befejezése teljesíti ezt a munkaegységet, ha az értékelő még bizonyos abban, hogy a tesztelésre használt TOE-t megfelelően telepítették és ismert állapotban van. Amennyiben nem ez a helyzet, akkor az értékelőnek a fejlesztő eljárásait kell követnie a TOE telepítéséhez és indításához, kizárólag a rendelkezésére bocsátott útmutatókra támaszkodva.

Amennyiben az értékelőnek végre kell hajtania a telepítési lépéseket, mert a TOE ismeretlen állapotban van, akkor e munkaegység sikeres befejezése kielégítheti az AGD_PRE.1-5 munkaegységet is.

ATE_IND.2.2C A fejlesztőnek biztosítania kell a TSF fejlesztői funkcionális tesztelése során használt erőforrás-készlettel azonos eszközkészletet.

ATE_IND.2-3 Az értékelőnek meg kell vizsgálnia a fejlesztő által rendelkezésére bocsátott erőforrás-készletet annak megállapítása érdekében, hogy az azonos-e a TSF fejlesztői funkcionális tesztelése során alkalmazott erőforrásokkal.

A fejlesztő által használt erőforrás-készletet a fejlesztői tesztelési terv dokumentálja, az ATE_FUN funkcionális tesztelés családban meggondolt módon. Az erőforrás-készlet többek között felölelhet laboratóriumi hozzáférést és speciális teszt berendezéseket is. Azokat az erőforrásokat, melyek nem egyeznek meg a fejlesztő által használtakkal, azonossá kell tenni a teszteredményekre gyakorolt lehetséges hatásuk szerint.

6.2.4.4.5.2. Az ATE_IND.2.2E értékelői akció

ATE_IND.2.2E Az értékelőnek végre kell hajtania a tesztelési dokumentációban szereplő tesztek valamely részhalmazát (mintáját) a fejlesztői teszt eredmények ellenőrzése érdekében.

ATE_IND.2-4 Az értékelőnek el kell végeznie a tesztelést a fejlesztői tesztelési tervben és eljárásokban található tesztekből vett mintára.

E munkaegység célja, hogy az értékelő elegendő számú fejlesztői teszt végrehajtásával meggyőződjön a fejlesztői teszteredmények érvényességéről. A minta nagyságáról, és a mintát alkotó fejlesztői tesztekről az értékelő dönt (lásd 7.2.1).

Minden fejlesztői teszt visszavezethető speciális interfészekre. Ezért a mintát alkotó tesztek kiválasztásakor figyelembe vett tényezők hasonlóak az ATE_IND.2-6 munkaegységnél leírtakhoz. Ezen kívül az értékelő alkalmazhat véletlenszerű mintavételezési módszert is a fejlesztői tesztek kiválasztásához, mintába vételéhez.

ATE_IND.2-5 Az értékelőnek ellenőriznie kell, hogy a tényleges teszteredmények összhangban állnak-e az elvárt teszteredményekkel.

A tényleges és az elvárt teszteredmények közti különbségek az ellentmondás feloldására késztetik az értékelőt. Az értékelő által feltárt ellentmondást a fejlesztő is feloldhatja kielégítő magyarázattal vagy az eltérések feloldásával.

Amennyiben nincs kielégítő magyarázat vagy feloldás, akkor az értékelő kevésbé megbízhatónak ítélheti a fejlesztői tesztelést, és növelheti a tesztelési minta nagyságát. Annak megerősítése érdekében, hogy az ATE_IND.2-4 munkaegységben azonosított mintát megfelelően tesztelték, a fejlesztői tesztelésben talált hiányosságokat meg kell szüntetni, akár a fejlesztői tesztelés kijavításával, akár az értékelő által végzett új tesztekkel.

6.2.4.4.5.3. Az ATE_IND.2.3E értékelői akció

ATE_IND.2.3E Az értékelőnek tesztelnie kell a TSF interfészeinek egy részét annak megerősítése érdekében, hogy a TSF a specifikáltaknak megfelelően működik.

ATE_IND.2-6 Az értékelőnek meg kell terveznie egy tesztkészletet.

Az értékelő válassza ki a TOE-nek megfelelő tesztkészletet és tesztelési stratégiát. Egy lehetséges szélsőséges tesztelési stratégia szerint a tesztkészlet annyi interfészt tartalmaz, amennyi csak tesztelhető kevés szigorral. Egy másik lehetséges tesztelési stratégia, hogy a teszt néhány interfészre terjed ki azok fontossága szerint és ezeket igen alapos ellenőrzésnek vetik alá.

Az értékelő által követett tesztelési módszer általában e két szélsőséges eset közé esik. Az értékelőnek ajánlott az interfészek nagy részére legalább egy tesztet végrehajtania, de a tesztelésnek nem kell teljes körű specifikáció-tesztelésnek lennie.

Az értékelőnek a tesztelendő interfész részhalmaz kiválasztásakor az alábbi tényezőket kell figyelembe vennie:

a) A fejlesztői tesztelés bizonyítékai. Ez a következőkből áll: tesztelési dokumentáció, teszt lefedettség elemzés, teszt mélység elemzés. A fejlesztői teszt bizonyíték betekintést nyújt abba, hogy a fejlesztő a tesztelés során hogyan aktivizálta a biztonsági funkciókat. Az értékelő ezt az információt felhasználja a TOE független teszteléséhez szükséges új tesztek tervezésékor. Fokozottan át kell gondolnia a következőket:
   aa) Az interfészekre vonatkozó fejlesztői tesztelés bővítése. Az értékelő végrehajthat ugyanolyan típusú teszteket változó paraméterekkel az interfész szigorúbb tesztelése céljából.
   ab) Az interfészekre vonatkozó fejlesztői tesztelési stratégia kiegészítése. Az értékelő módosíthatja egy adott interfészeknél alkalmazott tesztelési módszert egy új tesztelési stratégiát alkalmazva.
b) Azon interfészek száma, melyekből a tesztkészlet készül. Amennyiben a TOE csak kis számú, viszonylag egyszerű interfészt tartalmaz, célszerű lehet az összes szigorú tesztelése. Más esetekben ez nem költség-hatékony módszer, ekkor mintavételezésre van szükség.
c) Az értékelési tevékenységek egyensúlyának fenntartása. A tesztelésbe fektetett értékelői munka álljon arányban a többi értékelési feladatba fektetett munkával.

Az értékelő válassza ki az interfészek részhalmazát. Ez a kiválasztás több tényezőtől függ, és e tényezők is hatást gyakorolnak a tesztkészlet méretére:

a) Az interfészek fejlesztői tesztelésének szigora. Azokat az interfészeket, melyekre az értékelő további tesztelés szükségességét állapítja meg, ajánlott a tesztkészletbe bevenni.
b) A fejlesztői teszteredmények. Amennyiben a fejlesztői teszteredmény kétséget támaszt az értékelőben egy interfész megfelelő megvalósításával kapcsolatban, az adott interfészt ajánlott a tesztkészletbe bevenni.
c) Az interfészek fontossága. Azokat az interfészeket, amelyek a többieknél fontosabbak, ajánlott a tesztkészletbe bevenni. A „fontosság” egyik jelentős tényezője a biztonsági jelentőség (az SFR-t érvényre juttató interfészek fontosabbak az SFR-t támogató interfészeknél, ezek pedig fontosabbak az SFR-be nem beavatkozó interfészeknél, lásd 6.2.4.1.2 ADV_FSP.3 alfejezet). A „fontosság” másik jelentős tényezője az adott interfészre képezhető SFR-ek száma (ahogyan azt az ADV-beli absztrakciós szintek közötti megfelelés azonosításakor meghatározzák).

d) Az interfészek bonyolultsága. A bonyolult megvalósítást igénylő interfészek bonyolult teszteket követelhetnek meg a fejlesztőktől és az értékelőktől, melyek súlyos, a költség-hatékonysággal ellentétes követelmények. Ugyanakkor a bonyolult interfészeknél nagyobb a hibákra bukkanás valószínűsége, így jó jelöltek lehetnek a tesztkészletbe. Az értékelőnek a fenti két ellentétes szempontot kell mérlegelnie.
e) Közvetett tesztelés. Egyes interfészek tesztelése gyakran más interfészek közvetett tesztelésével is jár, így ezek tesztkészletbe vétele maximalizálja a tesztelt interfészek számát (még ha csak közvetett módon is). Egyes interfészeket általában széleskörű biztonsági funkcionalitásra használnak, így egy hatékony tesztelési megközelítés ezeket megcélozza.
f) Az interfészek típusai (pl. programozott, parancs-soros, protokoll). Az értékelőnek a TOE által támogatott minden TOE által támogatott interfész típusból ajánlott bevennie teszteket.
g) Új vagy szokatlan megoldásokat használó interfészek. Amennyiben a TOE újszerű vagy szokatlan tulajdonságokat tartalmaz, melyek erős üzleti hangsúlyt kaphatnak, az ezeknek megfelelő interfészek is erős jelöltek a tesztelésre.

A fenti útmutató kiemeli a megfelelő tesztkészlet kiválasztási folyamata során figyelembe veendő tényezőket, de semmiképpen nem tekinthető teljesnek.

ATE_IND.2-7 Az értékelőnek el kell készítenie a tesztkészlethez a tesztelési dokumentációt, amely kellőképpen részletes a tesztek megismételhetősége érdekében.

A TSF elvárt működésének az ST-ből, a funkcionális specifikációból és a TOE tervből való megértése után az értékelőnek meg kell határoznia az interfész tesztelésére leginkább alkalmas módot. Az értékelő különösen az alábbiakat vegye figyelembe:

a) a használni kívánt módszer, például egy külső vagy egy belső interfészt tesztelnek, esetleg egy alternatív teszt módszert (pl. különleges esetben kód vizsgálatot) alkalmaznak,
b) az interfész(ek), melye(ke)t a tesztelésnél és a válaszok megfigyelésénél használnak,
c) a teszteléshez szükséges kezdeti feltételek (például bármely szükséges különleges objektum vagy szubjektum, a szükséges biztonsági tulajdonságokkal),
d) a teszteléshez szükséges speciális berendezések, mely vagy egy interfész aktivizálásához (pl. csomag generátorok), vagy egy interfész megfigyeléséhez (pl. hálózati analizátorok) szükségesek.

Az értékelő tesztelhet úgy is minden interfészt, hogy teszt-esetek sorozatát használja, ahol az egyes teszt-eset az adott interfészt elvárt működésének egy különleges szempontját vizsgálja.

Az értékelő tesztelési dokumentációjában ajánlott meghatározni a teszt származtatásokat, visszavezetve azokat az érintett interfész(ek)re.

ATE_IND.2-8 Az értékelőnek végre kell hajtani a tesztelést.

Az értékelő az elkészített tesztelési dokumentációt alapként használja a TOE tesztelésének végrehajtásához. Bár a végrehajtandó tesztelés alapja a tesztelési dokumentáció, az értékelő ad hoc is végezhet teszteket. A tesztelés során feltárt TOE viselkedés alapján az értékelő új teszteket is készíthet. Az új teszteket is le kell írni a dokumentációban.

ATE_IND.2-9 Az értékelőnek jelentésbe kell foglalnia a tesztkészletben szereplő tesztekről az alábbi információkat:

a) a tesztelendő interfész azonosítása;
b) a tesztekhez szükséges berendezések összekapcsolásához és beállításához tartozó utasítások;
c) a teszt előfeltételek kialakítására vonatkozó utasítások;
d) az interfész kiváltására (aktivizálására) vonatkozó utasítások;
e) az interfész működésének megfigyelésére vonatkozó utasítások;
f) az összes elvárt eredmény leírása, valamint a megfigyelt viselkedés és az elvárt eredmények összehasonlításához szükséges elemzések;
g) a tesztek lezárására és a TOE tesztelés utáni állapotának kialakítására vonatkozó utasítások;
h) tényleges teszteredmények.

A leírásnak olyan részletességűnek kell lennie, hogy egy másik értékelő képes legyen megismételni a teszteket és azonos eredményt kapjon. Míg a teszteredmények bizonyos részei eltérhetnek egymástól (pl. naplórekordok dátum és időbejegyzései), az általános eredménynek meg kell egyezni.

Lehetnek olyan esetek, amikor szükségtelen e munkaegységben minden információt megadni (például egy teszt tényleges eredménye nem követeli meg az elemzést, mielőtt az elvárt eredmények összehasonlítása nem történik meg). Ennek eldöntése és a döntés indoklása az értékelő hatásköre.

ATE_IND.2-10 Az értékelőnek ellenőriznie kell, hogy a tényleges teszteredmények megegyeznek-e az elvárt eredményekkel.

Bármilyen különbözőség az elvárt és tényleges eredmények között a TOE helytelen működését vagy a dokumentáció hibáját jelezheti. A nem várt tényleges eredmény a TOE vagy a tesztelési dokumentáció javítását, esetleg a tesztek összeállításának módosítását, bizonyos tesztek megismétlését igényelheti. Ennek eldöntése és a döntés indoklása az értékelő hatásköre.

ATE_IND.2-11 Az értékelőnek az értékelési jelentésben le kell írnia az értékelői tesztelési munkát, áttekintést adva a tesztelési módszerről, konfigurációról, mélységről és eredményekről.

Az értékelési jelentésben rögzített értékelői tesztelésről szóló információ lehetővé teszi az értékelő számára, hogy bemutassa az általános tesztelési módszert és a tesztelésbe fektetett munkát. A cél a tesztelési munka érdemi áttekintése. Nem cél, hogy az értékelési jelentésben a teszteléssel kapcsolatos információk a specifikus tesztlépések vagy egyedi tesztek eredményeinek pontos megismétlése legyenek. A cél elegendő részletesség biztosítása más értékelők és a tanúsító szervezet számára ahhoz, hogy betekintést kapjanak a választott tesztelési módszerbe, az értékelő által végrehajtott tesztek nagyságrendjébe, a fejlesztő által végrehajtott tesztek nagyságrendjébe, a TOE teszt konfigurációjába és a tesztelés általános eredményébe.

Az értékelési jelentés értékelői tesztekről szóló részében általában az alábbi információk találhatók meg:

a) TOE teszt konfigurációk. A ténylegesen tesztelt TOE konfigurációk.
b) A kiválasztott tesztelési készlet (részhalmaz) nagysága. Az értékelés során tesztelt interfészek mennyisége és ennek indoklása.
c) A részhalmazt alkotó interfészek kiválasztásának szempontjai. Rövid állítások azokról a tényezőkről, melyeket figyelembe vettek az interfészek készletbe választása során.
d) A tesztelt interfészek. Rövid felsorolása a készletbe került interfészeknek.
e) A végrehajtott fejlesztői tesztek. Ezek mennyisége és a kiválasztásukhoz használt szempontok rövid leírása.
f) A tevékenység alapján hozott határozat. Az értékelés során végzett tesztelés eredményének általános elbírálása.

E lista korántsem teljes, csupán megmutat néhány területet, melyeket az értékelői teszteléssel kapcsolatosan az értékelési jelentésben ajánlott szerepeltetni.

6.2.4.5. A Sebezhetőség felmérés garanciaosztály (AVA) értékelése

A sebezhetőség felmérés tevékenység célja a TOE üzemeltetési környezetében lévő hibák vagy gyengeségek kihasználhatóságának megállapítása. Ez a megállapítás az értékelési bizonyíték vizsgálatán, valamint az értékelő által a nyilvánosan elérhető anyagokban való keresésen alapul, és az értékelő áthatolás tesztelése támogatja ezt.

A 7.3 melléklet részletes útmutatót biztosít a sebezhetőség vizsgálat általános fogalmairól és megközelítés módjáról.

6.2.4.5.1. Sebezhetőségi elemzés: Az AVA_VAN.2 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a TOE üzemeltetési környezetében vannak-e alap támadó képességgel rendelkező támadók által kihasználható sebezhetőségek.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) TOE tervek,
d) biztonsági szerkezet leírása,
e) útmutató dokumentáció,
f) tesztelésre alkalmas TOE,
g) nyilvánosan elérhető információk a lehetséges sebezhetőségek azonosításának támogatására.

Egyéb bemenet ehhez az altevékenységhez:

a) a lehetséges sebezhetőségekre és támadásokra vonatkozó aktuális, nyilvánosan elérhető információk (pl. egy tanúsító szervezettől).

Az értékelő vegye figyelembe azokat a kiegészítő teszteket is, melyek az értékelés egyéb részeinél felmerült lehetséges sebezhetőségek eredményeként születtek.

6.2.4.5.1.1. Az AVA_VAN.2.1E értékelői akció

AVA_VAN.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

AVA_VAN.2.1C A TOE-nak alkalmasnak kell lennie tesztelésre.

AVA_VAN.2-1 Az értékelőnek meg kell vizsgálnia a TOE-t annak megállapítása érdekében, hogy a teszt konfiguráció megegyezik-e az ST-ben meghatározott, értékelés alatt álló konfigurációval.

A fejlesztő által biztosított és a teszt tervben azonosított TOE-nek ugyanazt az egyedi hivatkozást kell alkalmaznia, mint amit a „Konfiguráció kezelés képességei” (ALC_CMC) altevékenységekben fektettek le, illetve amit az ST bevezetőjében azonosítottak.

Az ST meghatározhat egynél több konfigurációt is az értékeléshez. A TOE több különálló hardver és szoftver elemből állhat, melyeket az ST-nek megfelelően kell tesztelni. Az értékelő ellenőrizze, hogy valamennyi teszt konfiguráció ellentmondás mentes-e az ST-vel.

Az értékelő vegye figyelembe azokat az ST-ben leírt, a TOE üzemeltetési környezetére vonatkozó biztonsági célokat, amelyek a teszt környezetre alkalmazhatók. Lehet hogy néhány cél nem alkalmazható a teszt környezetre. Például egy a felhasználói engedélyekkel kapcsolatos cél nem alkalmazható, míg a „csatlakozás a hálózathoz egyetlen ponton” alkalmazható.

Bármilyen tesztelési erőforrás (mérőműszer, elemző készülék) használatakor az értékelő felelőssége annak biztosítása, hogy ezek az erőforrások megfelelően hitelesítve legyenek.
AVA_VAN.2-2 Az értékelőnek meg kell vizsgálnia a TOE-t annak megállapítása érdekében, hogy azt megfelelően telepítették-e, és ismert állapotban van-e.

Az értékelő a TOE állapotát többféle módon is megállapíthatja. Például az AGD_PRE.1 altevékenység értékelésének előzetes sikeres befejezése teljesíti ezt a munkaegységet, ha az értékelő még bizonyos abban, hogy a tesztelésre használt TOE-t megfelelően telepítették és ismert állapotban van. Amennyiben nem ez a helyzet, akkor az értékelőnek a fejlesztő eljárásait kell követnie a TOE telepítéséhez és indításához, kizárólag a rendelkezésére bocsátott útmutatókra támaszkodva.

Amennyiben az értékelőnek végre kell hajtania a telepítési lépéseket, mert a TOE ismeretlen állapotban van, akkor e munkaegység sikeres befejezése kielégítheti az AGD_PRE.1-5 munkaegységet is.

6.2.4.5.1.2. Az AVA_VAN.2.2E értékelői akció

AVA_VAN.2.2E Az értékelőnek egy keresést kell végrehajtania nyilvános forrásokban a TOE lehetséges sebezhetőségeinek azonosítása érdekében.

AVA_VAN.2-3 Az értékelőnek tanulmányoznia kell a nyilvánosan rendelkezésre álló információ forrásokat a TOE lehetséges sebezhetőségeinek a meghatározása céljából.

Az értékelő tanulmányozza a nyilvánosan rendelkezésre álló információ forrásokat, amelyek rendelkezésre állnak a TOE lehetséges sebezhetőségei meghatározásainak elősegítéséhez. Sokféle nyilvánosan rendelkezésre álló információ forrás létezik, amelyeket az értékelőnek ajánlatos figyelembe vennie, felhasználva a világhálón elérhető anyagokat, beleértve a következőket:

a) szakértői publikációk (folyóiratok, könyvek);
b) tanulmányok.

Az értékelő ne korlátozza az általa figyelembevett nyilvánosan rendelkezésre álló információkat a fentiekre, hanem vegyen figyelembe bármely egyéb vonatkozó rendelkezésre álló információt.

Az értékelő az átadott bizonyítékok vizsgálata közben használja fel a nyilvános információkat abból a célból, hogy további vizsgálatokat végezzen lehetséges sebezhetőségek felkutatására. Ha az értékelő problémás területeket határozott meg, vegye figyelembe azokat a nyilvánosan rendelkezésre álló információkat, amelyek az adott problémás területre vonatkoznak.

Az olyan információk elérhetősége, amely azonnal rendelkezésre állhat egy támadó számára, s amely elősegíti támadások meghatározását és megkönnyíti a támadások hatékony végrehajtását, jelentősen megnövelheti egy adott támadó támadási lehetőségeit. A sebezhetőségi információk és kifinomult támadó eszközök hozzáférhetősége az Interneten nagyon valószínűvé teszi, hogy ezeket megpróbálják felhasználni a TOE lehetséges sebezhetőségeinek meghatározására és kihasználására. A modern kereső eszközök az ilyen információkat könnyen elérhetővé teszik az értékelő számára, és a publikált lehetséges sebezhetőségekkel, valamint a jól ismert általános támadásokkal szembeni ellenállóképesség költséghatékony módon meghatározható.

A nyilvánosan rendelkezésre álló információ keresése célirányosan azokra a forrásokra irányuljon, amelyek a TOE alapját képező termékre vonatkoznak. Az ilyen keresés terjedelme vegye figyelembe a következő tényezőket: a TOE típusa, az értékelő tapasztalatai ezzel a TOE típussal, a feltételezett támadó képesség és a rendelkezésre álló ADV bizonyíték szintje.

A meghatározási folyamat iteratív, ahol egy lehetséges sebezhetőség meghatározása egy másik problémás terület meghatározásához vezethet, amely további vizsgálatokat igényel.

Az értékelőnek jelentést kell készítenie arról, hogy mit tett a bizonyítékokban található lehetséges sebezhetőségek meghatározására. Az ilyen típusú keresésre azonban lehet, hogy az értékelő nem tudja a vizsgálat megkezdése előtt leírni a lehetséges sebezhetőségek meghatározására teendő lépéseket, mivel lehetséges, hogy a módszert a keresés során találtak alakítják.

Az értékelőnek jelentést kell készíteni a megvizsgált bizonyítékokról a lehetséges sebezhetőségekre irányuló keresés befejezésekor. A bizonyítékok kiválasztása származhat az értékelő által meghatározott olyan problémás területekből, amely a támadó által is feltehetően elérhető bizonyítékhoz kapcsolódik, vagy megfelelhet az értékelő által adott valamilyen más magyarázatnak.

6.2.4.5.1.3. Az AVA_VAN.2.3E értékelői akció

AVA_VAN.2.3E Az értékelőnek egy független sebezhetőség vizsgálatot kell végrehajtania a TOE-ra, az útmutató dokumentációt, funkcionális specifikációt, TOE tervet, és a biztonsági szerkezet leírást használva, a TOE lehetséges sebezhetőségeinek azonosítása érdekében.

AVA_VAN.2-4 Az értékelőnek egy keresést kell folytatnia az ST-re, az útmutató dokumentációra, a funkcionális specifikációra, a TOE tervre és a biztonsági szerkezet leírásra vonatkozóan abból a célból, hogy meghatározza a TOE-ban esetlegesen előforduló lehetséges sebezhetőségeket.

A bizonyítékokban való keresést a TOE-ra vonatkozó tervek és dokumentációk vizsgálata során kell teljesíteni, majd pedig feltételezéseket vagy találgatásokat kell tenni a TOE lehetséges sebezhetőségeit illetően. Ezután a feltételezett lehetséges sebezhetőségeket fontossági sorrendbe kell állítani az alábbiak alapján: a sebezhetőség fennállásának becsült valószínűsége, a kiaknázásához szükséges támadó képesség (feltételezve, hogy fennáll a sebezhetőség), az általa elérhető felügyelet vagy veszélyeztetés mértéke.

A biztonsági szerkezet leírás szolgáltatja a fejlesztő sebezhetőség vizsgálatát, minthogy ez dokumentálja, hogy a TSF hogyan védi saját magát a nem-megbízható szubjektumokkal szemben, és hogyan akadályozza meg a biztonságot érvényre juttató funkcionalitás megkerülését. Ennélfogva az értékelő a TSF lehetséges aláaknázási módszerei keresésének alapjaként használja ezt a leírást a TSF védelméről.

Azoktól az SFR-ektől függően, amelyeket a TOE-nak teljesítenie kell az üzemeltetési környezetben, az értékelő független sebezhetőség vizsgálata vegye tekintetbe az általános lehetséges sebezhetőségeket az alábbi fejezetcímek mindegyike alatt:

a) az értékelés alatt álló TOE típusára vonatkozó általános lehetséges sebezhetőségek, amint ilyeneket a tanúsító szervezet szolgáltathat;
b) megkerülés;
c) hamisítás;
d) közvetlen támadások;
e) megfigyelés;
f) helytelen használat/visszaélés.

A b) - f) tételeket részletesen magyarázza a 7.3 melléklet.

A biztonsági szerkezet leírást a fenti általános lehetséges sebezhetőségek szem előtt tartása mellett kell mérlegelni. Minden lehetséges sebezhetőséget mérlegelni kell azon lehetséges módok felkutatására, amelyekkel a TSF védelmet hatálytalanítani, a TSF-et aláaknázni lehet.

AVA_VAN.2-5 Az értékelőnek az ETR-ben rögzítenie kell a meghatározott lehetséges sebezhetőségeket, amelyek tesztelhetők, és a TOE üzemeltetési környezetében szóba jöhetnek.

Nem szükséges a lehetséges sebezhetőségek további mérlegelése, ha az értékelő azt állapítja meg, hogy az üzemeltetési környezetben meglévő IT vagy nem-IT intézkedések meggátolják a lehetséges sebezhetőségek kiaknázását az adott üzemeltetési környezetben. Például, ha a TOE-hoz való fizikai hozzáférés kizárólag a jogosult felhasználókra van korlátozva, akkor ez a hamisítás lehetséges sebezhetőségét eredményesen nem kihasználhatóvá teheti.

Az értékelőnek minden okot rögzítenie kell a lehetséges sebezhetőségek további mérlegelésből való kizárására, ha azt állapítja meg, hogy a lehetséges sebezhetőség nem kerülhet szóba az üzemeltetési környezetben. Egyéb esetekben az értékelőnek a lehetséges sebezhetőséget további mérlegelésre rögzítenie kell.

Az értékelőnek az ETR-ben meg kell adnia a TOE-val kapcsolatos, annak üzemeltetési környezetében felmerülő lehetséges sebezhetőségek listáját, mely az áthatolás tesztelési tevékenység bemeneteként használható.

6.2.4.5.1.4. Az AVA_VAN.2.4E értékelői akció

AVA_VAN.2.4E Az értékelőnek az azonosított lehetséges sebezhetőségek alapján áthatolás tesztelést kell végrehajtania, annak megállapítása érdekében, hogy a TOE ellenáll egy alap támadó képességgel bíró támadó által végrehajtott támadásnak.

AVA_VAN.2-6 Az értékelőnek a lehetséges sebezhetőségekre irányuló független keresés alapján meg kell terveznie az áthatolás teszteket.

Az értékelőnek kellően fel kell készülnie az áthatolás tesztelésre annak megállapítása érdekében, hogy a TOE üzemeltetési környezetében mennyire érzékeny azokra a lehetséges sebezhetőségekre, melyeket a nyilvánosan elérhető információ forrásokban való keresés során azonosított. Az értékelőnek figyelembe kell vennie bármely harmadik féltől (pl. tanúsító szervezet) kapott, ismert lehetséges sebezhetőségre vonatkozó aktuális információt, valamint a más értékelői tevékenységek eredményeként talált lehetséges sebezhetőségeket is.

Az értékelőnek szem előtt kell tartania, hogy ugyanúgy, mint a biztonsági szerkezet leírás mérlegelése esetében a sebezhetőségek felkutatásánál (ahogyan az AVA_VAN.2-3-ben részletezve van), tesztelést kell végrehajtania a szerkezeti tulajdonságok megerősítésére. Ez valószínűleg negatív teszteket igényel, amelyek a biztonsági szerkezet tulajdonságainak megcáfolását kísérlik meg. Az áthatolás tesztelés stratégiájának kialakításakor az értékelőnek garantálnia kell, hogy a biztonsági szerkezet leírás minden főbb jellegzetessége tesztelésre kerüljön vagy a funkcionális tesztelésnél, vagy az értékelői áthatolás tesztelésnél.

Az áthatolás tesztelést az értékelő valószínűleg tesztesetek sorozatával találja célszerűnek elvégezni, ahol az egyes tesztesetek egy-egy adott lehetséges sebezhetőséget próbálnak ki.

Az értékelőre nézve nem elvárás, hogy teszteket végezzen azokon a lehetséges sebezhetőségeken (beleértve a nyilvánosan ismerteket is) túlmutatóan, melyek

kihasználásához alap támadó képesség szükséges. Egyes esetekben azonban még a kihasználhatóság meghatározása előtt szükség lehet egy teszt végrehajtására. Amennyiben értékelői tapasztalata segítségével az értékelő egy alap támadó képesség felett álló kihasználható sebezhetőséget tár fel, ezt az értékelési jelentésében maradvány sebezhetőségként szerepeltetnie kell.

Egy adott lehetséges sebezhetőség kihasználásához szükséges támadó képesség meghatározásához útmutató található a 7.3.4 pontban.

Az olyan lehetséges sebezhetőségek, melyek feltételezhetően csak megemelt-alap, közepes vagy magas támadó képességgel kihasználhatók, nem eredményeznek „nem felelt meg" eredményt erre az értékelői tevékenységre. Amennyiben vizsgálat támogatja a fenti feltételezést, az érintett lehetséges sebezhetőséget a továbbiakban nem szükséges az áthatolás tesztelés bemeneteként kezelni. Ugyanakkor az ilyen sebezhetőséget az értékelési jelentésben maradvány sebezhetőségként szerepeltetni kell.

Az olyan lehetséges sebezhetőségeket, melyek feltételezhetően alap támadó képességgel kihasználhatók, és a biztonsági célok megsértését eredményezik, a legnagyobb elsőbbséggel ajánlott a lehetséges sebezhetőségek azon listájára felvenni, mely alapján a TOE közvetlen áthatolás tesztelését végzik.

AVA_VAN.2-7 Az értékelőnek a lehetséges sebezhetőségek listáján alapulva el kell készítenie az áthatolás tesztelési dokumentációt, a tesztek megismételhetőségét lehetővé tévő részletességgel. A tesztelési dokumentációnak tartalmaznia kell az alábbiakat:

a) a lehetséges sebezhetőség azonosítását, melyre a TOE-t tesztelik;
b) az áthatolás teszteléshez szükséges minden tesztberendezés csatlakoztatását és beállítását előíró utasítást;
c) az áthatolás tesztelés összes kezdeti előfeltételét kialakító utasításokat;
d) a TSF működését kiváltó utasításokat;
e) a TSF viselkedése megfigyeléséhez szükséges utasításokat;
f) minden várható eredmény leírását, valamint a várható eredményekkel való összehasonlításhoz végrehajtandó, megfigyelt működésre vonatkozó elemzéseket;
g) a tesztek befejezéséhez szükséges és a TOE tesztelés utáni állapotát biztosító utasításokat.

Az értékelőnek a lehetséges sebezhetőségek listáján alapulva el kell készítenie az áthatolás tesztelési dokumentációt, a tesztek megismételhetőségét lehetővé tévő részletességgel.

Az értékelőre nézve nem elvárás, hogy meghatározza a kihasználhatóságát azon lehetséges sebezhetőségeknek, melyek hatásos támadásához alap feletti támadó képesség szükséges. Ugyanakkor értékelői tapasztalata segítségével az értékelő feltárhat olyan lehetséges sebezhetőséget, melyet csak olyan támadó használhat ki, aki magasabb mint alap támadó képességgel rendelkezik. Az ilyen sebezhetőségeket az értékelési jelentésében maradvány sebezhetőségként szerepeltetni kell.

A lehetséges sebezhetőség ismeretében az értékelő határozza meg a leginkább megfelelő módot a TOE érzékenységének kimutatásához. Az értékelő különösen az alábbiakat vegye tekintetbe:

a) a TSFI és más TOE interfészeket, melyeket a TSF kiváltására és a válaszok megfigyelésére használnak (Lehet, hogy az értékelőnek egy TSFI-n kívüli TOE interfészt szükséges használnia a TOE azon tulajdonságainak demonstrálására, melyeket (az ADV_ARC által megkövetelt) biztonsági szerkezet leírás ír le. Megjegyzendő, hogy bár ezek a TOE interfészek lehetőséget adnak a TSF tulajdonságok tesztelésére, nem képezik tárgyát a tesztelésnek);
b) azokat a kezdeti feltételeket, melyek a tesztekhez szükségesek (azaz bármilyen szükséges objektum vagy szubjektum, illetve ezek szükséges biztonsági tulajdonságai);
c) speciális tesztberendezések, amelyek egy TSFI kiváltásához vagy megfigyeléséhez szükségesek (bár nem valószínű, hogy egy alap támadó képességet feltételező lehetséges sebezhetőség speciális tesztberendezést igényel);
d) bár elméleti vizsgálat helyettesítheti a fizikai tesztelést, különösen fontos eset, amikor egy kezdeti teszt eredményeként előre jelezhető, hogy egy támadás adott számú megismétlése valószínűleg sikeres lesz.

Az értékelő az áthatolás tesztelést valószínűleg tesztesetek sorozatával találja célszerűnek elvégezni, ahol az egyes tesztesetek egy-egy adott lehetséges sebezhetőséget próbálnak ki.

A tesztelési dokumentáció ilyen szintű részletessége azt hivatott biztosítani, hogy más értékelők is meg tudják ismételni a teszteket, és azonos eredményre juthassanak.

AVA_VAN.2-8 Az értékelőnek végre kell hajtania az áthatolás tesztelést.

Az értékelő az AVA_VAN.2-6 munkaegység eredményeképpen létrejött áthatolás tesztelési dokumentációt a TOE áthatolás tesztelésének alapjaként használja, de ez nem zárja ki, hogy más, ad hoc áthatolás tesztelést ne végezhessen el. Amennyiben szükséges, az értékelő ad hoc teszteket is elvégezhet az áthatolás tesztelés során tapasztaltak következtében, melyeket – ha az értékelő elvégzi azokat - az áthatolás tesztelési dokumentációban rögzítenie kell. E tesztekkel szemben követelmény lehet, hogy a nem várt eredményeket vagy megfigyeléseket ellenőrizzék, vagy hogy a tesztelés előkészítési szakaszában az értékelőnek javasolt lehetséges sebezhetőségeket megvizsgálják.

Amennyiben az áthatolás tesztelés azt mutatja, hogy egy feltételezett lehetséges sebezhetőség nem létezik, az értékelőnek ajánlott megállapítania, hogy a saját elemzése volt téves, vagy az értékelésre átadandók voltak hibásak, hiányosak.

Az értékelőre nézve nem elvárás, hogy teszteket végezzen azokon a lehetséges sebezhetőségeken (beleértve a nyilvánosan ismerteket is) túlmutatóan, melyek kihasználásához alap támadó képesség szükséges. Egyes esetekben azonban még a kihasználhatóság meghatározása előtt szükség lehet egy teszt végrehajtására. Amennyiben értékelői tapasztalata segítségével az értékelő egy alap támadó képesség felett álló kihasználható sebezhetőséget tár fel, ezt az értékelési jelentésében maradvány sebezhetőségként szerepeltetnie kell.

AVA_VAN.2-9 Az értékelőnek rögzítenie kell az áthatolás tesztek tényleges eredményeit.
A tényleges eredmények bizonyos részletei különbözhetnek a várható értékektől (pl. idő és dátummezők a naplóban), de az összeredménynek meg kell egyeznie. Javasolt minden

váratlan teszteredményt kivizsgálni, valamint ezek értékelésre gyakorolt hatását kimondani és igazolni.

AVA_VAN.2-10 Az értékelőnek az értékelési jelentés keretén belül jelentést kell írnia az értékelői áthatolás tesztelésről, leírván a tesztelési módszert, konfigurációt, mélységet és eredményeket.

Az értékelési jelentésben rögzített áthatolás tesztelésről szóló információ lehetővé teszi az értékelő számára, hogy bemutassa az általános tesztelési módszert és az ezen tevékenység végrehajtásába fektetett munkát. A cél az értékelő áthatolás tesztelési munkájának érdemi áttekintése. Nem cél, hogy az értékelési jelentésben az áthatolás teszteléssel kapcsolatos információk a specifikus tesztlépések vagy egyedi áthatolás tesztek eredményeinek pontos megismétlése legyenek. A cél elegendő részletesség biztosítása más értékelők és a tanúsító szervezet számára ahhoz, hogy betekintést kapjanak a választott áthatolás tesztelési módszerbe, a végrehajtott áthatolás tesztek nagyságrendjébe, a TOE teszt konfigurációjába és az áthatolás tesztelési tevékenység általános eredményébe.

Az értékelési jelentés értékelői áthatolás tesztelésről szóló része általában az alábbi információkat tartalmazza:

a) TOE tesztkonfigurációk; az áthatolás tesztelésnél használt konkrét TOE konfigurációk.
b) Az áthatolás teszt során tesztelt TSFI-k. Az áthatolás tesztelés középpontjában álló TSFI-k és egyéb TOE interfészek rövid felsorolása.
c) Az altevékenység alapján született határozat. Az áthatolás tesztelés eredményeinek általános megítélése.

E lista korántsem teljes, csupán felvillant néhány szempontot, melyeknek az értékelő áthatolás tesztelésével kapcsolatosan az értékelési jelentésben ajánlott szerepelniük.

AVA_VAN.2-11 Az értékelőnek meg kell vizsgálnia az összes áthatolás teszt eredményét annak megállapítása érdekében, hogy a TOE üzemeltetési környezetében ellenáll-e egy alap támadó képességgel rendelkező támadónak.

Amennyiben az eredmények azt mutatják, hogy a TOE üzemeltetési környezetében kihasználható sebezhetőségeket tartalmaz alap támadó képességgel rendelkező támadók számára, akkor ez az értékelői akció "Nem felelt meg" határozatot eredményez.

A 7.3.4 mellékletet kell használni egy adott sebezhetőség kihasználásához szükséges támadó képesség meghatározásához, illetve annak eldöntésére, hogy a sebezhetőség a tervezett üzemeltetési környezetben kihasználható-e. Nem feltétlenül kell minden esetben kiszámolni a támadó képességet, csak ha felmerül annak lehetősége, hogy egy alap támadó képességgel rendelkező támadó kihasználhatja a sebezhetőséget.

AVA_VLA.2-12 Az értékelőnek az értékelési jelentés keretén belül jelentést kell írnia az összes kihasználható sebezhetőségről és maradvány sebezhetőségről, az alábbi adatokkal:

a) forrás (pl. azon CEM tevékenység, melynek végrehajtása során észlelték, az értékelő ismerte, szakirodalomban olvasott róla);
b) a nem kielégített SFR(-ek);

c) leírás;
d) kihasználható-e vagy sem az üzemeltetési környezetben (vagyis kihasználható vagy maradvány sebezhetőségről van szó);
e) az azonosított sebezhetőség kihasználáshoz szükséges felhasznált idő, szakértelem, TOE ismeret, hozzáférési lehetőség, eszköz, valamint az ezekhez rendelt értékek a 7.3.4 melléklet 8. és 9. táblázata alapján.

6.2.5. Termék értékelés kiemelt garanciaszinten

6.2.5.1. A Fejlesztés garanciaosztály (ADV) értékelése

A fejlesztési tevékenységnek az a célja, hogy a terv dokumentációt felmérje abból a szempontból, hogy az megfelelő-e annak megértéséhez, hogy a TSF hogyan teljesíti az SFR-eket, és hogy az SFR-ek megvalósítását nem lehet meghamisítani vagy megkerülni. Ezt a megértést a TSF terv dokumentációhoz tartozó egyre részletesebb leírások vizsgálatán keresztül lehet elérni. A terv dokumentáció a funkcionális specifikációból (ami a TSF interfészeit írja le), a TOE tervből (ami a TSF szerkezetét írja le abból a szempontból, hogy az hogyan működik a megkívánt SFR-ekhez kapcsolódó funkciók végrehajtása érdekében) és egy megvalósítási leírásból (forráskód szintű leírás) áll. Ezenfelül létezik egy biztonsági szerkezet leírás, amely a TSF szerkezeti tulajdonságait ismerteti annak kifejtése céljából, hogy ennek biztonsági szempontú érvényre jutását nem lehet meghamisítani vagy megkerülni.

A terv dokumentációra vonatkozó CC követelmények szintjei aszerint különböznek, hogy mennyi és milyen részletes információt kell biztosítani, milyen mértékű formalizmussal. Az alacsonyabb szinteken a TSF biztonság szempontból legkritikusabb részeit a legnagyobb részletességgel kell ismertetni, míg a biztonság szempontjából kevésbé fontos részeket csak összegezni kell; további garancia nyerhető azáltal, ha növelik a TSF biztonság szempontból legkritikusabb részeire vonatkozó információk mennyiségét, és ha növelik a kevésbé fontos részekre vonatkozó részleteket. A legnagyobb garancia akkor érhető el, ha minden részre vonatkozóan mélyreható részleteket és információkat adnak meg.

A CC a dokumentumok formalizmusának a mértékét (vagyis azt, hogy a dokumentum informális-e vagy félformális) hierarchikusnak tekinti. Informális az a dokumentum, amelyet természetes nyelven fejeztek ki. A módszertan nem ír elő kötelezően használandó meghatározott nyelvet; ez a kérdés a sémára van hagyva. A következő fejezetek a különböző informális dokumentumok tartalmát ismertetik.

Egy funkcionális specifikáció leírást nyújt a TSF-hez kapcsolódó interfészek rendeltetéséről és használati módjáról. Például, ha egy operációs rendszer eszközt biztosít a felhasználó számára az ön-azonosításra, fájlok létrehozására, fájlok módosítására vagy törlésére, olyan engedélyek beállítására, amelyek meghatározzák, hogy mely egyéb felhasználók férhetnek hozzá fájlokhoz, és eszközt biztosít a távoli gépekkel való kommunikációra, akkor az operációs rendszer funkcionális specifikációjának tartalmaznia kell mindezeknek az ismertetését, és azt, hogy ezeket hogyan valósítják meg a TSF-hez csatlakozó kívülről látható interfészeken keresztüli kölcsönhatások. Ha létezik egy naplózási funkcionalitás is, amely észleli és rögzíti az ilyen események előfordulásait, akkor az is elvárás, hogy ez a naplózási funkcionalitás része legyen a funkcionális specifikációnak; és bár ezt a funkcionalitást

technikailag nem közvetlenül a felhasználó idézi elő a külső interfészen, biztosan kihat erre az, ami a felhasználói külső interfészen történik.

A terv leírást logikai alkotóelemek (alrendszerek vagy modulok) szerint fejezik ki, amelyek mindegyike egy érthető szolgáltatást vagy funkciót biztosít. Például egy tűzfal állhat olyan alrendszerekből, amelyek csomagszűréssel, távoli adminisztrációval, naplózással és kapcsolat-szintű szűréssel foglalkoznak. A tűzfal terv leírásnak ekkor ismertetnie kell, hogy az egyes alrendszerek milyen tevékenységeket hajtanak végre, amikor egy bejövő csomag megérkezik a tűzfalhoz.

6.2.5.1.1. Biztonsági szerkezet: Az ADV_ARC.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak a megállapítása, hogy a TSF olyan módon van-e megszerkesztve, hogy azt nem lehet meghamisítani vagy megkerülni, és hogy a biztonsági tartományokat biztosító TSF-ek a szóbanforgó tartományokat elkülönítik-e egymástól.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) TOE terv,
d) biztonsági szerkezet leírás,
e) megvalósítás reprezentáció,
f) üzemeltetési felhasználói útmutató.

Az önvédelem, a tartomány szétválasztás és a nem-megkerülhetőség elveit elkülönítik attól a biztonsági funkcionalitástól, melyet a CC 2. részbeli SFR-ek fejeznek ki, minthogy az önvédelem és nem-megkerülhetőség egyáltalán nem rendelkezik közvetlenül megfigyelhető interfésszel a TSF-en. Ezek inkább olyan tulajdonságai a TSF-nek, amelyeket a TOE és TSF tervezésén keresztül valósítanak meg, és amelyeket a szóbanforgó terv helyes megvalósításával juttatnak érvényre. Ezenfelül ezen tulajdonságok értékelése kevésbé célirányos, mint a mechanizmusok értékelése; egy funkcionalitásnak a hiányát sokkal nehezebb ellenőrizni, mint a meglétét. Annak a megállapítása azonban, hogy ezek a tulajdonságok teljesülnek, éppen olyan kritikus, mint annak a megállapítása, hogy egy mechanizmust helyesen valósítottak meg.

Az általánosan alkalmazott megközelítési mód szerint a fejlesztő biztosítja a fent említett tulajdonságokat teljesítő TSF-et, és bizonyítékot is átad (dokumentáció formájában), amelyet megvizsgálásával belátható, hogy a tulajdonságok valóban teljesülnek. Az értékelő felelőssége, hogy megtekintse a bizonyítékot, a TOE-hoz és TSF-hez átadott egyéb bizonyítékokkal társítva, és megállapítsa, hogy a tulajdonságok megvalósulnak-e. A munkaegységek jellemezhetők úgy, hogy vannak olyanok, amelyek azzal foglalkoznak, hogy milyen információt kell átadni, és vannak olyanok, amelyek az értékelő által végrehajtott tényleges vizsgálatokkal foglalkoznak.

A biztonsági szerkezet leírás ismerteti, hogy a biztonsági tartományokat hogyan definiálták, és a TSF hogyan tartja fenn ezek elkülönülését. Ismerteti, hogy mi gátolja meg a nem-megbízható eljárásokat abban, hogy hozzájussanak a TSF-hez és módosítsák azt. Ismerteti, hogy mi garantálja azt, hogy a TSF ellenőrzése alá tartozó minden erőforrás megfelelő módon

védve van, és hogy minden SFR-vonatkozású tevékenységet a TSF közvetít. Megmagyaráz minden szerepet, amit a környezet tölt be ezek valamelyikénél (pl. hogyan történik a biztonsági funkcionalitás aktivizálása, feltételezve, hogy a tevékenységet az alátámasztó környezet helyesen aktivizálja?). Röviden, megmagyarázza, hogy a TOE az elgondolások szerint hogyan fog valamilyen biztonsági szolgáltatást nyújtani.

Az értékelők által végrehajtott vizsgálatokat a TOE-hoz átadott minden fejlesztői bizonyítékkal kapcsolatban olyan részletesen kell elvégezni, ahogyan az adott bizonyítékot szolgáltatták.

6.2.5.1.1.1. Az ADV_ARC.1.1E értékelői akció

ADV_ARC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ADV_ARC.1.1C A biztonsági szerkezet leírást olyan szinten kell részletezni, amely összemérhető a TOE terv dokumentációban ismertetett, SFR-t érvényre juttató absztrakciók leírásával.

ADV_ARC.1-1 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy az ebben biztosított információk részletessége összemérhető-e a TOE terv dokumentációban és a funkcionális specifikációban ismertetett, SFR-t érvényre juttató absztrakciók leírásával.

A funkcionális specifikáció vonatkozásában az értékelő győződjön meg arról, hogy az ismertetett önvédelmi funkcionalitás lefedi-e azokat a hatásokat, amelyek nyilvánvalóak a TSFI-n. Egy ilyen leírás magában foglalhatja a TSF futtatható formáira, illetve az objektumokra (pl. TSF által használt fájlok) elhelyezett védelmet. Az értékelő győződjön meg arról, hogy a TSFI-n keresztül aktivizálható funkcionalitást leírták.

Az értékelő győződjön meg arról, hogy a biztonsági szerkezet leírás tartalmaz-e megvalósítás-függő információt is. Például, egy ilyen leírás tartalmazhat információt az olyan paraméter ellenőrzésekre vonatkozó kódolási konvenciókról, amelyek meggátolják a TSF veszélyeztetését (pl. buffer túlcsordulás), és tartalmazhat információt a hívási és visszatérési műveletekhez tartozó stack kezelésről. Az értékelő ellenőrizze a mechanizmusok leírását, és győződjön meg arról, hogy a részletezettségi szint miatt kicsi a kétértelműség a biztonsági szerkezet leírás és a megvalósítási reprezentáció között.

Az ehhez a munkaegységhez kapcsolódó értékelői akció kapjon „nem felelt meg” határozatot, ha a biztonsági szerkezet leírás megemlít bármilyen olyan modult, alrendszert vagy interfészt, amelyet a funkcionális specifikáció vagy a TOE terv dokumentum nem ismertet.

ADV_ARC.1.2C A biztonsági szerkezet leírásnak ismertetnie kell a TSF által kezelt biztonsági tartományokat, összhangban az SFR-ekkel.

ADV_ARC.1-2 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy az ismerteti-e a TSF által kezelt biztonsági tartományokat.

A biztonsági tartományok olyan környezetekre vonatkoznak, amelyeket a TSF nyújt potenciálisan kárt-okozó egyedek általi használatra; például, egy tipikus biztonságos operációs rendszer számos erőforrást nyújt olyan eljárások számára, amelyek korlátozott hozzáférési jogokkal és biztonsági tulajdonságokkal rendelkeznek. Az értékelő állapítsa meg, hogy a biztonsági tartományok fejlesztői leírása minden olyan SFR-t figyelembe vesz, amit a TOE megkíván.

Bizonyos TOE-k esetében nem léteznek ilyen tartományok, mivel a felhasználók számára rendelkezésre álló minden kölcsönhatást szigorúan a TSF tartalmaz. Ilyen TOE-ra példa egy csomag-szűrő tűzfal. A LAN-on vagy WAN-on lévő felhasználók nem lépnek kölcsönhatásba a TOE-val, így nincsen szükség biztonsági tartományokra; csak a TSF által kezelt adat-struktúrák szolgálnak arra, hogy a felhasználói csomagokat elkülönítetten tartsák. Az értékelő győződjön meg arról, hogy minden olyan állítás, hogy nincsen biztonsági tartomány, alá van támasztva bizonyítékkal, és győződjön meg arról is, hogy ilyen tartományok valóban nem állnak rendelkezésre.

ADV_ARC.1.3C A biztonsági szerkezet leírásnak ismertetnie kell, hogy a TSF inicializálási eljárása milyen mértékben biztonságos.

ADV_ARC.1-3 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy a TSF inicializálási eljárása megőrzi a biztonságot.

A TSF inicializálására vonatkozó, a biztonsági szerkezet leírásban megadott információ azokra a TOE összetevőkre irányul, amelyek közreműködnek abban, hogy a TSF-et egy kezdeti biztonságos állapotba hozzák (vagyis amikor a TSF-nek már minden része működőképes), bekapcsoláskor vagy reset esetén. A biztonsági szerkezet leírásban ez a fejtegetés sorolja fel azokat a rendszer-inicializálási összetevőket és feldolgozásokat, amelyek érintve vannak a „kikapcsolt” állapotból a kezdeti biztonságos állapotba való átmenet során.

Gyakran fordul elő az az eset, hogy az inicializálási funkciót ellátó összetevők a biztonságos állapot elérése után már nem állnak rendelkezésre; ebben az esetben a biztonsági szerkezet leírás határozza meg ezeket az összetevőket, és magyarázza meg, hogy milyen mértékben igaz az, hogy nem-megbízható egyedek nem tudják elérni ezeket a TSF felállása után. Ebben a vonatkozásban az a tulajdonság, amelyet fenn kell tartani, az, hogy 1) a biztonságos állapot elérése után nem-megbízható egyedek nem férhetnek hozzá ezekhez az összetevőkhöz, vagy pedig 2) ha ezek az összetevők nyújtanak is interfészeket nem-megbízható egyedek számára, akkor ezek a TSFI-k nem használhatók a TSF működésébe történő hamisításra.

A TSF inicializálásához kapcsolódó TOE összetevők a TSF inicializálását követően a TSF részeként kezelik magukat, és ebből a nézőpontból vizsgálandók. Meg kell jegyezni, hogy még ha ezeket a TSF részeként is kezelik, valószínűleg megindokolható, hogy ezeknek nem kell teljesíteni az ADV_INT belső szerkezeti követelményeket (ahogyan az ADV_INT erre lehetőséget nyújt).

ADV_ARC.1.4C A biztonsági szerkezet leírásnak szemléltetnie kell, hogy a TSF megvédi magát a hamisítással szemben.

ADV_ARC.1-4 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy az kellő információt biztosít annak megállapításához, hogy a TSF képes megvédi magát a nem-megbízható aktív egyedek hamisításával szemben.

Az „önvédelem” a TSF-nek arra a képességére utal, hogy meg tudja védeni saját magát a külső egyedek olyan manipulációival szemben, amelyek a TSF megváltoztatásaihoz vezethetnek. A más IT egyedektől függő TOE-k esetében gyakran előfordul, hogy a TOE olyan szolgáltatást használ fel funkciói végrehajtásához, amelyeket más IT egyedek szolgáltatnak. Az ilyen esetekben a TSF önmagában nem tudja megvédeni saját magát, mivel más IT egyedektől függ az, hogy valamilyen védelmet tud biztosítani. A biztonsági szerkezet leírás szempontjából az önvédelem elve csak azokra a szolgáltatásokra vonatkozik, amelyeket a TSF nyújt a TSFI-ken keresztül, és nem vonatkozik azokra a szolgáltatásokra, amelyeket az általa használt támogató IT egyedek szolgáltatnak.

Az önvédelem általában számos eszközzel elérhető, a TOE-hoz való hozzáférés fizikai és logikai korlátozásától kezdődően a hardver-alapú (pl. memóriakezelési funkcionalitás) és szoftver-alapú (pl. bemenetek korlát-érték ellenőrzései egy megbízható szerveren) eszközökig. Az értékelő állapítsa meg, hogy minden ilyen mechanizmus ismertetve lett.
Az értékelő állapítsa meg, hogy a terv leírás lefedi azt, hogy a TSF hogyan kezeli a felhasználói bemenetet abból a szempontból, hogy az ne ronthassa le a TSF-et. Például a TSF megvalósíthatja a privilégium elvét és megvédheti magát azzal, hogy privilegizált-módban futó rutinokat alkalmaz a felhasználói bemenetek kezelésére. A TSF hasznosíthatja az olyan processzor-alapú elkülönítési mechanizmusokat, mint amilyenek a privilégium szintek vagy gyűrűk. A TSF megvalósíthat olyan szoftver védelmi szerkezeteket vagy kódolási konvenciókat, amelyek hozzájárulnak a szoftver tartományok elkülönítésének megvalósításához, feltehetően azzal, hogy a felhasználói címteret elhatárolják a rendszer címtértől. Ezenfelül a TSF bízhat abban, hogy a környezet biztosít bizonyos védelmet.

A tartomány elválasztási funkciókhoz hozzájáruló összes mechanizmust le kell írni. Az értékelő mindazokat az ismereteket, amelyeket más bizonyítékokból (kiemelt garanciaszinten: funkcionális specifikáció, TOE terv, a biztonsági szerkezet egyéb részeinek leírása, megvalósítási reprezentáció) szerzett meg, használja fel annak megállapításánál, hogy az önvédelemhez hozzájáruló minden olyan funkcionalitást is ismertettek, amely a biztonsági szerkezet leírásban nem szerepel.

Az önvédelmi mechanizmusok leírásának helyessége az a tulajdonság, hogy a leírás hitelt érdemlően ismerteti, hogy mit valósítottak meg. Az értékelő használjon fel egyéb bizonyítékokat (kiemelt garanciaszinten: funkcionális specifikáció, TOE terv, a biztonsági szerkezet egyéb részeinek leírása, megvalósítási reprezentáció) annak megállapításához, hogy az önvédelmi mechanizmus leírásai ellentmondanak-e egymásnak. Mivel a kiemelt garanciaszint tartalmazza a „Megvalósítási reprezentáció”-t (ADV_IMP.1), az értékelő mintát fog venni a megvalósítási reprezentációból; ekkor az értékelő győződjön meg a leírások helyességéről a kiválasztott mintára vonatkozóan is. Ha egy értékelő nem látja át, hogy egy meghatározott önvédelmi mechanizmus hogyan működik, vagy hogyan működne a rendszer architektúrában, lehetséges, hogy ez egy olyan eset, amikor a leírás nem helyes.

ADV_ARC.1.5C A biztonsági szerkezet leírásnak szemléltetnie kell, hogy a TSF meggátolja az SFR-t érvényre juttató funkcionalitás megkerülését.

ADV_ARC.1-5 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy az bemutat-e olyan vizsgálatot, ami megfelelő módon ismerteti, hogy az SFR-t érvényre juttató mechanizmusokat milyen mértékben nem lehet megkerülni.

A nem-megkerülhetőség egy olyan tulajdonság, hogy a TSF biztonsági funkcionalitása (ahogyan azt az SFR-ek specifikálják) mindig működésbe lép. Például, ha a fájlokhoz való hozzáférés a TSF-nek az egyik, SFR-en keresztül specifikált tulajdonsága, akkor nem szabad előfordulnia olyan interfésznek, amin keresztül a fájlokhoz hozzá lehet férni a TSF hozzáférés ellenőrzési mechanizmusa aktivizálása nélkül (vagyis nem szabad előfordulnia például olyan interfésznek, amelyen keresztül közvetlenül hozzá lehet férni egy diszkhez).

Annak leírása, hogy a TSF mechanizmusokat miért nem lehet megkerülni, általában módszeres indoklást igényel a TSF-en és a TSFI-ken alapulva. Annak leírása, hogy a TSF hogyan működik (amit a terv lebontási bizonyítékok, vagyis a funkcionális specifikáció és TOE terv dokumentáció tartalmaznak) – a TSS-ben foglalt információ mellett – biztosítja a szükséges hátteret ahhoz, hogy az értékelő megértse, hogy mely erőforrásokat kell védeni, és milyen biztonsági funkciókat kell biztosítani. A funkcionális specifikáció adja meg a TSFI-k ismertetését, amelyeken keresztül az erőforrások/funkciók hozzáférhetők.

Az értékelő becsülje fel az átadott leírásokat (és a fejlesztő által biztosított egyéb információkat, mint például a funkcionális specifikáció), hogy meggyőződjön arról, hogy nem áll rendelkezésre olyan interfész, amelyet a TSF megkerülésére lehetne használni. Ez azt jelenti, hogy az egyes interfészeknek vagy nem szabad kapcsolatban állniuk az ST-ben előírt SFR-ekkel (és nem szabad kölcsönhatásban lenniük semmi olyannal sem, amit felhasználnak az SFR-ek kielégítésére), vagy a más fejlesztői bizonyítékokban leírt biztonsági funkcionalitást az ismertetett módon kell használniuk. Például egy játék valószínűleg nem áll kapcsolatban az SFR-ekkel, így meg kell magyarázni, hogy miért nem befolyásolja a biztonságot. A felhasználói adatokhoz való hozzáférés azonban feltehetően kapcsolatban áll hozzáférés ellenőrzési SFR-ekkel, így a magyarázatnak ismertetnie kell azt, hogy a biztonsági funkcionalitás hogyan működik, amikor az adathozzáférési interfészeken keresztül aktivizálódik. Ilyen leírás szükséges minden elérhető interfészre.

Leírásra példa a következő. Tegyük fel, hogy a TSF fájlvédelmet biztosít. Tegyük fel továbbá, hogy bár a „hagyományos” TSFI megnyitási, olvasási és írási rendszerhívások aktivizálják a TOE tervben ismertetett fájlvédelmi mechanizmusokat, létezik egy TSFI, amely hozzáférést biztosít egy batch job lehetőséghez (batch job-ok létrehozása, job-ok törlése, nem végrehajtott job-ok módosítása). Az értékelőnek a megbízó által biztosított leírásból dönteni kell tudnia arról, hogy a szóbanforgó TSFI ugyanazt a védelmi mechanizmust aktivizálja-e, mint a „hagyományos” interfészek. Ez elérhető például a TOE terv megfelelő részeire való hivatkozással, amely azt tárgyalja, hogy a batch job lehetőséggel rendelkező TSFI hogyan valósítja meg biztonsági céljait.

Ugyanezen példát használva tételezzük fel, hogy létezik egy TSFI, amelynek az egyetlen célja, hogy kijelezze az időpontot. Az értékelő állapítsa meg, hogy a leírás megfelelő módon bizonyítja, hogy ez a TSFI nem képes egyetlen védett erőforrás manipulálására sem, és nem aktivizálhat egyetlen biztonsági funkcionalitást sem.

A megkerülésre egy másik példa az, amikor feltételezik, hogy a TSF megőrzi egy kriptográfiai kulcs bizalmasságát (ami felhasználható kriptográfiai műveletekhez, de amit nem szabad írni és olvasni). Ha egy támadó közvetlenül fizikailag hozzáfér az eszközhöz, képes lehet arra, hogy oldal-csatornákat vizsgáljon -mint például az eszköz áramfelvételét, az eszköz pontos időzítését, vagy az eszköz valamilyen elektromágneses kisugárzását-, és ebből következtessen a kulcsra.

Ha létezhetnek ilyen oldal-csatornák, a szemléltetés vegye tekintetbe azokat a mechanizmusokat, amelyek meggátolják ezeknek az oldal-csatornáknak a bekövetkezését, mint például véletlen belső órák, két-utas technológia stb. A szóbanforgó mechanizmusok ellenőrizhetők a tisztán terv-alapú érvelések és a tesztelések kombinációjával.

Utolsó példáként arra, hogy biztonsági funkcionalitást használnak védett erőforrás helyett, tételezzünk fel egy olyan ST-t, amely tartalmazza az „Az eredet kikényszerített bizonyítása” (FCO_NRO_2) biztonsági követelményt, amely megkívánja, hogy a TSF bizonyítékot nyújtson az ST-ben specifikált információ-típusok eredetére vonatkozóan. Tételezzük fel, hogy az „információ-típusok” magukban foglalnak minden információt, amelyet a TOE felhasználásával küldenek e-mailen keresztül. Ebben az esetben az értékelő vizsgálja meg a leírást, hogy meggyőződjön arról, hogy minden TSFI részletezve van, amely aktivizálható e-mail küldése céljából, és ezek végrehajtják az „Az eredet kikényszerített bizonyítása” funkciót. A leírás utalhat az üzemeltetési felhasználói útmutatóra, hogy minden helyet bemutasson, ahonnan e-mail származhat (pl. levelező program, scriptektől/batch-job-októl származó értesítések), és hogy bemutassa, hogy mindezek a helyek hogyan aktivizálják az eredet előállítása funkciót.

Az értékelő győződjön meg arról is, hogy a leírás átfogó, amelyben minden interfészt megvizsgálnak a megkívánt SFR-ek teljes összessége szerint. Ez megkívánhatja az értékelőtől, hogy vizsgálja meg az alátámasztó információkat (funkcionális specifikáció, TOE terv, a biztonsági szerkezet leírás egyéb részei, az üzemeltetési felhasználói útmutató, és a megvalósítási reprezentáció) annak megállapítása érdekében, hogy a leírás helyesen ragadta-e meg az egyes interfésznek minden vonatkozását. Az értékelő gondolja át, hogy az egyes TSFI-k mely SFR-ekre lehetnek befolyással (a TSFI leírásból és ennek megvalósításából az alátámasztó dokumentációban), és ezután vizsgálja meg a leírást annak megállapítása érdekében, hogy az lefedi-e a szóbanforgó vonatkozást.

6.2.5.1.2. Funkcionális specifikáció: Az ADV_FSP.4 altevékenység értékelése

Ennek az altevékenységnek a célja annak a megállapítása, hogy a fejlesztő teljes mértékben leírt-e minden TSFI-t oly módon, hogy az értékelő képes legyen megállapítani, hogy a TSFI-ket teljes mértékben és helyesen ismertették, és nyilvánvaló-e, hogy ezek megvalósítják az ST biztonsági funkcionális követelményeit.

Az ehhez az altevékenységhez a munkaegységek által megkövetelt értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) TOE terv.

Az ehhez az altevékenységhez felhasznált egyéb értékelési bizonyíték:

a) biztonsági szerkezet leírása,
b) megvalósítási reprezentáció,
c) üzemeltetési felhasználói útmutató.

A funkcionális specifikáció a TSF-hez csatlakozó interfészeket (TSFI-ket) rendszerezetten ismerteti. Az ADV_TDS.l altevékenység értékelésétől való függőség miatt az értékelőtől elvárják, hogy azonosítsa a TSF-et, mielőtt megkezdi az ezen altevékenységhez tartozó munkát. A TSF teljessége nem értékelhető annak pontos ismerete nélkül, hogy miből áll a TSF.

Az ezen családhoz tartozó különféle munkaegységek végrehajtása közben szükséges, hogy az értékelő számos tényező helyességét és teljességét felmérje (magának a TSFI-nek, illetve a TSFI egyedi összetevőinek (paramétereknek, tevékenységeknek, hibaüzeneteknek, stb.) is). A vizsgálathoz az értékelőnek fel kell használnia az értékeléshez átadott dokumentációt. Ez magában foglalja az ST-t, a TOE tervet, valamint magában foglalhat további dokumentációt, mint például az üzemeltetési felhasználói útmutatót, a biztonsági szerkezet leírást, és a megvalósítási reprezentációt. A dokumentáció legyen iteratív módon vizsgálva. Az értékelő elolvashatja például a TOE tervben, hogy egy bizonyos funkciót hogyan valósítottak meg, de lehet, hogy nem lát módot arra, hogy a szóbanforgó funkciót aktivizálják az interfészről. Ez azt eredményezheti, hogy az értékelő megkérdőjelezheti, hogy egy meghatározott TSFI leírás teljes-e, vagy hogy nem lett-e egy interfész teljesen kifelejtve a funkcionális specifikációból. Az ilyenfajta vizsgálati tevékenységek értékelési jelentésben történő ismertetése kulcsfontosságú módszer annak indoklására, hogy a munkaegységet megfelelően hajtották végre.

Léteznek olyan funkcionális követelmények, amelyek funkcionalitása teljes egészében vagy részben architektúrálisan jelenik meg, nem egy meghatározott mechanizmuson keresztül. Példák erre a „Maradék információ védelem” (FDP_RIP) követelményeket megvalósító mechanizmusok. Az ilyen mechanizmusokat általában annak biztosítására valósítják meg, hogy egy bizonyos viselkedésmód ne valósuljon meg. Ezt nehéz tesztelni, és általában nehéz vizsgálatokkal igazolni. Azokban az esetekben, amikor az ST tartalmaz ilyen funkcionális követelményeket, az értékelőnek fel kell ismernie, hogy létezhetnek ilyen típusú SFR-ek, amelyekhez nem tartoznak interfészek, és hogy ezt nem lehet a funkcionális specifikáció hiányosságának tekinteni.

6.2.5.1.2.1. Az ADV_FSP.4.1E értékelői akció

ADV_FUN.4.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ADV_FSP.4.1C A funkcionális specifikációnak teljes mértékben be kell mutatnia a TSF-et.

ADV_FSP.4-1 Az értékelőnek meg kell vizsgálnia a funkcionális specifikációt annak megállapítása érdekében, hogy az teljes mértékben bemutatja-e a TSF-t.

Ennél az altevékenységnél a TSFI azonosítása szükséges előfeltétel minden egyéb tevékenységhez. A TSFI azonosítása érdekében azonosítani kell a TSF-t (a „TOE terv” (ADV_TDS) munkaegységei részeként). Ez a tevékenység végrehajtható magas szinten, annak biztosításával, hogy az interfészek nagy csoportjai (hálózati protokollok, hardver interfészek, konfigurációs fájlok) nem maradtak ki, vagy alacsony szinten, ahogy a funkcionális specifikáció értékelése előrehalad.

Ezen munkaegység értékelésekor az értékelő állapítsa meg, hogy a TSF minden részét figyelembe vették-e a funkcionális specifikációban felsorolt interfészek szerint. A TSF minden részéhez tartozzon egy interfész leírás, vagy ha a TSF valamely részéhez nem tartozik interfész, az értékelő állapítsa meg, hogy ez elfogadható.

ADV_FSP.4.2C A funkcionális specifikációnak le kell írnia minden TSFI rendeltetését és használati módját.

ADV_FSP.4-2 Az értékelőnek meg kell vizsgálnia a funkcionális specifikációt annak megállapítása érdekében, hogy az meghatározza-e minden TSFI rendeltetését.

Egy TSFI rendeltetése egy olyan általános kijelentés, amely összegzi az interfész által nyújtott funkcionalitást. Az interfészhez kapcsolódó minden tevékenység és eredmény teljes megfogalmazása nem szükséges, de a felhasználót segítenie kell annak általános megértésében, hogy az interfészt mire szánták. Az értékelő ne csak a rendeltetés létezését állapítsa meg, hanem azt is, hogy ez helyesen tükrözi a TSFI-t, figyelembe véve az interfészre vonatkozó egyéb információkat is, mint például a tevékenységek leírása és a hibaüzenetek.

ADV_FSP.4-3 Az értékelőnek meg kell vizsgálnia a funkcionális specifikációt annak megállapítása érdekében, hogy az meghatározza-e minden TSFI használati módját.

Egy TSFI használati módja összegzi, hogy az interfészt hogyan kell kezelni a TSFI-vel kapcsolatos tevékenységek kiváltása és az eredmények megszerzése érdekében. Az értékelő állapítsa meg a funkcionális specifikációban megadott anyagból, hogy hogyan kell használni az interfészt. Ez nem feltétlenül jelenti azt, hogy minden egyes TSFI-hez léteznie kell egy külön használati módnak, például valószínűleg általánosan leírható a kernel-hívások aktivizálási módja, majd megadható minden olyan interfész, ami ezt az általános módszert használja. A különböző típusú interfészek eltérő használási mód meghatározást kívánnak. Az API-k, a hálózati protokoll interfészek, a rendszer konfigurációs paraméterek és hardver busz interfészek mindegyikéhez eltérő használati mód tartozik, és ezt a fejlesztőnek figyelembe kell vennie, amikor a funkcionális specifikációt kialakítja, ahogy az értékelőnek is figyelembe kell vennie, amikor a funkcionális specifikáció értékeli.

Az olyan adminisztrációs interfészek esetében, amelyek funkcionalitását úgy dokumentálták, hogy ahhoz nem-megbízható felhasználó nem férhet hozzá, az értékelőnek meg kell győződnie arról, hogy a funkcionális specifikáció leírja azt a módszert, amellyel a funkciót hozzáférhetetlenné teszik. Meg kell jegyezni, hogy a hozzáférhetetlenséget a fejlesztőnek tesztelnie kell tesztkészletében.

Az értékelőnek nemcsak a használati mód leírások létezését kell megállapítania, hanem azt is, hogy ezek pontosan lefednek minden TSFI-t.

ADV_FSP.4-4 Az értékelőnek meg kell vizsgálnia a funkcionális specifikációt a TSFI teljessége megállapítása érdekében.

Az értékelőnek a terv dokumentációt kell felhasználnia arra, hogy minden lehetséges interfész típust azonosítson. Az értékelő vizsgálja át a terv dokumentációt és az útmutató dokumentációt olyan lehetséges TSFI-k felkutatása céljából, amelyek nem fordulnak elő a fejlesztői dokumentációban, ami azt jelezné, hogy a fejlesztő által meghatározott TSFI nem teljes. Az értékelőnek meg kell vizsgálnia a fejlesztő által bemutatott indoklásokat arra, hogy a TSFI teljes, és ellenőriznie kell a terv legalacsonyabb szintjéig, vagy a megvalósítási reprezentáció felhasználásával, hogy további TSFI nem létezik.

ADV_FSP.4.3C A funkcionális specifikációnak azonosítania kell és le kell írnia minden TSFI-hez kapcsolódó összes paramétert.

ADV_FSP.4-5 Az értékelőnek meg kell vizsgálnia a TSFI bemutatását annak megállapítása érdekében, hogy az teljes mértékben azonosít-e minden TSFI-hez kacsolódó összes paramétert.

Az értékelő vizsgálja át a funkcionális specifikációt, hogy meggyőződjön arról, hogy minden egyes TSFI-hez kapcsolódó összes paramétert leírtak. A paraméterek olyan közvetlen bemenetei vagy kimenetei egy interfésznek, amelyek a szóbanforgó interfész működését irányítják. Például paraméterek az API-knak átadott argumentumok; a különféle mezők egy meghatározott hálózati protokoll csomagjaiban; a Windows Registry-ben lévő egyedi kulcs értékek; egy chip érintkezői közötti jelek; stb.

Annak megállapítása érdekében, hogy minden paraméter megvan-e a TSFI-ben, az értékelő vizsgálja át az interfész leírás további részeit is (tevékenységeket, hibaüzeneteket, stb.), hogy megállapítsa, vajon az interfész leírások figyelembe vették-e a paraméterek leírásait. Az értékelő ellenőrizze az értékeléshez átadott egyéb bizonyítékokat is (pl. TOE terv, biztonsági szerkezet leírás, üzemeltetési felhasználói dokumentáció, megvalósítási reprezentáció), hogy észrevegye, ha ezek leírnak egy olyan működést meghatározó vagy kiegészítő paramétert, amit a funkcionális specifikáció nem tartalmaz.

ADV_FSP.4-6 Az értékelőnek meg kell vizsgálnia a TSFI bemutatását annak megállapítása érdekében, hogy az teljesen és helyesen leír-e minden TSFI-hez kapcsolódó összes paramétert.

Az összes paraméter azonosítása után az értékelőnek meg kell győződnie arról, hogy ezeket helyesen és teljesen írták le. Egy paraméter leírása azt közli valamilyen érthető módon, hogy mi is a paraméter. Például a foo(i) interfész leírható úgy, hogy tartozik hozzá egy „i paraméter, ami egy egész”; ez azonban nem egy elfogadható paraméter leírás. Sokkal inkább elfogadható egy olyan leírás, hogy „az i paraméter egy egész szám, amely jelzi a rendszerbe jelenleg bejelentkezett felhasználók számát”.

Annak megállapítása érdekében, hogy minden paraméter leírása teljes, az értékelő vizsgálja át az interfész leírások további részeit is (rendeltetés, felhasználási mód, tevékenységek, hibaüzenetek, stb.), hogy megállapítsa, vajon az interfész leírások figyelembe vették-e a

paraméterek leírásait. Az értékelő ellenőrizze az értékeléshez átadott egyéb bizonyítékokat is (pl. TOE terv, biztonsági szerkezet leírás, üzemeltetési felhasználói dokumentáció, megvalósítási reprezentáció), hogy észrevegye, ha ezek leírnak egy olyan működést meghatározó vagy kiegészítő paramétert, amit a funkcionális specifikáció nem tartalmaz.

ADV_FSP.4.4C A funkcionális specifikációnak le kell írnia minden egyes TSFI-hez kapcsolódó összes tevékenységet.

ADV_FSP.4-7 Az értékelőnek meg kell vizsgálnia a TSFI bemutatását annak megállapítása érdekében, hogy az teljesen és helyesen leír-e minden egyes TSFI-hez kapcsolódó összes tevékenységet.

Az értékelő győződjön meg arról, hogy minden tevékenységet leírtak-e. Az interfészen elérhető tevékenységek azt írják le, amit az interfész tesz (ellentétben a TOE tervvel, amely azt írja le, hogy a TSF hogyan biztosítja a tevékenységeket).

Egy interfész tevékenységei leírják az interfészen keresztül aktivizálható funkcionalitást, és általános, illetve SFR-vonzatú tevékenységekként kategorizálhatók. Az általános tevékenységek annak a leírásai, hogy az interfész mit végez el. Az ehhez a leíráshoz megadott információ mennyisége az interfész bonyolultságától függ. Az SFR-vonzatú tevékenységek azok, amelyek bármely külső interfészen láthatók (például egy interfész aktivizálásával kiváltott naplózási tevékenység (feltéve, hogy az ST tartalmaz naplózási követelményeket) akkor is leírandó, ha az adott tevékenység eredménye általában nem látható az aktivizált interfészen). Az interfész paramétereitől függően több különböző tevékenység is kiváltható az interfészen. (Például egy API esetében lehetséges, hogy az első paraméter egy „alparancs”, és a rákövetkező paraméterek alparancs-specifikusak. Néhány Unix rendszerben az IOCTL API példa ilyen interfészre).

Annak megállapítása érdekében, hogy egy TSFI tevékenységnek teljes a leírása, az értékelő vizsgálja át az interfész leírások további részeit is (paraméter leírások, hibaüzenetek stb.), hogy megállapítsa, vajon az interfész leírások figyelembe vették-e a paraméterek leírásait. Az értékelő ellenőrizze az értékeléshez átadott egyéb bizonyítékokat is (pl. TOE terv, biztonsági szerkezet leírás, üzemeltetési felhasználói dokumentáció, megvalósítási reprezentáció), hogy észrevegye, ha ezek leírnak egy olyan működést meghatározó vagy kiegészítő paramétert, amit a funkcionális specifikáció nem tartalmaz.

ADV_FSP.4.5C A funkcionális specifikációnak le kell írnia minden közvetlen hibaüzenetet, melyet valamelyik TSFI meghívása eredményezhet.

ADV_FSP.4-8 Az értékelőnek meg kell vizsgálnia a TSFI bemutatását annak megállapítása érdekében, hogy az teljesen és helyesen leír-e minden hibaüzenetet, amelyet valamelyik TSFI aktivizálása eredményez.

A hibák sokféle formát ölthetnek, a leírandó interfésztől függően. Egy API esetében maga az interfész visszaadhat hibakódot; beállíthat egy globális hibafeltételt; vagy beállíthat egy hibakóddal kapcsolatos meghatározott paramétert. Egy konfigurációs fájl esetében egy helytelenül beállított paraméter kiválthat egy naplófájlban rögzítendő hibaüzenetet. Egy

hardver PCI kártya esetében egy hibafeltétel egy jelet válthat ki a buszon, vagy egy CPU-hoz kapcsolódó kivétel feltételt idézhet elő.

Hibák (és a kapcsolódó hibaüzenetek) egy interfész aktivizálásán keresztül következnek be. Az interfész aktivizálására adott válaszként jelentkező feldolgozás hiba körülményekkel találhatja szemben magát, ami egy hibaüzenet előállítását váltja ki (egy megvalósítás-specifikus mechanizmuson keresztül). Bizonyos esetekben ez lehet egy visszatérési érték magától az interfésztől; más esetekben lehetséges, hogy egy globális értéket állítanak be, és az interfész aktivizálása után ezt ellenőrzik. Valószínű, hogy a TOE számos olyan alacsony-szintű hibaüzenettel rendelkezik, amelyek alapvető erőforrás körülményekből erednek, mint például „a diszk megtelt", vagy „erőforrás lock-olva van". Bár az ilyen hibaüzenetek számos TSFI-hez hozzárendelhetők, felhasználhatók az olyan esetek felismerésére, amikor egy interfész leírás kimaradt. Például egy olyan TSFI, amely „a diszk megtelt" üzenetet állít elő, de amihez a tevékenységek ismertetésénél nem tartozik kézzelfogható leírás arról, hogy a TSFI miért idéz elő diszk hozzáférést, arra ösztönözheti az értékelőt, hogy a szóbanforgó TSFI-vel kapcsolatos egyéb bizonyítékokat is megvizsgálja (biztonsági szerkezet (ADV_ARC), TOE terv (ADV_TDS)), annak megállapítása érdekében, hogy a leírás teljes és helyes-e.

Az értékelő állapítsa meg, hogy minden interfész esetén meghatározható-e az adott interfész aktivizálására adott válaszként visszaadható hibaüzenetek pontos összessége. Az értékelő vizsgálja át az interfészhez átadott bizonyítékokat annak megállapítása érdekében, hogy a hibák összessége teljesnek tűnik-e. Kereszt-ellenőrzést is végezzen, összevetve ezt az információt az értékeléshez átadott egyéb dokumentumokkal (pl. TOE terv, biztonsági szerkezet leírás, üzemeltetési felhasználói dokumentáció, megvalósítási reprezentáció), hogy meggyőződjön arról, nem merülhetnek-e fel az említett eljárásból olyan hibák, amelyeket nem ír le a funkcionális specifikáció.

ADV_FSP.4-9 Az értékelőnek meg kell vizsgálnia a TSFI bemutatását annak megállapítása érdekében, hogy az teljesen és helyesen írja-e le minden egyes TSFI-hez a kapcsolódó összes hiba jelentését.

A helyesség megállapításának céljából az értékelőnek feltétlenül meg kell értenie a hiba jelentését. Például, ha egy interfész egy 0, 1, vagy 2 numerikus kódot ad vissza, az értékelő nem értheti meg a hibát, ha a funkcionális specifikáció csak annyit sorol fel: „a foo() interfész aktivizálásából származó lehetséges hibák 0, 1 vagy 2". Az értékelő ellenőrzéssel győződjön meg arról, hogy a hibák ehelyett például a következőképpen vannak leírva: „a foo() interfész aktivizálásából származó lehetséges hibák 0 (a feldolgozás sikeres), 1 (a fájl nem található) vagy 2 (nem megfelelő fájl specifikáció)"

Annak megállapítása érdekében, hogy a TSFI aktivizálása következtében fellépő hibák leírása teljes-e, az értékelő vizsgálja át az interfész leírások további részeit is (paraméter leírások, tevékenységek, stb.), hogy megállapítsa, vajon az interfész leírások figyelembe vették-e a paraméterek leírásait. Az értékelő ellenőrizze az értékeléshez átadott egyéb bizonyítékokat is (pl. TOE terv, biztonsági szerkezet leírás, üzemeltetési felhasználói dokumentáció, megvalósítási reprezentáció), hogy észrevegye, ha ezek leírnak egy olyan TSFI-hez kapcsolódó hiba feldolgozást, amit a funkcionális specifikáció nem tartalmaz.

ADV_FSP.4.6C A visszavezetésnek szemléltetnie kell az SFR-ek visszavezetését a funkcionális specifikáció TSFI-eire.

ADV_FSP.4-10 Az értékelőnek ellenőriznie kell, hogy a visszavezetés összekapcsolja-e az SFR-eket a megfelelő TSFI-kkel.

A visszavezetés a fejlesztőnek kell megadnia abból a célból, hogy útmutatóként szolgáljon ahhoz, hogy mely SFR-ek, mely TSFI-kkel állnak kapcsolatban. Ez a visszavezetés lehet olyan egyszerű, mint például egy táblázat; ez bemenetként szolgál az értékelő számára a következő munkaegységekben való felhasználáshoz, amelyekben az értékelő ellenőrzi ennek helyességét és teljességét.

6.2.5.1.2.2. Az ADV_FSP.4.2E értékelői akció

ADV_FSP.4.2E Az értékelőnek meg kell állapítania, hogy a funkcionális specifikáció az SFR-ek pontos és teljes megjelenítése-e.

ADV_FSP.4-11 Az értékelőnek meg kell vizsgálnia a funkcionális specifikációt annak megállapítása érdekében, hogy az az SFR-ek teljes megjelenítése-e.

Az értékelő építhet a fejlesztő visszavezetésére (lásd ADV_FSP.4-10), ami egy megfeleltetés a TOE biztonsági funkcionális követelmények és a TSFI között, hogy meggyőződjön arról, hogy a funkcionális specifikáció és a teszt lefedettség vizsgálat minden SFR-t lefed. Meg kell jegyezni, hogy a szóbanforgó megfeleltetés részletezettségi szintje lehet alacsonyabb, mint a követelmények összetevő-, sőt elem szintje, a funkcionális követelményeken végrehajtott műveletek miatt (értékadások, pontosítások és kiválasztások), amit az ST szerzője végez el.

Például az FDP_ACC.l komponens tartalmazhat egy értékadásokkal rendelkező elemet. Ha az ST például tíz szabályt tartalmaz az FDP_ACC.l értékadásban, és ezt a tíz szabályt esetleg három különböző TSFI fedi le, az értékelő számára nem lenne elegendő az FDP_ACC.l-hoz hozzárendelni a TSFI A, B és C-t, és kijelenteni, hogy ezzel teljesítetve van a munkaegység. Ehelyett az értékelő feltehetően hozzárendeli az FDP ACC.l (1-es szabály) –t a TSFI A-hoz; az FDP ACC.l (2-es szabály) –t a TSFI B-hez; stb. Lehetséges az az eset is, hogy az interfész egy gyűjtő interfész (pl. IOCTL), amikor a megfeleltetést az adott interfész bizonyos paraméterkészletére kell megadni.

Az értékelőnek fel kell ismernie, hogy az olyan követelményekre vonatkozóan, amelyek kevéssé vagy egyáltalán nem öltenek testet a TSF határán (pl. FDP_RIP), nincsen elvárva, hogy ezeket teljes mértékben megfeleltessék a TSFI-nek. A szóbanforgó követelmények vizsgálatát a TOE terv vizsgálatakor fogják elvégezni (ADV_TDS), ha ez benne van az ST-ben. Fontos megjegyezni azt is, hogy mivel a TSFI-hez kapcsolódó paramétereket, tevékenységeket és hibaüzeneteket teljes mértékben specifikálni kell, az értékelőnek képesnek kell lennie annak megállapítására, hogy egy SFR minden vonatkozásáról látszik-e, hogy azt interfész szinten valósították meg.

ADV_FSP.4-12 Az értékelőnek meg kell vizsgálnia a funkcionális specifikációt annak megállapítása érdekében, hogy az az SFR-ek helyes megjelenítése-e.

Az ST-ben lévő minden olyan funkcionális követelmény esetében, amely a TSF határán látható hatásokban nyilvánul meg, a követelményhez kapcsolódó TSFI-hez megadott információ specifikálja a követelmény által leírt megkívánt funkcionalitást. Ha például az ST hozzáférés ellenőrzési listákra vonatkozó követelményt tartalmaz, és ennek a követelménynek egyetlen olyan TSFI-t feleltettek meg, amely Unix-fajtájú védelmi bitekre specifikál funkcionalitást, akkor a funkcionális specifikáció az adott követelmény szempontjából helytelen.

Az értékelőnek tudnia kell, hogy az olyan követelményekre vonatkozóan, amelyek kevéssé vagy egyáltalán nem öltenek testet a TSF határán (pl. FDP_RIP), nem várják el, hogy teljes mértékben megfeleltessék a TSFI-nek. A szóbanforgó követelmények vizsgálatát a TOE terv vizsgálatakor fogják elvégezni (ADV_TDS), ha ez benne van az ST-ben.

6.2.5.1.3. TOE tervezés: Az ADV_TDS.3 altevékenység értékelése

Ennek az altevékenységnek a célja annak a megállapítása, hogy a TOE terv nyújt-e ismertetést a TOE-ről alrendszerek szerint, amely elegendő a TSF határainak megállapításához, és nyújt-e ismertetést a TSF belső részeiről modulok (és esetlegesen magasabb-szintű absztrakciók) szerint. Részletes ismertetést nyújt az SFR-t érvényre juttató modulokról, és elegendő információt nyújt az SFR-t támogató és az SFR-be nem beavatkozó modulokról az értékelő számára ahhoz, hogy meg tudja állapítani, hogy az SFR-eket teljesen és helyesen valósították meg; és ily módon, a TOE terv magyarázatot nyújt a megvalósítási reprezentációról.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) biztonsági szerkezet leírás,
d) TOE terv.

A TOE terv vonatkozásában az értékelőnek háromféle tevékenységre kell vállalkoznia. Először, az értékelő állapítsa meg, hogy a TSF határait megfelelő módon írták le. Másodszor, az értékelő állapítsa meg, hogy a fejlesztő olyan dokumentációt bocsátott rendelkezésre, amely megfelel a tartalomra és bemutatásra vonatkozó követelményeknek a szóbanforgó alrendszer esetében, és összhangban áll a TOE-hoz átadott egyéb dokumentációval is. Végül, az értékelőnek meg kell vizsgálnia a terv információt az SFR-t érvényre juttató modulokra vonatkozóan (részletes szinten), valamint az SFR-t támogató és az SFR-be nem beavatkozó modulokra vonatkozóan (kevésbé részletes szinten). Ennek célja, hogy megértse a rendszer megvalósítás módját, ennek segítségével pedig meggyőződjön arról, hogy a TSFI-t a funkcionális specifikáció megfelelően ismerteti és hogy a teszt információ megfelelő módon teszteli a TSF-et (az ATE: Tesztelés osztály munkaegységeiben elvégezve).

Fontos megjegyezni, hogy bár a fejlesztőnek egy teljes leírást kell biztosítania a TSF-ről (az SFR-t érvényre juttató modulokat nagyobb részletességgel, mint az SFR-t támogató vagy az SFR-be nem beavatkozó modulokat), az értékelőnek saját megítélését kell használnia a vizsgálatok elvégzésekor. Bár az értékelőnek minden modult át kell néznie, az egyes modulok vizsgálatának részletessége változhat. Az értékelő minden modult vizsgáljon meg abból a célból, hogy elegendő ismeretet szerezzen ahhoz, hogy meghatározza a modul

funkcionalitásának a kihatását a rendszer biztonságára. Az, hogy milyen mélységig szükséges vizsgálnia a modult, változhat a modul rendszerben betöltött szerepétől függően. Ennek a vizsgálatnak egy fontos vonatkozása, hogy az értékelő használja fel a többi dokumentációt (TOE összefoglaló előírás, funkcionális specifikáció és a biztonsági szerkezet leírása) annak megállapítása céljából, hogy az ismertetett funkcionalitás helyes, és hogy az SFR-t támogató vagy SFR-be nem beavatkozó modulok közvetett megjelölését (lásd alább) alátámasztja a rendszer szerkezetében betöltött szerepük.

A fejlesztő megjelölheti a modulokat SFR-t érvényre juttatóként, SFR-t támogatóként, és SFR-be nem beavatkozóként, bár ezek csak annak jelzésére szolgálnak, hogy a fejlesztőnek milyen mennyiségű és típusú információt kell szolgáltatnia, és a fejlesztő által kidolgozandó információ mennyiség korlátozására használható, ha az előkészítési munkálatok nem állítják elő a megkívánt dokumentációt. Akár kategorizálta a modulokat a fejlesztő, akár nem, az értékelő felelőssége annak megállapítása, hogy a modulok rendelkeznek-e megfelelő információval TOE-beli szerepüket illetően (SFR-t érvényre juttató, stb.), és a megfelelő információ megszerzése a fejlesztőtől, amennyiben a fejlesztő elmulasztotta biztosítani a megkívánt információt egy meghatározott modul esetében.

6.2.5.1.3.1. Az ADV_TDS.3.1E értékelői akció

ADV_TDS.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ADV_TDS.3.1C A tervnek le kell írnia a TOE szerkezetét alrendszerek szerint.

ADV_TDS.3-1 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy a teljes TOE szerkezetet leírták-e alrendszerek szerint.
Az értékelő győződjön meg arról, hogy a TOE minden alrendszerét azonosították. Ez a TOE leírás bemenetként szolgál az ADV_TDS.3-3 munkaegységhez, ahol a TOE TSF-et alkotó részeit azonosítják. Vagyis ez a követelmény a teljes TOE-ra vonatkozik, nem csak a TSF-re.

A TOE (és a TSF) leírható az absztrakció több szintjén (vagyis alrendszerek és modulok szintjén). A TOE bonyolultságától függően a terv leírható alrendszerek és modulok szerint. Egy nagyon egyszerű TOE esetében, amely kizárólag „modul” szinten is leírható (lásd ADV_TDS.3-2), ez a munkaegység nem értelmezhető, ennélfogva teljesítettnek tekintendő.

E tevékenység végrehajtásakor az értékelő vizsgáljon meg a TOE-hoz bemutatott egyéb bizonyítékot is (pl. ST, üzemeltetési felhasználói útmutató) annak megállapítása érdekében, hogy a TOE leírása ezekben a bizonyítékokban összhangban áll-e a TOE tervben leírtakkal.

ADV_TDS.3.2C A tervnek le kell írnia a TSF-et modulok szerint.

ADV_TDS.3-2 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy a teljes TSF-t leírták-e modulok szerint.

Az értékelő a modulokat a speciális tulajdonságok szempontjából más munkaegységekben fogja megvizsgálni; ebben a munkaegységben az értékelő azt állapítsa meg, hogy a moduláris

leírás lefedi-e a teljes TSF-et, és nem csak a TSF-nek egy részét. Az értékelő ehhez a megállapításhoz használja fel az értékeléshez átadott egyéb bizonyítékokat is (pl. funkcionális specifikáció, biztonsági szerkezet leírás). Például, ha a funkcionális specifikáció tartalmaz a funkcionalitáshoz csatlakozó olyan interfészt, amelyről úgy tűnik, hogy nincsen ismertetve a TOE tervben, akkor lehet, hogy ez egy olyan eset, amikor a TSF-nek egy része nincsen megfelelő módon csatolva. Az érintett megállapítás feltehetően iteratív eljárással hozható meg, amelynek során minél több vizsgálatot végeznek el a többi bizonyítékokon, annál nagyobb bizonyosság szerezhető a dokumentáció teljességét illetően.

Az alrendszerektől eltérően a modulok a megvalósítást olyan részletesen írják le, amely útmutatóként szolgálhat a megvalósítási reprezentáció áttekintésénél. Egy modul ismertetése olyan legyen, hogy a leírás alapján a modul megvalósítható úgy, hogy a keletkező megvalósítás 1) azonos lesz a tényleges TSF megvalósítással a modul által nyújtott és használt interfészek vonatkozásában, és 2) algoritmikusan azonos lesz a TSF modullal. Például az RFC 793 megadja a TCP protokoll magas szintű leírását. Ez szükségszerűen megvalósítás-független. Bár ez kellően részletes, mégsem megfelelő tervleírás, mivel nem specifikus egy megvalósításra. Az RFC-ben specifikált protokollhoz egy tényleges megvalósítás tehető hozzá és ennek választásai (például a megvalósítás különböző részeinél globális adatok használata lokális adatokkal szemben) befolyásolhatják a végrehajtandó vizsgálatot. A TCP modul tervleírása biztosan a megvalósítás interfészeit sorolja fel (nem pedig az RFC 793-ben meghatározottakat), és a TCP-t megvalósító modulokhoz kapcsolódó feldolgozás algoritmikus leírását is megadja (feltéve, hogy ez a TSF-nek a része).

ADV_TDS.3.3C A tervnek azonosítania kell a TSF minden alrendszerét.

ADV_TDS.3-3 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy az a TSF minden alrendszerét azonosítja-e.

Ha a tervet kizárólag modulok szerint mutatják be, akkor ebben a követelményben az alrendszerek azonosak a modulokkal, és a tevékenységet modul szinten kell végrehajtani.

Az ADV_TDS.3-1 munkaegységben a TOE valamennyi alrendszere legyen azonosítva, és állapítsák meg, hogy a nem-TSF alrendszereket helyesen jellemezték-e. Erre a munkára alapozva, pontosan azonosítani kell azokat az alrendszereket, melyeket nem jellemeztek nem-TSF alrendszerként. Az értékelő állapítsa meg az „Előkészítő eljárások” (AGD_PRE) útmutatónak megfelelően installált hardverről és szoftverről, hogy minden alrendszert figyelembe vettek, akár része a TSF-nek, akár nem.

ADV_TDS.3.4C A tervnek leírást kell biztosítania a TSF minden alrendszeréről.

ADV_TDS.3-4 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy a TSF minden alrendszerére leírja-e azt a szerepet, amelyet az ST-ben ismertetett SFR-ek érvényre juttatásában tölt be.

Ha a tervet kizárólag modulok szerint mutatják be, akkor feltételezetten ezt a munkaegységet a következő munkaegységek teljesítik; ebben az esetben az értékelő részéről semmilyen közvetlen akció nem szükséges.

Az olyan rendszerek esetében, amelyek elég összetettek ahhoz, hogy indokolt legyen a TSF-nek alrendszer-szintű leírása a moduláris leíráson túl, az alrendszer-szintű leírásnak az a célja, hogy megadja az értékelő számára követhető, moduláris leírásra vonatkozó összefüggéseket. Ezért az értékelő győződjön meg arról, hogy az alrendszer-szintű leírás tartalmaz-e ismertetést arról, hogy a biztonsági funkcionális követelmények hogyan valósulnak meg a tervben, de a moduláris leírásnál magasabb absztrakciós szinten. Ez a leírás a mechanizmusokat olyan szinten tárgyalja, amely összhangban áll a modul leírással; ez fogja nyújtani az értékelő számára a kapcsolatok feltérképezését, amely a modul leírásokban megadott információk értelmes felméréséhez szükséges. Az alrendszerek egy jól megírt halmaza útmutatást ad az értékelőnek annak megállapításához, hogy mely modulokat legfontosabb megvizsgálni, hogy így az értékelési tevékenység a TSF-nek azon részeire irányuljon, amelyek a legfontosabbak az SFR-ek érvényre juttatása szempontjából.

Az értékelő győződjön meg arról, hogy a TSF minden alrendszerét leírták. Bár a leírásnak arra a szerepre kell koncentrálnia, amelyet az alrendszer az SFR-ek megvalósításának érvényre juttatásában vagy támogatásában tölt be, ahhoz elegendő információt kell bemutatni, hogy az SFR-vonzatú funkcionalitás megértéséhez szükséges összefüggések biztosítva legyenek.

ADV_TDS.3.5C A tervnek leírást kell nyújtania a TSF összes alrendszere közötti kölcsönhatásokról.

ADV_TDS.3-5 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy a TSF alrendszerei közötti kölcsönhatásokat leírja-e.

Ha a tervet kizárólag modulok szerint mutatják be, akkor feltételezetten ezt a munkaegységet a következő munkaegységek teljesítik; ebben az esetben az értékelő részéről semmilyen közvetlen akció nem szükséges.

Az olyan rendszerek esetében, amelyek elég összetettek ahhoz, hogy indokolt legyen a TSF-nek egy alrendszer-szintű leírása a moduláris leíráson túl, az alrendszerek közötti kölcsönhatások leírásának az a célja, hogy segítse az olvasót annak jobb megértésében, hogy a TSF hogyan hajtja végre a funkcióit. Ezeket a kölcsönhatásokat nem szükséges megvalósítási szinten jellemezni (pl. egy alrendszer valamelyik rutinjából paramétereknek az átadása egy másik alrendszerhez tartozó rutin számára; globális változók; hardver jelzések (pl. megszakítások) az egyik hardver alrendszertől egy megszakítás-kezelő alrendszer felé), de ebben a fejtegetésben legyenek lefedve azok az adatelemek, amelyeket egy speciális alrendszerhez úgy határoztak meg, hogy ezeket egy másik alrendszerben való felhasználásra szántak. Az alrendszerek közötti minden felügyeleti kapcsolatot is ismertetni kell (pl. az egyik alrendszer felelős egy tűzfal rendszer szabályzat-bázisának konfigurálásáért és a másik alrendszer megvalósítja a szóbanforgó szabályokat).

Meg kell jegyezni, hogy bár a fejlesztőnek jellemeznie kell az alrendszerek közötti összes kölcsönhatást, az értékelőnek magának kell megítélnie a leírás teljességét. Ha egy kölcsönhatás oka nem világos, vagy ha vannak olyan SFR-vonzatú kölcsönhatások (például a modul-szintű dokumentáció vizsgálata közben felfedezve), amelyekről úgy tűnik, hogy nincsenek ismertetve, az értékelő gondoskodjon arról, hogy ezt az információt a fejlesztő átadja. Ha azonban az értékelő azt állapítja meg, hogy bizonyos alrendszerek közötti

kölcsönhatásokat ugyan nem ismertetett teljes mértékben a fejlesztő, de a teljes leírás nem járulna hozzá sem az általános funkcionalitás, sem a TSF által nyújtott biztonsági funkcionalitás megértéséhez, akkor az értékelő dönthet úgy, hogy a leírást elegendőnek tekinti, és nem kívánja meg a teljességet csak önmagáért.

ADV_TDS.3.6C A tervnek megfeleltetést kell nyújtania a TSF alrendszerei és a TSF moduljai között.

ADV_TDS.3-6 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy a TSF alrendszerei és a TSF moduljai közötti megfeleltetés teljes-e.
Ha a terv kizárólag modulok szerint van bemutatva, akkor ezt a munkaegységet teljesítettnek kell tekinteni.

Az olyan TOE-k esetében, amelyek elég összetettek ahhoz, hogy indokolt legyen a TSF alrendszer-szintű leírása a moduláris leíráson túl, a fejlesztő nyújtson egy egyszerű megfeleltetést, amely megmutatja, hogy a TSF moduljai hogyan lettek kiosztva az alrendszerek között. Ez útmutatóként fog szolgálni az értékelő számára a modul-szintű kiértékelésnél. A teljesség megállapítása érdekében az értékelő vizsgáljon át minden megfeleltetést, és állapítsa meg, hogy minden alrendszerhez hozzá van-e rendelve legalább egy modul, és hogy minden modul pontosan egy alrendszerhez van-e hozzárendelve.

ADV_TDS.3-7 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy a TSF alrendszerei és a TSF moduljai közötti megfeleltetés helyes-e.

Ha a tervet kizárólag modulok szerint mutatják be, akkor ezt a munkaegységet teljesítettnek kell tekinteni.

Az olyan TOE-k esetében, amelyek elég összetettek ahhoz, hogy indokolt legyen a TSF alrendszer-szintű leírása a moduláris leíráson túl, a fejlesztő nyújtson egy egyszerű megfeleltetést, amely megmutatja, hogy a TSF moduljai hogyan lettek kiosztva az alrendszerek között. Ez útmutatóként fog szolgálni az értékelő számára a modul-szintű kiértékelésnél. Az értékelő választhatja azt a megoldást is, hogy a megfeleltetés helyességét más munkaegységek végrehajtásával együtt ellenőrzi. „Nem-helyes” egy megfeleltetés, ha a modul tévesen van hozzárendelve egy alrendszerhez, ahol az alrendszeren belül nem használják a funkcióit. Minthogy a megfeleltetés azt a célt szolgálja, hogy útmutatásként szolgáljon a részletesebb vizsgálatok támogatására, az értékelőnek csak a megfelelő erőfeszítést ajánlott erre a munkaegységre fordítania. A megfeleltetés helyességét ellenőrző széleskörű értékelői erőforrások ráfordítása nem szükséges. Az itt vagy más munkaegységek során feltárt, félreértésre vezető pontatlanságokat kell ehhez a munkaegységhez rendelni és kijavíttatni.

ADV_TDS.3.7C A tervnek minden SFR-t érvényre juttató modult le kell írnia a céljának és a többi modullal való kölcsönhatásának a szempontjából.

ADV_TDS.3-8 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy minden SFR-t érvényre juttató modul céljának a leírása teljes és helyes-e.

A fejlesztő megjelölheti a modulokat SFR-t érvényre juttatóként, SFR-t támogatóként, és SFR-be nem beavatkozóként, bár ezek a „megjelölések” csak annak jelzésére szolgálnak, hogy a fejlesztőnek milyen mennyiségű és típusú információt kell szolgáltatnia, és felhasználható azon információ mennyiségének korlátozására, amelyet a fejlesztőnek kell kidolgoznia, ha az előkészítési munkálatok nem állítják elő a megkívánt dokumentációt. Akár kategorizálta a modulokat a fejlesztő, akár nem, az értékelő felelőssége annak megállapítása, hogy a modulok rendelkeznek-e megfelelő információval a TOE-beli szerepüket illetően (SFR-t érvényre juttató, stb.), és a megfelelő információ megszerzése a fejlesztőtől, ha a fejlesztő elmulasztotta biztosítani a megkívánt információt egy meghatározott modul esetében.

A modul célja azt mutatja meg, hogy a modul melyik funkciót elégíti ki. E munkaegység fő célja, hogy áttekintést nyújtson az értékelőnek a modul működésmódjáról, annak érdekében, hogy megállapításokat tehessen az SFR-ek megvalósításának megbízhatóságáról. Az ADV_ARC összetevő kapcsán végrehajtott szerkezeti vizsgálat támogatása is cél. Amennyiben az értékelő teljesen átlátja a modul működését és annak kapcsolatait az összes többi modullal, valamint a TOE-val, mint egésszel, az értékelő tekintse a munka célját teljesítettnek, és ne terhelje a fejlesztőt dokumentálási feladatokkal (megkövetelve, például, egy teljes algoritmust egy önmagában is nyilvánvaló megvalósítási reprezentációhoz).

ADV_TDS.3.8C A tervnek le kell írnia minden SFR-t érvényre juttató modult az SFR-vonzatú interfészei szerint, a visszatérési értékeket a szóbanforgó interfészekről, és a más modulokkal való kölcsönhatást, illetve az ilyenek általi meghívásokat.

ADV_TDS.3-9 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy minden SFR-t érvényre juttató modul tartalmaz-e helyes és teljes leírást az SFR-vonzatú paraméterekről, az interfészekre vonatkozó aktivizálási konvenciókról és az interfészektől közvetlenül visszatérő értékekről.

Egy modul SFR-vonzatú interfészei azok az interfészek, amelyeket más modulok használnak arra, hogy eszközként szolgáljanak a nyújtott SFR-vonzatú műveletek aktivizálásához, illetve arra, hogy bemenetet adjanak át, vagy kimenetet vegyenek át a modulnak/modultól. Az ilyen interfész specifikáció célja a tesztelés lehetővé tétele. A nem SFR-vonzatú modulok közötti interfészeket nem szükséges specifikálni vagy leírni, minthogy ezek nem kerülnek tesztelésre. Hasonlóan, az egyéb olyan belső interfészeket, amelyek nem keresztezik az SFR-vonzatú végrehajtási útvonalakat (mint amilyenek a rögzített belső útvonalak), nem szükséges specifikálni vagy leírni, minthogy ezek sem kerülnek tesztelésre.

Az SFR-vonzatú interfészek legyenek leírva abból a szempontból, hogy ezek hogyan aktivizálhatóak és hogy milyen értékeket adnak vissza. Ez az értékelés tartalmazzon egy felsorolást az SFR-vonzatú paraméterekről, és egy leírást ezekről. Meg kell jegyezni, hogy a globális adatokat szintén paramétereknek kell tekinteni, ha azokat a modul használja (akár bemenetként, akár kimenetként) az aktivizálás során. Ha egy paraméterről feltételezett, hogy értékek egy halmazát veheti csak fel (pl. egy „flag” paraméter), akkor legyen specifikálva azon értékek teljes halmaza, amelynek felvétele mellett a paraméter kihat a modul feldolgozására. Hasonlóan, legyenek leírva az adat struktúrákat reprezentáló paraméterek, az adat-struktúra minden mezőjének azonosításával és ismertetésével. Meg kell jegyezni, hogy a különböző programozási nyelvek rendelkezhetnek további nem-nyilvánvaló „interfészek”-kel;

példa lehet erre a C++-ban a művelet/függvény overloading. Ez az „implicit interfész” az osztály leírásnál szintén legyen ismertetve az alacsony szintű TOE terv részeként. Meg kell jegyezni, hogy egy modul bemutathat csak egy interfészt, sokkal gyakoribb azonban, ha a modul kapcsolódó interfészek egy kisebb halmazát mutatja be.

A modul (bemeneti vagy kimeneti) paramétereinek felmérése szempontjából a globális adatok bármilyen felhasználása szintén legyen figyelembe véve. A modul „felhasznál” globális adatot, ha az adatot olvassa, vagy írja. Abból a célból, hogy az értékelő állíthassa, hogy az ilyen paraméterek leírása teljes (ha használnak ilyeneket), használjon fel egyéb információkat is, amelyeket a TOE-ről adtak meg a TOE tervben (interfészek, algoritmikus leírások, stb.), és használja fel a globális adatok meghatározott halmazának a leírását, amelyet az ADV_TDS.3-9-ben mértek fel. Például az értékelő először megállapíthatja az eljárást, amit a modul végrehajt, a bemutatott funkciók és interfészek vizsgálatán keresztül (különös tekintettel az interfészek paramétereire). Ezek után ellenőrzést végezhet, hogy észrevegye, ha az eljárásról kitűnik, hogy „érint” valamilyen globális adatterületet, amelyet a TOE terv azonosított. Az értékelő ezek után állapítsa meg, hogy a szóbanforgó globális adatterületet „érintőnek” tűnő minden egyes globális adat fel van-e sorolva bemeneti vagy kimeneti eszközként a vizsgált modulhoz.

Az aktivizálási konvenciók programozási hivatkozás-típusú leírások, amelyeket egy modul interfész helyes aktivizálására lehet felhasználni, ha valaki olyan programot ír, amely kihasználja a modulnak az interfészen keresztül nyújtott funkcionalitását. Ez magában foglalja a szükséges bemeneteket és kimeneteket, beleértve minden beállítást, amelyet szükséges lehet végrehajtani a globális változókkal kapcsolatba.

Az interfész által visszaadott értékek olyan értékek, amelyeket paraméterek vagy üzenetek útján adnak tovább; vagy olyan értékek, amelyeket egy “C”-programbeli függvényhívás típusú funkcióhívás visszaad; vagy olyan értékek, amelyeket globális eszközökkel adnak tovább (mint például bizonyos hiba rutinok a *ix fajtájú operációs rendszereknél).

Abból a célból, hogy az értékelő állíthassa, hogy a leírás teljes, használjon fel a TOE tervben nyújtott egyéb információkat is, hogy meggyőződjön arról, hogy a modul funkcióinak végrehajtásához szükséges minden adatot bemutattak a modulnál, és hogy a modul által visszaadandó adatként minden olyan adatot azonosítottak, amelyet más modulok várnak el az értékelés adat álló modultól. Az értékelő állapítsa meg a helyességet azzal, hogy meggyőződik arról, hogy az eljárás leírása megfelel azoknak az információknak, amelyeket interfésznek átadandó vagy attól átveendő adatokként soroltak fel.

Mivel a modulok egészen alacsony szintűek, nehéz lehet megállapítani a teljesség és helyesség kihatásait a többi dokumentációból, mint például az üzemeltetési felhasználó dokumentáció, funkcionális specifikáció, vagy a biztonsági szerkezet leírása. Az értékelő mégis használja fel a szóbanforgó dokumentumokban megadott információkat olyan mértékben, amennyire ezek segítik azt a meggyőződést, hogy a cél helyesen és pontosan lett leírva. Ezt a vizsgálatot elősegítheti az ADV_TDS.3.10C elemhez kapcsolódó vizsgálat; a szóbanforgó elem a funkcionális specifikációban megadott TSFI-t megfelelteti a TSF moduljainak.

ADV_TDS.3.9C A tervnek le kell írnia minden SFR-t támogató vagy SFR-be nem beavatkozó modult a céljai és a többi modullal való kölcsönhatásai szempontjából.

ADV_TDS.3-10 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy az SFR-t támogató és az SFR-be nem beavatkozó modulok helyesen lettek-e kategorizálva.

Azokban az esetekben, amikor a fejlesztő eltérő mennyiségű információt nyújt a különböző modulokról, akkor ezzel egy közvetett kategorizálást végez. Vagyis (például) a kapcsolódó SFR-vonzatú interfészekkel részletesen bemutatott modulok (lásd ADV_TDS.3.10C) jelöltek az SFR-t érvényre juttató modulok közé sorolásra, bár az értékelő vizsgálatai vezethetnek arra a megállapításra is, hogy ezeknek bizonyos részhalmazai SFR-t támogatóak vagy SFR-be nem beavatkozók. Azok a modulok pedig (például), amelyekre csak a célokat és a többi modullal való kölcsönhatásokat írták le, „közvetve” SFR-t támogatóként vagy SFR-be nem beavatkozóként kategorizálták.

Ezekben az esetekben az értékelő arra összpontosítson, hogy minden egyes, közvetve SFR-t támogatónak vagy SFR-be nem beavatkozónak kategorizált modulról próbálja megállapítani az átadott információ és a többi modulra vonatkozó értékelési információ alapján (ami a TOE tervben, a funkcionális specifikációban, a biztonsági szerkezet leírásban és az üzemeltetési felhasználói dokumentációban található), hogy a modul valóban SFR-t támogató vagy SFR-be nem beavatkozó. A garanciának ezen a szintjén bizonyos hiba tolerálható; nem szükséges, hogy az értékelő abszolút biztos legyen abban, hogy egy adott modul SFR-t támogató vagy SFR-be nem beavatkozó-e, még akkor sem, ha ezek ilyennek vannak felcímkézve. Ha azonban a nyújtott bizonyíték azt jelzi, hogy egy SFR-t támogató vagy SFR-be nem beavatkozó modul (valójában) SFR-t érvényre juttató, az értékelő kérjen kiegészítő információkat a fejlesztőtől abból a célból, hogy feloldja a jelentkezett ellentmondást. Például tételezzük fel, hogy a Modul-A-ra (ami egy SFR-t érvényre juttató modul) vonatkozó dokumentáció azt jelzi, hogy ez meghívja a Modul-B-t, hogy hozzáférés ellenőrzést végezzen egy bizonyos típusú szerkezetre. Amikor az értékelő megvizsgálja a Modul-B-vel kapcsolatos információkat, azt találja, hogy erre a fejlesztő mindössze a célt és a kölcsönhatásokat adta át (ami így a Modul-B-t közvetve SFR-t támogató vagy SFR-be nem beavatkozó modulként kategorizálja). A Modul-A-hoz tartozó cél és kölcsönhatások vizsgálatakor azonban az értékelő nem talál semmilyen említést arról, hogy a Modul-B valamilyen hozzáférés ellenőrzést végezne, és a Modul-A-t nem sorolják a Modul-B-vel kölcsönhatásban álló modulok közé. Ezen a ponton az értékelő lépjen kapcsolatba a fejlesztővel, hogy feloldja a Modul-A-ra és a Modul-B-re megadott információk közötti ellentmondásokat.

Egy másik példában az értékelő megvizsgálja az ADV_TDS.3.2D által megadott TSFI – modulok megfeleltetést. Ez a vizsgálat kimutatja, hogy a Modul-C kapcsolatban áll egy SFR által megkövetelt felhasználói azonosítással. Amikor az értékelő megvizsgálja a Modul-C-hez kapcsolódó információkat, ismét csak azt találja, hogy a fejlesztő mindössze a célt és kölcsönhatások egy összességét adta át (ami így a Modul-C-t közvetve SFR-t támogató vagy SFR-be nem beavatkozó modulként kategorizálja). A Modul-C-re megadott cél és kölcsönhatások vizsgálatakor az értékelő nem képes megállapítani, hogy az egy felhasználói azonosítással foglalkozó TSFI-hez kapcsolódó modulként felsorolt Modul-C-t miért nem SFR-t érvényre juttatóként osztályozták. Az értékelő ekkor is lépjen kapcsolatba a fejlesztővel, hogy feloldja ezt az ellentmondást.

Egy utolsó példa az ellenkező nézőpontból a következő. Az előzőekkel megegyezően, a fejlesztő a Modul-D-vel kapcsolatban csak a célt és a kölcsönhatások egy összességét adja meg (ami így a Modul-D-t közvetve SFR-t támogató vagy SFR-be nem beavatkozó modulként kategorizálja). Az értékelő megvizsgálja az összes átadott bizonyítékot, beleértve a Modul-D-re vonatkozó célt és kölcsönhatásokat. Kitűnik, hogy a cél egy értelmezhető leírást ad a Modul-D TOE-beli funkciójáról, és a kölcsönhatások összhangban állnak a szóbanforgó leírással, és így semmi sem utal arra, hogy a Modul-D SFR-t érvényre juttató lenne. Ebben az esetben az értékelő „biztos ami biztos" alapon ne kérjen több információt a Modul-D-ről, hogy az helyesen lett kategorizálva. A fejlesztő teljesítette kötelezettségeit, és az a bizonyosság, amelyet az értékelő ebből merített a Modul-D implicit (definíció szerinti) kategorizálására vonatkozóan, megfelelő ezen a garanciaszinten.

ADV_TDS.3-11 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy az SFR-t támogató vagy SFR-be nem beavatkozó modulok cél leírása teljes és pontos-e.

Egy modul cél leírása azt jelzi, hogy a modul milyen szerepet tölt be. Az értékelőnek a leírásból egy általános képet kell kapnia a modul szerepéről. A leírás teljességének megállapíthatósága céljából az értékelő használjon fel egyéb információkat is, amelyeket a modulnak a többi modullal való kölcsönhatásairól megadtak, és mérje fel, hogy az az ok, ami miatt a modult meghívják, összhangban áll-e a modul céljával. Ha a kölcsönhatás leírása tartalmaz olyan funkcionalitást, amely nem látszik a modul céljából, vagy ellentétben áll azzal, az értékelőnek el kell döntenie, hogy ez a helyességnek vagy a pontosságnak a hiányossága-e. Az értékelő tekintse gyanakvóan azokat a célokat, amelyek túl rövidek, mivel sokatmondó vizsgálat feltehetően nem végezhető egy egymondatos cél alapján.

Ezekben az esetekben az értékelő arra összpontosítson, hogy minden egyes, közvetve SFR-t támogatónak vagy SFR-be nem beavatkozónak kategorizált modulról próbálja megállapítani az átadott információ és a többi modulra vonatkozó értékelési információ alapján (ami a TOE tervben, a funkcionális specifikációban, a biztonsági szerkezet leírásban és az üzemeltetési felhasználói dokumentációban található), hogy a modul valóban SFR-t támogató vagy SFR-be nem beavatkozó. A garanciának ezen a szintjén bizonyos hiba tolerálható; nem szükséges, hogy az értékelő abszolút biztos legyen abban, hogy egy adott modul SFR-t támogató vagy SFR-be nem beavatkozó-e, még akkor sem, ha ezek ilyennek vannak felcímkézve. Ha azonban a nyújtott bizonyíték azt jelzi, hogy egy SFR-t támogató vagy SFR-be nem beavatkozó modul (valójában) SFR-t érvényre juttató, az értékelő kérjen kiegészítő információkat a fejlesztőtől abból a célból, hogy feloldja a jelentkezett ellentmondást. Például tételezzük fel, hogy a Modul-A-ra (ami egy SFR-t érvényre juttató modul) vonatkozó dokumentáció azt jelzi, hogy ez meghívja a Modul-B-t, hogy hozzáférés ellenőrzést végezzen egy bizonyos típusú szerkezetre. Amikor az értékelő megvizsgálja a Modul-B-vel kapcsolatos információkat, azt találja, hogy erre a fejlesztő mindössze a célt és a kölcsönhatásokat adta át (ami így a Modul-B-t közvetve SFR-t támogató vagy SFR-be nem beavatkozó modulként kategorizálja). A Modul-A-hoz tartozó cél és kölcsönhatások vizsgálatakor azonban az értékelő nem talál semmilyen említést arról, hogy a Modul-B valamilyen hozzáférés ellenőrzést végezne, és a Modul-A-t nem sorolják a Modul-B-vel kölcsönhatásban álló modulok közé. Ezen a ponton az értékelő lépjen kapcsolatba a fejlesztővel, hogy feloldja a Modul-A-ra és a Modul-B-re megadott információk közötti ellentmondásokat.

ADV_TDS.3-12 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy az SFR-t támogató és az SFR-be nem beavatkozó modulok kölcsönhatását az egyéb modulokkal helyesen és pontosan írták-e le.

Fontos megjegyezni, hogy a 3. rész követelményeinek és ennek a munkaegységnek a szempontjából a kölcsönhatás kifejezés kevesebb szigorúságot hordoz, mint az interfész. Egy kölcsönhatást nem szükséges megvalósítási szinten jellemezni (pl. egy modul valamelyik rutinjából paramétereknek az átadása egy másik modulhoz tartozó rutin számára; globális változók; hardver jelzések (pl. megszakítások) az egyik hardver alrendszertől egy megszakítás-kezelő alrendszer felé), de ebben a fejtegetésben legyenek lefedve azok az adatelemek, amelyeket egy speciális modulhoz úgy határoztak meg, hogy ezeket egy másik modulban való felhasználásra szántak. A modulok közötti minden felügyeleti kapcsolatot is ismertetni kell (pl. az egyik modul felelős egy tűzfal rendszer szabályzat-bázisának konfigurálásáért és a másik modul megvalósítja a szóbanforgó szabályokat).

Mivel a modulok egészen alacsony szintűek, nehéz lehet megállapítani a teljesség és helyesség kihatásait a többi dokumentációból, mint például az üzemeltetési felhasználó dokumentáció, funkcionális specifikáció, vagy a biztonsági szerkezet leírása. Az értékelő mégis használja fel a szóbanforgó dokumentumokban megadott információkat olyan mértékben, amennyire ezek segítik azt a meggyőződést, hogy a célt helyesen és pontosan írták le. Ezt a vizsgálatot elősegítheti az ADV_TDS.3.10C elemhez kapcsolódó vizsgálat; a szóbanforgó elem a funkcionális specifikációban megadott TSFI-t megfelelteti a TSF moduljainak.

Egy modul kölcsönhatása a többi modullal túlnyúlik egy csak meghívási-fa típusú dokumentumon. A kölcsönhatás olyan funkcionális nézőpontból legyen leírva, hogy a modul miért lép kölcsönhatásba a többi modullal. A modul célja ismertesse, hogy a modul milyen funkciókat nyújt a többi modulnak; a kölcsönhatások ismertessék, hogy a modul funkciójának teljesítése érdekében hogyan függ a többi modultól.

Mivel a modulok egészen alacsony szintűek, nehéz lehet megállapítani a teljesség és helyesség kihatásait a többi dokumentációból, mint például az üzemeltetési felhasználó dokumentáció, funkcionális specifikáció, vagy a biztonsági szerkezet leírása. Az értékelő mégis használja fel a szóbanforgó dokumentumokban megadott információkat olyan mértékben, amennyire ezek segítik azt a meggyőződést, hogy a kölcsönhatásokat helyesen és pontosan írták le.

ADV_TDS.3.10C A megfeleltetésnek szemléltetnie kell, hogy a TOE tervben ismertetett minden működésmódot megfeleltették az ezt aktivizáló TSFI-nek.

ADV_TDS.3-13 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy az tartalmaz-e teljes és helyes megfeleltetést a funkcionális specifikációban leírt TSFI és a TOE tervben leírt TSF modulok között.

A TOE tervben leírt modulok ismertetik a TSF megvalósítását. A TSFI azt ismerteti hogy a megvalósítás hogyan használható. A fejlesztőtől származó bizonyíték azonosítja azt a modult, ami először aktivizálódik, mikor műveletet kérnek a TSFI-től, valamint azonosítja az

aktivizált modul-láncot, egészen a funkcionalitás megvalósításáért elsődlegesen felelős modulig bezárólag. A teljes hívási fa nem szükséges minden egyes TSFI-hez ennél a munkaegységnél. Több modult kell azonosítani azokban az esetekben, amikor olyan „belépési pont" modulok vagy gyűjtő modulok léteznek, amelyeknek nincsen funkcionalitásuk azon kívül, hogy a bemenetekre feltételeket ellenőriznek vagy elvégzik a bemeneti csatorna leválasztását. Egy olyan megfeleltetés, amely a szóbanforgó moduloknak csak az egyikére vonatkozik, nem nyújt hasznos információt az értékelő számára.

Az értékelő mérje fel a megfeleltetés teljességét meggyőződve arról, hogy minden TSFI-hez legalább egy modult hozzárendeltek. A helyesség ellenőrzése bonyolultabb.

Mivel a modulok egészen alacsony szintűek, nehéz lehet megállapítani a teljesség és helyesség kihatásait a többi dokumentációból, mint például az üzemeltetési felhasználó dokumentáció, funkcionális specifikáció, vagy a biztonsági szerkezet leírása. Az értékelő mégis használja fel a szóbanforgó dokumentumokban megadott információkat olyan mértékben, amennyire ezek segítik azt a meggyőződést, hogy a kölcsönhatások helyesen és pontosan írták le.

6.2.5.1.3.2. Az ADV_TDS.3.2E értékelői akció

ADV_TDS.3.2E Az értékelőnek meg kell erősítenie, hogy a terv az összes funkcionális biztonsági követelmény (SFR) pontos és teljes megjelenítése.

ADV_TDS.3-14 Az értékelőnek meg kell vizsgálnia a TOE biztonsági funkcionális követelményeket és a TOE tervet annak megállapítása érdekében, hogy a TOE terv az ST minden funkcionális biztonsági követelményét (SFR) lefedi-e.

Az értékelő összeállíthat egy megfeleltetést a TOE funkcionális biztonsági követelményei és a TOE terv között. Ez a megfeleltetés feltehetően egy SFR-től az alrendszerek, majd később a modulok egy halmazáig fog vezetni. Meg kell jegyezni, hogy a szóbanforgó megfeleltetés részletezettségi szintje lehet alacsonyabb, mint a követelmények összetevő-, sőt elem szintje, az ST szerzője által az SFR-eken végrehajtott műveletek (értékadások, pontosítások és kiválasztások) miatt.

Például a „Részleges hozzáférés ellenőrzés" (FDP_ACC.l) összetevő tartalmazhat egy értékadásokkal rendelkező elemet. Ha az ST például tíz szabályt tartalmaz a „Részleges hozzáférés ellenőrzés" (FDP_ACC.l) értékadásában, és ezt a tíz szabályt tizenöt modulon belüli megadott helyeken valósították meg, nem lenne elegendő, ha az értékelő a „Részleges hozzáférés ellenőrzés"-t (FDP_ACC.l) egy alrendszerhez rendelné hozzá, majd kijelentené, hogy a munkaegység teljesítve lett. Ehelyett, az értékelő rendelje hozzá a „Részleges hozzáférés ellenőrzés" (FDP_ACC.l) (1-es szabály)-t az A alrendszer x, y, és z moduljaihoz, a „Részleges hozzáférés ellenőrzés" (FDP_ACC.l) (2-es szabály)-t az A alrendszer x, p, és q moduljaihoz, és így tovább.

ADV_TDS.3-15 Az értékelőnek meg kell vizsgálnia a TOE tervet annak megállapítása érdekében, hogy az minden funkcionális biztonsági követelményt helyesen jelenít-e meg.
Az értékelő összeállíthat egy megfeleltetést a TOE funkcionális biztonsági követelményei és a TOE terv között. Ez a megfeleltetés feltehetően egy SFR-től az alrendszerek és a modulok

egy halmazáig fog vezetni. Meg kell jegyezni, hogy a szóbanforgó megfeleltetés részletezettségi szintje lehet alacsonyabb, mint a követelmények összetevő-, sőt elem szintje, az ST szerzője által az SFR-eken végrehajtott műveletek (értékadások, pontosítások és kiválasztások) miatt.

Példaként, ha az ST követelmények szerepkör-alapú hozzáférés ellenőrzési mechanizmust specifikálnak, az értékelő először azonosítsa azokat az alrendszereket, majd modulokat, amelyek hozzájárulnak ennek a mechanizmusnak a megvalósításához. Ez megtehető a TOE terv mélyreható ismerete vagy megértése alapján, vagy a megelőző munkaegységben elvégzett munkán keresztül. Meg kell jegyezni, hogy ennek a nyomkövetésnek csak az a célja, hogy azonosítsa az alrendszereket és modulokat, nem pedig a teljes vizsgálat.

A következő lépés annak megértése, hogy az alrendszerek és a modulok milyen mechanizmusokat valósítanak meg. Például, ha a terv egy olyan hozzáférés ellenőrzési megvalósítást ír le, amely UNIX-típusú védelmi biteken alapul, a terv nem pontos megvalósulása azoknak a hozzáférés ellenőrzési követelményeknek, amelyeket a fenti ST példa mutat be. Ha az értékelő a részletek hiánya miatt nem tudja megállapítani, hogy pontosan milyen mechanizmusokat valósítottak meg, becsülje fel, hogy minden SFR-t érvényre juttató alrendszert és modult azonosítottak-e, vagy hogy a szóbanforgó alrendszerekről és modulokról elegendő részleteket nyújtottak-e.

6.2.5.1.4. Megvalósítási reprezentáció: Az ADV_IMP.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztőnek átadott megvalósítási reprezentáció alkalmas-e arra, hogy ezt az egyéb vizsgálati tevékenységeknél felhasználják; az alkalmasság annak alapján bírálható el, hogy megfelel-e ezen komponens követelményeinek.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) a megvalósítási reprezentáció,
b) az ALC_TAT-ból származó fejlesztő eszközök dokumentációja,
c) TOE terv.

A teljes megvalósítási reprezentáció elérhetősége szükséges annak biztosítására, hogy a vizsgálati tevékenységek nem csorbulnak információ hiány következtében. Ez azonban nem vonja maga után azt, hogy a teljes reprezentációt át kell vizsgálni az értékelés során. Ez feltehetően majdnem mindig kivihetetlen, ráadásul minden valószínűség szerint nem eredményezne nagyobb garanciájú TOE-t a megvalósítási reprezentáció célirányos mintavételezésével szemben. Ezen altevékenység esetében ez még inkább igaz. Nem lenne eredményes az értékelő számára, ha sok időt fordítana a megvalósítási reprezentáció egyik részére vonatkozó követelmények ellenőrzésére, és ezt követően a megvalósítási reprezentációnak egy másik részét használná fel a többi munkaegységre vonatkozó vizsgálatok végrehajtásánál. Az értékelő válasszon ki egy mintát a megvalósítási reprezentációból, a TOE olyan területeiről, amelyek a leginkább érdekesek lehetnek az egyéb családokhoz tartozó munkaegységek (pl. ATE_IND, AVA_VAN és ADV_INT) során végrehajtott vizsgálatoknál.

6.2.5.1.4.1. Az ADV_IMP.1.1E értékelői akció

ADV_IMP.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ADV_IMP.1.1C A megvalósítási reprezentációnak a TSF-et olyan részletezettségi szinten kell meghatároznia, hogy a TSF-et elő lehessen állítani további tervezési döntések nélkül.

ADV_IMP.1-1 Az értékelőnek ellenőriznie kell, hogy a megvalósítási reprezentáció a TSF-et olyan részletezettségi szinten határozza-e meg, amelynek alapján a TSF-et további tervezési döntések nélkül elő lehet állítani.

A szoftver forráskód, a förmver forráskód, a tényleges hardver felépítéséhez használt hardver diagram és/vagy hardver-tervezési nyelven írott kód vagy tervrajz adat, példák egy megvalósítási reprezentáció részeire. Az értékelő vegyen mintát a megvalósítási reprezentációból, hogy meggyőződjön arról, hogy az megfelelő szintű, és például nem pszeudo-kód szintű, ami további tervezési döntéseket tenne szükségessé. Javasolt, hogy az értékelő egy gyors ellenőrzést végezzen a megvalósítási reprezentáció első megtekintésekor, s ezzel megbizonyosodjon arról, hogy a fejlesztő jó úton jár. Az is javasolt, hogy az értékelő a vizsgálat nagy részét akkor hajtsa végre, amikor más olyan munkaegységeken dolgozik, amelyek megkívánják a megvalósítás vizsgálatát; ez biztosítja a munkaegység során vizsgált minta megfelelőségét.

ADV_IMP.1.2C A megvalósítási reprezentációnak olyan formájúnak kell lennie, mint ahogyan azt a fejlesztői személyzet használja.

ADV_IMP.1-2 Az értékelőnek ellenőriznie kell, hogy a megvalósítási reprezentáció olyan formájú, mint ahogyan azt a fejlesztői személyzet használja.

A megvalósítási reprezentációt a fejlesztőnek olyan formára kell alakítania, amely alkalmas arra, hogy a tényleges megvalósításra áttranszformálják. Például a fejlesztő dolgozhat forráskódokat tartalmazó fájlokkal, amelyeket végül lefordítanak, hogy a TSF részeivé váljanak. A fejlesztőnek a megvalósítási reprezentációt olyan formában kell rendelkezésre bocsátania, ahogyan azt a fejlesztő használja, hogy az értékelő automatizált technikákat tudjon használni a vizsgálatoknál. Ez szintén megnöveli a bizonyosságot abban, hogy a vizsgált megvalósítási reprezentáció tényleg az, mint amit a TSF előállítására használnak (szemben azzal az esettel, amikor a reprezentáció egy változó bemutatási formátumban van megadva, mint amilyen például egy szövegszerkesztővel előállított dokumentum). Meg kell jegyezni, hogy a megvalósítási reprezentáció más formáit is használhatja a fejlesztő; ezeket a formákat ugyancsak rendelkezésre kell bocsátani. Az általános cél az, hogy az értékelő számára szolgáltatni kell azokat az információkat, amelyek fokozzák az értékelő vizsgálati törekvéseinek a hatékonyságát.

Az értékelő vegyen mintát a megvalósítási reprezentációból, hogy megbizonyosodjon arról, hogy valóban olyan verzióról van-e szó, amelyet a fejlesztő használhat. A minta legyen olyan, hogy az értékelő biztosítékot nyerjen arról, hogy a megvalósítási reprezentáció minden

területe összhangban áll a követelményekkel; a teljes megvalósítási reprezentáció vizsgálata azonban szükségtelen.

A megvalósítási reprezentáció bizonyos formáiban alkalmazott konvenciók nehézzé vagy lehetetlenné tehetik, hogy csak magából a megvalósítási reprezentációból meg lehessen határozni, hogy mi lesz a tényleges eredménye a fordításnak vagy futás-idejű parancs-értelmezésnek. Például a C nyelvű fordítóprogramoknak szóló szerkesztési direktívák azt fogják eredményezni, hogy a fordítóprogram teljes kód-részeket kihagy vagy hozzácsatol.

A megvalósítási reprezentáció bizonyos formái kiegészítő információkat tehetnek szükségessé, mert jelentősen megnehezítik a megértést és a vizsgálatokat. Példa erre a „leplezett” vagy más módon elhomályosított forráskód, amely gátolja a megértést és/vagy a vizsgálatokat. A megvalósítási reprezentációnak ezek a formái általában úgy keletkeznek, hogy a TOE fejlesztője a megvalósítási reprezentáció egy verziójára ráereszt egy leplező vagy elhomályosító programot. Bár a leplezett reprezentáció az, amit lefordítottak, és lehet, hogy ez közelebb áll a megvalósításhoz (a szerkezet szempontjából), mint az eredeti, nem-leplezett reprezentáció, egy ilyen homályossá tett kódnak a rendelkezésre bocsátása azt eredményezheti, hogy jelentősen több időt kell fordítani a reprezentációt érintő vizsgálati feladatokra. Ilyen formájú reprezentáció kialakítása esetén az összetevők megkövetelik a használt leplező eszközökre/algoritmusokra vonatkozó részleteket, hogy vissza lehessen állítani a nem-leplezett reprezentációt, és a kiegészítő információk felhasználásával megbizonyosodjanak arról, hogy a leplező eljárás nem ront le egyetlen biztonsági funkcionalitást sem.

Az értékelő vegyen mintát a megvalósítási reprezentációból, hogy megbizonyosodhasson arról, hogy a megvalósítási reprezentáció értelmezéséhez szükséges minden információt biztosítottak. Meg kell jegyezni, hogy az eszközök azok közé az eszközök közé tartoznak, amelyekre az „Eszközök és technikák” (ALC_TAT) összetevői hivatkoznak. Javasolt, hogy az értékelő egy gyors ellenőrzést végezzen a megvalósítási reprezentáció első megtekintésekor, s ezzel megbizonyosodjon arról, hogy a fejlesztő jó úton jár. Az is javasolt, hogy az értékelő a vizsgálat nagy részét akkor hajtsa végre, amikor más olyan munkaegységeken dolgozik, amelyek megkívánják a megvalósítás vizsgálatát; ez biztosítja a munkaegység során vizsgált minta megfelelőségét.

ADV_IMP.1.3C A TOE terv és a megvalósítási reprezentáció mintája közötti megfeleltetésnek szemléltetnie kell ezek összetartozását.

ADV_IMP.1-3 Az értékelőnek meg kell vizsgálnia a TOE terv és a megvalósítási reprezentáció mintája közötti megfeleltetést annak megállapítása érdekében, hogy az helyes.

Az értékelő (az ADV_IMP.1-1 munkaegységben meghatározott) megállapítását erősítse tovább azzal, hogy ellenőrzi a megvalósítási reprezentáció egyik része és a TOE terv helyességét. A TOE terv érdeklődést kiváltó részeire az értékelő ellenőrizze, hogy a megvalósítási reprezentáció helyesen tükrözi-e a TOE tervben megadott ismertetést.

Például a TOE terv azonosíthat egy login modult, amely felhasználók azonosítására és hitelesítésére szolgál. Ha a felhasználó-hitelesítés elég fontos, az értékelő ellenőrizze, hogy a megfelelő kód valóban megvalósítja az adott szolgáltatást a TOE tervben ismertetett módon.

Érdemes lehet azt is ellenőrizni, hogy a kód a funkcionális specifikációban leírtaknak megfelelően fogadja-e be a paramétereket.

Fel kell hívni a figyelmet arra, hogy a fejlesztőnek választania kell abban, hogy vagy a teljes megvalósítási reprezentációra elvégzi a megfeleltetést, és ezzel biztosítja, hogy a kiválasztott mintát biztosan lefedi, vagy pedig megvárja a minta kiválasztását a megfeleltetés elvégzése előtt. Az első lehetőség feltehetően több munkával jár, de befejezhető az értékelés megkezdése előtt. A második lehetőség kevesebb munkával jár, de az értékelési tevékenység késleltetését okozza, amíg a szükséges bizonyítékokat elő nem állítják.

6.2.5.2. Az Útmutató dokumentumok garanciaosztály (AGD) értékelése

Az útmutató dokumentumokhoz kapcsolódó tevékenységnek az a célja, hogy elbírálják annak a dokumentációnak a megfelelőségét, amely ismerteti, hogy a felhasználó hogyan tudja a TOE-t biztonságos módon kezelni. Az ilyenfajta dokumentációnak figyelembe kell vennie a különféle felhasználó típusokat (például azokat, akik befogadják, telepítik, adminisztrálják vagy üzemeltetik a TOE-t), akiknek a helytelen akciói hátrányosan befolyásolhatják a TOE-nak vagy a saját adataiknak a biztonságát.

Az útmutató dokumentumok osztály két családra van osztva, amelyek elsősorban az előkészítő felhasználói dokumentációval foglalkoznak (ami mindazt tartalmazza, amit meg kell tenni annak érdekében, hogy a leszállított TOE-t átalakítsák a környezet értékelt konfigurációjához, ahogyan az az ST-ben le van írva, vagyis ahogyan a TOE-t befogadják és telepítik), másodsorban pedig az üzemeltetői felhasználói dokumentációval (ami mindazt tartalmazza, amit meg kell tenni a TOE üzemeltetése során az értékelt konfigurációban, vagyis az üzemeltetést és adminisztrációt).

Az útmutató dokumentumokhoz kapcsolódó tevékenység azokra a funkciókra és csatlakozási felületekre vonatkozik, amelyek a TOE biztonságához kapcsolódnak. A TOE biztonságos konfigurálása az ST-ben van leírva.

6.2.5.2.1. Üzemeltetési felhasználói útmutató: Az AGD_OPE.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy az üzemeltetési felhasználói útmutató leírja-e minden felhasználói szerepkörre a TSF által nyújtott biztonsági funkcionalitást és interfészeket, tartalmazza-e a TOE biztonságos használatához szükséges utasításokat és útmutatást, lefedi-e az összes üzemeltetési mód biztonságos eljárásait, lehetővé teszi-e a TOE nem biztonságos állapotainak megelőzését és észlelését, egyúttal egyértelmű és megalapozott-e.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) a funkcionális specifikáció,
c) a TOE terv
d) az üzemeltetési felhasználói útmutató.

6.2.5.2.1.1. Az AGD_OPE.1.1E értékelői akció

AGD_OPE.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

AGD_OPE.1.1C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre le kell írnia azokat a felhasználó által elérhető funkciókat és jogosultságokat (beleértve a megfelelő figyelmeztetéseket is), melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

AGD_OPE.1-1 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót, annak megállapítása érdekében, hogy az leírja-e azokat a felhasználó által elérhető funkciókat és jogosultságokat (beleértve a megfelelő figyelmeztetéseket is), melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

A TOE konfigurálása lehetővé teheti, hogy a különböző felhasználói szerepkörök a TOE különböző funkcióihoz eltérő jogosultságokkal rendelkezzenek. Ezáltal egyes felhasználók számára engedélyezve lesznek olyan funkciók, melyek mások számára nem. Ezeket a funkciókat és jogosultságokat minden felhasználói szerepkörre le kell írni az üzemeltetési felhasználói útmutatóban.

Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre azonosítania kell az ellenőrzés alatt tartandó funkciókat és jogosultságokat, az ezek számára szükséges utasítás típusokat, valamint az utasítások okait. Az üzemeltetési felhasználói útmutatónak figyelmeztetéseket kell tartalmaznia az ellenőrzés alatt tartandó funkciókra és jogosultságokra vonatkozóan. A figyelmeztetéseknek a várt hatásokról, az esetleges mellékhatásokról és a más funkciókkal és jogosultságokkal kapcsolatos lehetséges kapcsolatokról kell szólniuk.

AGD_OPE.1.2C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre le kell írnia, hogy a TOE által biztosított, elérhető interfészeket hogyan kell biztonságos módon használni.

AGD_OPE.1-2 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e a TOE által biztosított, elérhető interfészek biztonságos használatát.

Az üzemeltetési felhasználói útmutatónak javaslatokat kell megfogalmaznia a TSF hatékony használatához (például jelszó kialakítási gyakorlat áttekintése, felhasználói állományok mentésének javasolt gyakorisága, felhasználói hozzáférési jogok megváltoztatása hatásának elemzése).

AGD_OPE.1.3C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre le kell írnia az elérhető funkciókat és interfészeket, különösen a felhasználó ellenőrzése alá tartozó minden biztonsági szempontból fontos paramétert, jelezve (ahol ez lehetséges) a biztonságos értékeket.

AGD_OPE.1-3 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e az elérhető funkciókat és interfészeket, különösen a felhasználó ellenőrzése alá tartozó minden biztonsági paramétert, jelezve (ahol ez lehetséges) a biztonságos értékeket is.

Az üzemeltetési felhasználói útmutatónak áttekintést kell adnia a felhasználói interfészeken keresztül látható biztonsági funkcionalitásról.

Az üzemeltetési felhasználói útmutatónak azonosítania kell, és le kell írnia a biztonsági funkciók és interfészek célját, működésüket, illetve egymás között kapcsolataikat.

Minden felhasználó által elérhető interfészre az üzemeltetési felhasználói útmutatónak:

a) le kell írnia azokat a módszereket, melyekkel az interfész hívható (pl. parancssor, programozási nyelvi rendszerhívások, menükiválasztás, parancsgombok);
b) le kell írnia a felhasználó által állítandó paramétereket, azok célját, érvényes és alapértelmezett értékeiket, a paraméterek biztonságos és nem biztonságos használatát okozó beállításokat, mindezt egyenként vagy paraméter-kombinációkban;
c) le kell írnia a közvetlen TSF válaszokat, üzeneteket vagy visszaadott kódot.

Az értékelőnek elsősorban a funkcionális specifikációt és az ST-t kell figyelembe vennie annak megállapítása érdekében, hogy az ezekben leírt TSF összhangban áll-e az üzemeltetési felhasználói útmutatóval. Az értékelőnek meg kell győződnie az üzemeltetési felhasználói útmutató teljességéről, vagyis arról, hogy az összes emberi felhasználó számára lehető teszi az elérhető TSFI-k biztonságos használatát. Az értékelő segítségként elkészítheti az útmutató és ezen dokumentumok közötti informális leképezést. Az ebben fellelhető bármilyen hiányosság az útmutató teljességének csorbulását jelezheti.

AGD_OPE.1.4C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre világosan be kell mutatnia a felhasználó által elérhető funkciókkal kapcsolatban végrehajtandó, biztonsági szempontból fontos minden esemény típust, beleértve a TSF ellenőrzése alá eső egyedek biztonsági tulajdonságainak megváltoztatását is.

AGD_OPE.1-4 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e a felhasználói funkciókkal kapcsolatban végrehajtandó, biztonsági szempontból lényeges minden esemény típust, beleértve a TSF ellenőrzése alá tartozó egyedek biztonsági tulajdonságainak megváltoztatását is.

Minden biztonsági szempontból fontos esemény típust részletezni kell minden felhasználói szerepkörre, hogy minden felhasználó tudja, milyen események fordulhatnak elő, és mit kell tennie (ha szükséges) a biztonság fenntartása érdekében. A TOE üzemeltetése során előforduló biztonsági szempontból lényeges eseményeket (például naplótár túlcsordulás; rendszerösszeomlás; felhasználói rekordok felülírása, mint amikor egy felhasználó távozik a szervezettől, és a fiókját eltörlik) kellően meg kell határozni, hogy a felhasználó beavatkozhasson a biztonságos működés fenntartása érdekében.

AGD_OPE.1.5C Az üzemeltetési felhasználói útmutatónak azonosítani kell a TOE összes lehetséges üzemeltetési módját (beleértve a meghibásodás vagy üzemeltetési hiba utáni műveleteket is), valamint ezek biztonságos üzemeltetésre gyakorolt következményeit és kihatásait.

AGD_OPE.1-5 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót és az egyéb értékeléshez adott bizonyítékot annak megállapítása érdekében, hogy az útmutató azonosítja-e a TOE összes lehetséges üzemmódját (beleértve a meghibásodás vagy üzemeltetési hiba utáni működést is, amennyiben ilyen előfordulhat), valamint ezek következményét és kihatásait a biztonságos üzemelés fenntartására.

Más értékelési bizonyítékot, elsősorban a funkcionális specifikációt az értékelőnek annak megállapításához javasolt használnia, hogy az útmutató megfelelő eligazító leírást tartalmaz-e.

Amennyiben a garanciacsomaghoz tesztdokumentáció van csatolva, akkor az ebben a bizonyítékban nyújtott információ is felhasználható annak eldöntésére, hogy az útmutató elegendő útmutató információt tartalmaz-e. A tesztlépéseknél megadott részletek felhasználhatók annak megerősítésére, hogy a nyújtott útmutató elégséges a TOE használatához és adminisztrálásához.

Az értékelőnek egy időben egy ember számára látható TSFI-t ajánlott vizsgálnia, úgy, hogy összehasonlítja a TSFI biztonságos használatáról szóló útmutatást egyéb bizonyítékokkal, annak kiderítése érdekében, hogy a TSFI-vel kapcsolatos információk valóban jól írják-e le annak biztonságos használatát (azaz megfelelnek-e az SFR-eknek). Az értékelőnek az interfészek közötti kapcsolatokat is át kell néznie, potenciális ellentmondásokat keresve.

AGD_OPE.1.6C Az üzemeltetési felhasználói útmutatónak minden felhasználói szerepkörre le kell írnia azokat a betartandó biztonsági intézkedéseket, melyek az ST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célok elérését szolgálják.

AGD_OPE.1-6 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e azokat a betartandó biztonsági intézkedéseket, melyek az ST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célok elérését szolgálják.

Az értékelő elemezze az ST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célokat, majd állapítsa meg, hogy az üzemeltetési felhasználói útmutató minden felhasználói szerepkörre megfelelően leírja-e a fontos biztonsági intézkedéseket.

Az üzemeltetési felhasználói útmutatóban leírt biztonsági intézkedéseknek magukban kell foglalniuk az összes fontos külső eljárásrendi, fizikai, személyzeti és kapcsolódásra vonatkozó intézkedést.

Megjegyzendő, hogy a TOE biztonságos telepítésére vonatkozó intézkedéseket az Előkészítő eljárások (AGD_PRE) vizsgálja.

AGD_OPE.1.7C Az üzemeltetési felhasználói útmutatónak egyértelműnek és megalapozottnak kell lennie.

AGD_OPE.1-7 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az egyértelmű-e.

Az útmutató akkor nem egyértelmű (félrevezető), ha ez alapján egy egy felhasználó indokoltan félreértheti teendőit, és a TOE-ra vagy a TOE által nyújtott biztonságra nézve hátrányos módon alkalmazza a leírtakat.

AGD_OPE.1-8 Az értékelőnek meg kell vizsgálnia az üzemeltetési felhasználói útmutatót annak megállapítása érdekében, hogy az megalapozott-e.

Az útmutató akkor tekinthető megalapozatlannak, ha olyan követelményeket támaszt a TOE használatával vagy üzemeltetési környezetével szemben, melyek nem felelnek meg az ST-nek, vagy indokolatlanul nagy terhet jelentenek a biztonság fenntartásához.

6.2.5.2.2. Előkészítő eljárások: Az AGD_PRE.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a TOE biztonságos előkészületi eljárásait és lépéseit dokumentálták, s hogy ezek biztonságos konfigurációt eredményeznek.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) a TOE, beleértve az előkészítő eljárásait,
c) a fejlesztő szállítási eljárásainak leírása.

Az előkészületi eljárások az összes olyan elfogadási és telepítési eljárást jelentik, melyek ahhoz szükségesek, hogy a TOE-t az ST-ben leírt biztonságos konfiguráció állapotába juttassák.

6.2.5.2.2.1. Az AGD_PRE.1.1E értékelői akció

AGD_PRE.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

AGD_PRE.1.1C Az előkészítő eljárásoknak le kell írniuk a leszállított TOE biztonságos elfogadásához szükséges valamennyi lépést, a fejlesztő szállítási eljárásaival összhangban.

AGD_PRE.1-1 Az értékelőnek ellenőriznie kell, hogy biztosították-e a leszállított TOE biztonságos elfogadásához szükséges eljárásokat.

Amennyiben a fejlesztő szállítási eljárásaival kapcsolatban nem várható elfogadási eljárások alkalmazása, akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

AGD_PRE.1-2 Az értékelőnek meg kell vizsgálnia a biztosított elfogadási eljárásokat annak megállapítása érdekében, hogy azok leírják-e a TOE biztonságos elfogadásához szükséges lépéseket, a fejlesztő szállítási eljárásaival összhangban.

Az elfogadási eljárásoknak legalább az arra vonatkozó felhasználói ellenőrzést tartalmazniuk kell, hogy a TOE valamennyi részét az ST-ben jelzett helyes verziókkal szállították-e le.

Az elfogadási eljárásoknak tükrözniük kell azokat a felhasználó által a leszállított TOE elfogadásához alkalmazott lépéseket, melyek a fejlesztő szállítási eljárásaiból származnak.

Az elfogadási eljárásoknak részletes információt kell szolgáltatniuk az alábbiakhoz, amennyiben azok alkalmazhatók:

a) az arról való meggyőződés, hogy a leszállított TOE a teljes értékelt példány.
b) a leszállított TOE módosításának vagy hamisításának az észlelése.

AGD_PRE.1.2C Az előkészítő eljárásoknak le kell írniuk a TOE biztonságos telepítéséhez, valamint az üzemeltetési környezethez való biztonságos előkészülethez szükséges valamennyi lépést, az ST-ben leírt, üzemeltetési környezetre vonatkozó biztonsági célokkal összhangban.

AGD_PRE.1-3 Az értékelőnek ellenőriznie kell, hogy biztosították-e a TOE biztonságos telepítéséhez szükséges eljárásokat.

Amennyiben a TOE-vel és üzemeltetési környezetével kapcsolatban nem várható telepítési eljárások alkalmazása (mert például a TOE-t már működésre alkalmas állapotban szállították le, s nincsenek a környezetére vonatkozó követelmények), akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

AGD_PRE.1-4 Az értékelőnek meg kell vizsgálnia a biztosított telepítési eljárásokat annak megállapítása érdekében, hogy azok leírják-e a TOE biztonságos telepítéséhez, valamint az üzemeltetési környezet biztonságos előkészítéséhez szükséges lépéseket, az ST biztonsági céljaival összhangban.

Amennyiben nem várható telepítési eljárások alkalmazása (mert például a TOE-t már működésre alkalmas állapotban szállították le, s nincsenek a környezetére vonatkozó követelmények), akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

A telepítési eljárásoknak részletes információt kell szolgáltatniuk az alábbiakról, amennyiben azok alkalmazhatók:

a) a biztonságos telepítéshez szükséges minimális rendszer követelmények,
b) az üzemeltetési környezetre vonatkozó követelmények, az ST-ben meghatározott biztonsági célokkal összhangban,
c) a TSF ellenőrzése alatt álló egyedek telepítés-specifikus biztonsági tulajdonságainak módosítása,
d) kivételek és problémák kezelése.

6.2.5.2.2.2. Az AGD_PRE.1.2E értékelői akció

AGD_PRE.1.2E Az értékelőnek végre kell hajtania az előkészítő eljárásokat annak megerősítése érdekében, hogy a TOE biztonságosan előkészíthető a működésre.
Az előkészítés megköveteli az értékelőtől, hogy a TOE-t egy leszállításra alkalmas állapotból olyan állapotba állítsa át, amelyben a TOE üzemel, beleértve a TOE elfogadását és telepítését, valamint az ST-ben megadott biztonsági célokkal összhangban álló SFR-ek érvényre juttatását.

Az értékelőnek a TOE elfogadására és telepítésére kizárólag a fejlesztői eljárásokat szabad követnie, s csak a vásárlóktól általánosan elvárt tevékenységeket szabad végrehajtania, csak az előkészületi útmutatót használva. A végrehajtás során tapasztalt bármilyen nehézség hiányos, nem egyértelmű vagy megalapozatlan útmutatót jelenthet.

Az értékelő ezt a munkaegységet végrehajthatja a „Független tesztelés – minta” (ATE_IND.2) értékelési altevékenységgel együtt.

6.2.5.3. Az Életciklus támogatás garanciaosztály (ALC) értékelése

Az életciklus támogatáshoz kapcsolódó tevékenységnek az a célja, hogy elbírálja a fejlesztő által a TOE fejlesztése és kezelése során használt biztonsági eljárások megfelelőségét. Ezek az eljárások kiemelt garanciaszinten magukban foglalják a fejlesztő által használt életciklus modellt, a konfiguráció kezelést, a TOE fejlesztése során alkalmazott biztonsági intézkedéseket, a fejlesztő által a TOE életciklusa során használt eszközöket és a szállítási tevékenységet.

A TOE elégtelenül ellenőrzött fejlesztése és kezelése sebezhetőségekhez vezethet a megvalósításban. Egy definiált életciklus modellnek való megfelelőség elősegítheti az intézkedések javítását ezen a területen. Egy, a TOE-hoz alkalmazott felmérhető életciklus modell megszüntetheti a félreérthetőségeket a TOE fejlesztési eljárásának kiértékelésében.

A konfiguráció kezeléshez kapcsolódó tevékenységnek az a célja, hogy segítséget nyújtson a fogyasztónak az értékelt TOE beazonosításában, hogy biztosítsa a konfiguráció elemek egyedi azonosítását, és biztosítsa a fejlesztő által a TOE-n történt változtatások ellenőrzéséhez és nyomonkövetéséhez használt eljárások megfelelőségét. Ez magában foglalja az arra vonatkozó részleteket, hogy milyen változtatások vannak nyomonkövetve, hogy a lehetséges változtatások hogyan vannak beépítve, és magában foglalja, hogy milyen mértékben használnak automatizálást a hibalehetőségek csökkentésére.

A fejlesztő biztonsági eljárásainak az a célja, hogy védjék a TOE-t és a kapcsolódó tervezési információkat a hamisításokkal vagy felfedésekkel szemben. A fejlesztési folyamatba történő hamisítás lehetővé teheti sebezhetőségek szándékos bevitelét. A tervezési információk felfedése lehetővé teheti a sebezhetőségek könnyebb kiaknázhatóságát. Az eljárások megfelelősége a TOE és a fejlesztési folyamat természetétől függ.

Ha a fejlesztő és a fejlesztési folyamatba bevont harmadik felek jól meghatározott fejlesztő eszközöket használnak és megvalósítási szabványokat alkalmaznak, akkor ez segít annak biztosításában, hogy sebezhetőségeket ne vigyenek be figyelmetlenségből a pontosítás során.

A szállításhoz kapcsolódó tevékenység célja annak az elbírálása, hogy megfelelő azoknak az eljárásoknak a dokumentációja, amelyek biztosítják, hogy a TOE-t változtatás nélkül szállítják ki a fogyasztóhoz.

6.2.5.3.1. Konfiguráció kezelési képességek: Az ALC_CMC.4 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztő egyértelműen azonosította-e a TOE-t és annak konfiguráció elemeit, valamint hogy megfelelő módon, automatizált eszközökkel ellenőrzik-e ezen elemek módosíthatóságát, s ezáltal a konfiguráció kezelés rendszer kevésbé lesz-e érzékeny az emberi hibákra vagy hanyagságra.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) a tesztelésre alkalmas TOE,
c) a konfiguráció kezelési dokumentáció.

6.2.5.3.1.1. Az ALC_CMC.4.1E értékelői akció

ALC_CMC.4.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ALC_CMC.4.1C A TOE-t meg kell jelölni egyedi hivatkozásával.

ALC_CMC.4-1 Az értékelőnek ellenőriznie kell, hogy az értékelésre benyújtott TOE verzióját megjelölték-e hivatkozásával.

Az értékelőnek gondoskodnia kell arról, hogy a TOE tartalmazza az ST-ben megadott egyedi hivatkozást. Ez elérhető megjelölt csomagolással vagy adathordozóval, illetve a működő TOE által megjelenített címkével. Ez biztosítja, hogy a vásárlók is képesek a TOE megfelelő azonosítására (a vásárlás vagy használat időpontjában).

A TOE biztosíthat is egy olyan módszert, mellyel egyszerűen azonosítható. Például egy szoftver TOE induláskor vagy egy parancs-sorra adott válaszként kijelezheti nevét és verziószámát. Egy hardver vagy förmver TOE azonosítható a TOE-ra fizikailag rábélyegzett sorozatszámmal.

Alternatív megoldásként a TOE által biztosított egyedi hivatkozás lehet a TOE-t alkotó összes összetevő egyedi hivatkozásának kombinációja (egy összetett TOE esetén).

ALC_CMC.4-2 Az értékelőnek ellenőriznie kell, hogy az alkalmazott TOE hivatkozások ellentmondás mentesek-e.

Amennyiben a TOE-t egynél több helyen jelölik meg (címkézik), akkor a címkéknek egyezniük kell. Lehetséges például, hogy a TOE részeként biztosított, címkézett útmutató dokumentációkat az értékelt működő TOE-hez kapcsoljuk. Ez biztosítja, hogy a vásárlók

biztosak legyenek abban, hogy a TOE értékelt verzióját vették meg, telepítették, és az útmutató dokumentációból is a helyes verzióval rendelkeznek, az ST-nek megfelelő üzemeltetés érdekében.

Az értékelő azt is ellenőrizze, hogy a TOE hivatkozása megegyezik-e az ST-ben szereplővel.

Ha ezt a munkaegységet egy összetett TOE esetében alkalmazzák, akkor erre a következők lesznek érvényesek. Az összetett IT TOE-t nem fogják felcímkézni az egyedi (összetett) hivatkozásával, csak az egyes komponensek lesznek felcímkézve a megfelelő TOE hivatkozással. Az IT TOE további fejlesztését igényelné, hogy fel legyen címkézve az összetett hivatkozással, mégpedig az indítás és/vagy üzemeltetés során. Ha az összetett TOE-t az alkotóelem TOE-k formájában szállítják le, akkor a leszállított TOE elemek nem fogják tartalmazni az összetett hivatkozást. Azonban az összetett TOE ST tartalmazni fogja az összetett TOE-ra vonatkozó egyedi hivatkozást, és azonosítani fogja az összetett TOE-t képező alkotóelemeket, amin keresztül a fogyasztók képesek lesznek megállapítani, hogy a megfelelő elemekkel rendelkeznek-e.

ALC_CMC.4.2C A konfiguráció kezelés dokumentációnak le kell írnia a konfiguráció elemek egyértelmű azonosítására alkalmazott módszert.

ALC_CMC.4-3 Az értékelőnek meg kell vizsgálnia a konfiguráció elemek azonosításához alkalmazott módszert, annak megállapítása érdekében, hogy az leírja-e azt, hogy hogyan azonosítják egyedileg a konfiguráció elemeket.

Eljárások ismertessék, hogy az egyes konfiguráció elemek állapota hogyan követhető nyomon a TOE életciklusa során. Az eljárások részletezve lehetnek a CM tervben vagy szerte a CM dokumentációban. A tartalmazott információ ismertesse a következőket:

a) azt a módszert, ahogyan az egyes konfiguráció elemek egyedileg azonosítva lettek, hogy lehetséges legyen ugyanazon konfiguráció elem verzióinak nyomonkövetése;
b) azt a módszert, ahogyan a konfiguráció elemekhez egyedi azonosítókat jelölnek ki, és ahogyan ezek a CM rendszerbe bekerülnek;
c) azt a módszert, amely egy konfiguráció elem kiváltott verzióinak beazonosítására szolgál.

ALC_CMC.4.3C A konfiguráció kezelés rendszernek egyértelműen azonosítania kell minden konfiguráció elemet.

ALC_CMC.4-4 Az értékelőnek meg kell vizsgálnia a konfiguráció elemeket annak megállapítása érdekében, hogy azokat a konfiguráció kezelés rendszernek megfelelő módon azonosították.

Arra vonatkozó garancia, hogy a CM rendszer minden konfiguráció elemet egyedileg azonosít, a konfiguráció elemek azonosítóinak vizsgálatán keresztül nyerhető. Mind a TOE-t alkotó konfiguráció elemekre, mind pedig a fejlesztő által értékelési bizonyítékként átadott konfiguráció elem leírásokra vonatkozóan az értékelőnek meg kell erősítenie, hogy minden egyes konfiguráció elem olyan egyedi azonosítóval rendelkezik, amely összhangban áll a CM dokumentációban ismertetett egyedi azonosítási módszerrel.

ALC_CMC.4.4C A konfiguráció kezelés rendszernek olyan automatizált eszközöket kell biztosítania, mely csak jogosult változtatásokat enged végrehajtani a konfiguráció elemekben.

ALC_CMC.4-5 Az értékelőnek meg kell vizsgálnia a konfiguráció kezelési tervben leírt hozzáférés ellenőrzési intézkedéseket (lásd ALC_CMC.4.6C), annak megállapítása érdekében, hogy azok automatikusan és hatékonyan meggátolják-e a konfiguráció elemekhez való jogosulatlan hozzáféréseket.

Az értékelő többféleképpen is megállapíthatja a konfiguráció kezelés hozzáférés ellenőrzési intézkedéseinek hatékonyságát. Például az értékelő gyakorlati próbával győződhet meg azok kikerülhetetlenségéről. Az értékelő használhatja a konfiguráció kezelés rendszer (ALC_CMC.4.10C által megkövetelt) eljárásainak kimeneteit is. Az értékelő végignézhet egy olyan bemutatót is, mely a hozzáférés ellenőrzési intézkedések hatékony működését szemléltetik.

ALC_CMC.4.5C A konfiguráció kezelés rendszernek automatizált eszközökkel támogatnia kell a TOE előállítását.

ALC_CMC.4-6 Az értékelőnek ellenőriznie kell a konfiguráció kezelési tervet (lásd ALC_CMC.4.6C), hogy az tartalmaz-e automatizált eljárásokat a TOE előállításának támogatására.

Az „előállítás” kifejezés arra a tevékenységsorozatra vonatkozik, melyet a fejlesztő alkalmazott azon folyamat során, melyben a TOE az implementáció reprezentációból a végfelhasználóhoz történő szállításra elfogadható állapotba kerül.

Az értékelő igazolja az automatizált előállítást támogató eljárások meglétét a konfiguráció kezelési tervben.

A következők példák olyan automatizált eszközökre, amelyek elősegítik a TOE előállítását:
- szoftver TOE esetében egy "make" (szerkesztő) eszköz (ahogyan ezt sok szoftverfejlesztő eszköz biztosítja);
- hardver TOE esetében egy olyan eszköz, amely automatikusan biztosítja (például vonalkódok segítségével), hogy csak olyan részek lettek összekapcsolva, amelyek valóban összetartoznak.

ALC_CMC.4-7 Az értékelőnek meg kell vizsgálnia a TOE előállítást támogató eljárásokat annak megállapítása érdekében, hogy azok hatékonyan biztosítják, hogy a TOE generálás eredménye a megvalósítási reprezentációt tükrözi.

Az előállítást támogató eljárások világosan definiált módon ismertessék, hogy mely eszközöket kell használni a végleges TOE előállításához az implementációs megjelenési formából. A szokások, irányelvek és egyéb összeállítások az ALC_TAT alatt kerülnek ismertetésre.

Az értékelő állapítsa meg, hogy az előállítást támogató eljárásokat követve a TOE generálásához a helyes konfigurációs elemeket használják. Például egy szoftver TOE esetén ez magába foglalhatja annak ellenőrzését, hogy az automatizált előállítást támogató eljárások

biztosítják, hogy minden forrásállomány és kapcsolódó könyvtár szerepeljen a tárgykódban. Az eljárásoknak biztosítaniuk kell a fordító opciók, illetve az ezzel összehasonlítható egyéb opciók egyértelmű meghatározottságát is. Egy szoftver TOE esetén ez magába foglalhatja annak ellenőrzését, hogy az automatizált előállítást támogató eljárások biztosítják, hogy az összetartozó részek hiánytalanul egybeépítésre kerülnek.

A vásárló így bizonyos lehet afelől, hogy a telepítésre leszállított TOE verzió egyértelmű módon a megvalósítási reprezentációból keletkezett, és az ST-ben leírt SFR-eket valósítja meg.

Az értékelőnek tisztában kell lennie azzal, hogy a konfiguráció kezelés rendszer nem feltétlenül teszi lehetővé a TOE előállítását, csak támogatást biztosít ehhez a folyamathoz, segítve így az emberi tévedés valószínűségének csökkentését.

ALC_CMC.4.6C A konfiguráció kezelés dokumentációnak tartalmaznia kell egy konfiguráció kezelés tervet.

ALC_CMC.4-8 Az értékelőnek ellenőriznie kell, hogy a konfiguráció kezelés rendszer tartalmaz-e konfiguráció kezelés tervet.

A konfiguráció kezelés tervnek nem feltétlenül kell egy összefüggő dokumentumnak lennie, bár ajánlott, hogy legyen egy különálló dokumentum, mely leírja, hogy a konfiguráció kezelés terv különböző részei hol találhatók. Amennyiben a konfiguráció kezelés tervet több dokumentum együtteseként biztosítják, a következő munkaegység útmutatót ad az elvárt tartalomra.

ALC_CMC.4.7C A konfiguráció kezelés tervnek le kell írnia, hogy a TOE fejlesztéséhez a konfiguráció kezelés rendszer hogyan használják.

ALC_CMC.4-9 Az értékelőnek meg kell vizsgálnia a konfiguráció kezelés tervet annak megállapítása érdekében, hogy leírja-e azt, hogyan használják a konfiguráció kezelés rendszert a TOE fejlesztéséhez.

A konfiguráció kezelés terv az alábbiakat tartalmazhatja:

a) a TOE fejlesztői környezetében végrehajtott minden tevékenység, mely a konfiguráció kezelés hatáskörébe esik (pl. egy konfiguráció elem létrehozása, módosítása vagy törlése, adatmentés, archiválás);
b) milyen eszközök elérése szükséges (konfiguráció kezelés eszköz, űrlapok);
c) A konfiguráció kezelés eszközök használata: a konfiguráció kezelés rendszert használóknak szükséges részletek az eszközök helyes használatára, a TOE sértetlenségének biztosítása érdekében;
d) az előállítást támogató eljárások;
e) a konfiguráció kezelés hatáskörébe eső egyéb objektumok (fejlesztő komponensek és eszközök, vizsgáló környezetek, stb.);
f) az egyes konfiguráció elemeken a műveleteket végrehajtó szerepkörök és felelősségek (különböző típusú konfiguráció elemekre (pl. tervdokumentáció vagy forráskód) különböző lehet a szerepkör);
g) kik és hogyan határozhatnak a változásokról, interfész módosításról;

h) a változás kezelés leírása;
i)azon eljárások, melyek azt biztosítják, hogy a konfiguráció elemeken csak jogosult egyének végezhessenek módosításokat;
j)azon eljárások, melyek azt biztosítják, hogy segítségükkel a konfiguráció elemeken végzett egyidejű módosítások nem okoznak problémákat;
k) az eljárások alkalmazásának eredményeképp létrejött bizonyíték. Például egy konfiguráció elem változtatása esetén a konfiguráció kezelés rendszer a változtatás nyomon követhetősége érdekében naplózhatja a változtatás leírását, minden érintett konfiguráció elem azonosításával, a változtatás állapotával (felfüggesztett vagy befejezett), dátumával és időpontjával.
l)a verziókövetés és a TOE verziók egyedi hivatkozásához használt módszer (pl. operációs rendszer javítások kibocsátása, ezek alkalmazásának detektálása).

ALC_CMC.4.8C A konfiguráció kezelés tervnek le kell írnia azokat az eljárásokat, melyeket a módosított vagy újonnan létrehozott konfiguráció elemeknek a TOE részeként történő elfogadására használnak.

ALC_CMC.4-10 Az értékelőnek meg kell vizsgálnia a konfiguráció kezelés tervet annak megállapítása érdekében, hogy az leírja-e az újra létrehozott vagy módosított konfiguráció elemek elfogadására alkalmazott eljárásokat.

Az elfogadási eljárások konfiguráció kezelés tervbeli leírásának tartalmaznia kell az elfogadásért felelős fejlesztői szerepköröket vagy személyeket, valamint az elfogadás kritériumait. Ezeknek valamennyi elfogadási szempontot figyelembe kell venniük, különösen az alábbiakat:

a) egy konfiguráció elem első befogadása a konfiguráció kezelés rendszerbe különösen más gyártóktól származó szoftver, förmver és hardver összetevők beillesztése („integrálás”),
b) a konfiguráció elemek következő életciklus szakaszba továbbítása a TOE létrehozás minden fázisában (pl. modul, alrendszer, rendszer),
c) különböző fejlesztői helyszínek közötti továbbítás előtt,

Amennyiben ezt a munkaegységet egy összetett TOE-be integrálandó „függő” összetevőre alkalmazzák, a konfiguráció kezelés tervnek figyelembe kell vennie a függő TEO fejlesztője által megkapott „alap” összetevők ellenőrzését is.

Amikor az értékelők megkapják az alkotóelemeket, a következőket kell ellenőrizniük:

a) Minden egyes alapelemnek az átszállítása az alapelem fejlesztőjétől az összeszerelőhöz (függő TOE fejlesztő) az alapelem TOE-kra vonatkozó biztonságos szállítási eljárásokkal összhangban lett végrehajtva, ahogyan az az alapelem TOE-ra vonatkozó tanúsítási jelentésben ismertetve van.
b) Az átvett alkotóelemnek ugyanazok az azonosítói, mint amelyeket az ST-ben és az alkotóelem TOE-ra vonatkozó tanúsítási jelentésben kijelentenek.
c) Minden kiegészítő anyag, amely szükséges a fejlesztő számára az összeállításhoz (beillesztéshez), biztosítva van. Ez azért szükséges, hogy csatolva legyenek az alkotóelem TOE-k funkcionális specifikációinak szükséges kivonatai.

ALC_CMC.4.9C Bizonyítéknak kell kimutatnia, hogy konfiguráció kezelés rendszer minden konfiguráció elemet kezel.

ALC_CMC.4-11 Az értékelőnek ellenőriznie kell, hogy a konfiguráció listában azonosított konfiguráció elemeket a konfiguráció kezelés rendszerben kezelik-e.

A fejlesztő által alkalmazott konfiguráció kezelés rendszernek fenn kell tartania a TOE sértetlenségét. Az értékelő ellenőrizze, hogy minden konfiguráció elem típus (pl. terv dokumentáció vagy forrás kód modulok) esetén vannak-e a konfiguráció kezelés tervben leírt eljárások szerint generált bizonyíték példák. Ekkor a mintavételezési módszer a konfiguráció kezelés rendszerben használt tagoltság szintjétől függ. Amennyiben például 10.000 forráskód modul szerepel a konfiguráció listában, nyilván más mintavételezési stratégiát szükséges követni, mintha csak 1 vagy 5. A tevékenység célja nem az apró hibák felderítése, hanem annak biztosítása, hogy a konfiguráció kezelés rendszer helyesen működik.

A mintavételezésre útmutató található a 7.2.1 pontban.

ALC_CMC.4.10C Bizonyítéknak kell kimutatnia, hogy a konfiguráció kezelés rendszer a konfiguráció kezelés tervnek megfelelően működik.

ALC_CMC.4-12 Az értékelőnek ellenőriznie kell a konfiguráció kezelés dokumentációt annak kiderítéséhez, hogy tartalmazza-e a konfiguráció kezelés terv által meghatározott konfiguráció kezelés rendszer rekordokat.

A konfiguráció kezelés rendszer kimenetének bizonyítékot kell szolgáltatnia ahhoz, hogy az értékelő meg tudjon győződni arról, hogy a konfiguráció kezelés tervet valóban alkalmazzák-e, valamint a konfiguráció kezelés rendszer minden konfiguráció elemet kezel-e, ahogy azt az ALC_CMC.4.9C megköveteli. Egy példa kimenet tartalmazhat változáskezelési űrlapokat vagy konfiguráció elem hozzáférést jóváhagyó nyomtatványokat.

ALC_CMC.4-13 Az értékelőnek meg kell vizsgálnia a bizonyítékot annak meghatározása érdekében, hogy a konfiguráció kezelés rendszert a konfiguráció kezelés tervben szereplő módon használják.

Az értékelőnek ki kell választania minden konfiguráció kezelés szempontból fontos művelettípusra (pl. létrehozás, módosítás, törlés, korábbi verzióra visszatérés stb.) egy bizonyíték mintát annak megerősítése céljából, hogy a munkát a dokumentált eljárásoknak megfelelően végezték el. Az értékelőnek meg kell erősítenie, hogy a bizonyíték tartalmazza az összes információt, mely a konfiguráció kezelés tervben az adott műveletre elő van írva. A bizonyíték vizsgálata hozzáférést igényelhet a használt konfiguráció kezelés eszközhöz. Az értékelő használhat mintavételezést ehhez a munkához.

A mintavételezésre útmutató található a 7.2.1 pontban.

A fejlesztői csoport kiválasztott tagjaival készült interjú révén kiegészítő bizonyosságot szerezhet az értékelő a konfiguráció kezelés rendszer helyes használatáról, illetve a konfiguráció elemek hatékony kezeléséről. Az ilyen interjúk segítségével az értékelő mélyebb ismereteket szerezhet a konfiguráció kezelés rendszer használatáról, egyúttal megerősítést

nyerhet, hogy a konfiguráció kezelés eljárásait valóban a konfiguráció kezelés dokumentációban leírt módon alkalmazzák. Az ilyen interjúk azonban inkább csak kiegészítik, s nem helyettesítik a dokumentációs bizonyítékok vizsgálatát, s nem is szükségesek, ha a dokumentációs bizonyítékok egyedül kielégítik az elvárásokat. Olyan esetben, amikor bizonyos szempontokat (pl. szerepköröket és felelősségeket) a konfiguráció kezelés tervből nem sikerül teljes körűen felderíteni, az interjún alapuló módszer megoldást adhat.

E tevékenység végrehajtása során az értékelőnek várhatóan meg kell látogatnia a fejlesztés helyszínét.

A fejlesztői helyszín meglátogatására útmutató található a melléklet 7.2.3 pontjában.

6.2.5.3.2. Konfiguráció kezelés hatóköre: Az ALC_CMS.4 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a konfiguráció lista tartalmazza-e a TOE-t, a TOE-t alkotó részeket, a TOE megvalósítási reprezentációját, a biztonsági hibákat, valamint az értékelési bizonyítékokat.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) a konfiguráció lista.

6.2.5.3.2.1. Az ALC_CMS.4.1E értékelői akció

ALC_CMS.4.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ALC_CMS.4.1C A konfiguráció listának tartalmaznia kell a következőket: maga a TOE; a garanciális biztonsági követelmények (SAR) által megkövetelt értékelési bizonyítékok, a TOE-t alkotó részek; a megvalósítási reprezentáció; biztonsági hiba jelentések és megoldási állapotuk.

ALC_CMS.4-1 Az értékelőnek ellenőriznie kell, hogy a konfiguráció lista tartalmazza-e az alábbi elem készletet:

a) maga a TOE;
b) a TOE-t alkotó részek;
c) a TOE megvalósítási reprezentációja;
d) az ST garanciális biztonsági követelményei (SAR) által megkövetelt értékelési bizonyítékok;
e) a megvalósítással kapcsolatban bejelentett biztonsági hibák rögzítésére használt dokumentáció (pl. egy fejlesztői probléma jelentő adatbázisból származó probléma állapot jelentés).

ALC_CMS.4.2C A konfiguráció listának egyértelműen azonosítania kell a konfiguráció elemeket.

ALC_CMS.4-2 Az értékelőnek meg kell vizsgálnia a konfiguráció listát annak megállapítása érdekében, hogy az egyértelműen azonosít-e minden konfiguráció elemet.
A konfiguráció lista elegendő információt tartalmazzon ahhoz, hogy egyértelműen azonosítja az összes konfiguráció elem használt verzióját (ez tipikusan egy verzió szám). Ezen lista használatával az értékelő ellenőrizheti, hogy az értékelés a helyes konfiguráció elemekre, és mindegyikük helyes verziójára irányul.

ALC_CMS.4.3C A konfiguráció listának a TSF szempontból fontos minden konfiguráció elemre meg kell adni az elem fejlesztőjét.

ALC_CMS.4-3 Az értékelőnek ellenőriznie kell, hogy a konfiguráció lista megadja-e a TSF szempontból fontos összes konfiguráció elem fejlesztőjét.

Amennyiben a TOE fejlesztésében csak egy fejlesztő érintett, akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

6.2.5.3.3. Szállítás: Az ALC_DEL.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a szállítási dokumentáció leírja-e az összes olyan eljárást, amelyet a TOE biztonság fenntartásához használnak a vásárlókhoz történő szállítás során.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:
a) az ST,
b) a szállítási dokumentáció.

6.2.5.3.3.1. Az ALC_DEL.1.1E értékelői akció

ALC_DEL.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ALC_DEL.1.1C A szállítási dokumentációnak le kell írnia minden olyan eljárást, amely a TOE verzióinak vásárlókhoz történő szállítása során a biztonság fenntartásához szükséges.

ALC_DEL.1-1 Az értékelőnek meg kell vizsgálnia a szállítási dokumentációt annak megállapítása érdekében, hogy az leírja-e az összes olyan eljárást, amely a TOE vagy részei verzióinak felhasználókhoz történő szállítása során a biztonság fenntartásához szükségesek.

A szállítási eljárások leírják a TOE vagy összetevőinek szállítása során a TOE biztonságának fenntartására, valamint a TOE azonosítására alkalmas eljárásokat.

A szállítási dokumentáció az egész TOE-re vonatkozik, ugyanakkor a TOE különböző részeire különböző eljárások vonatkozhatnak. Az értékelésnek az eljárások összességét figyelembe kell vennie.

A szállítási eljárásokat a szállítás teljes folyamatában, a gyártási környezettől a telepítési környezetig alkalmazni kell (például csomagolás, tárolás és szétosztás). A csomagolás és szállítás szabványos kereskedelmi gyakorlata elfogadható lehet. Ez magában foglalja a zsugorfóliás csomagolást, a biztonsági csíkot vagy egy pecsételt borítékot. A szétosztásra fizikai (pl. nyilvános levelezés vagy magán szolgáltató) vagy elektronikus (pl. elektronikus mail vagy interneten keresztüli letöltés) eljárások alkalmazhatók.

A fejlesztő kriptográfiai ellenőrző összegeket vagy elektronikus aláírást használhat a módosítás vagy a hamisítás észlelhetősége érdekében. A hamisítás ellen védő pecsétek a bizalmasság megsértését is jelzik. Szoftver TOE esetén a bizalmasság titkosítás alkalmazásával biztosítható. Amennyiben a rendelkezésre állás fontos szempont, megbízható továbbítás követelhető meg.

A "biztonság fenntartásához szükséges" kitétel értelmezésekor figyelembe kell venni az alábbiakat:

- a TOE jellege (pl. szoftver vagy hardver),
- A TOE-ra kinyilvánított általános, a sebezhetőség vizsgálatnál megválasztott biztonsági szint. Amennyiben a TOE-nak üzemeltetési környezetében ellent kell állnia egy bizonyos támadó képességgel rendelkező támadókkal szemben, akkor ez a TOE szállítására is alkalmazandó. Az értékelőnek meg kell állapítania, hogy kiegyensúlyozott megközelítést alkalmaztak-e annak érdekében, hogy a szállítás ne jelentsen gyenge pontot egy egyébként biztonságos fejlesztési folyamatban.
- Az ST által meghatározott biztonsági célok. A szállítási dokumentációknál a hangsúly valószínűleg a sértetlenséggel kapcsolatos intézkedéseken lesz. Ugyanakkor bizonyos TOE-k szállítása esetében a bizalmasság és a rendelkezésre állás is kiemelt fontosságú, ilyenkor ezeket a szempontokat is vizsgálni kell.

Az ALC_DEL.1.2D bizonyítékból származtatott értékelői akció

ALC_DEL.1.2D A fejlesztőnek használnia kell a szállítási eljárásokat.

ALC_DEL.1-2 Az értékelőnek meg kell vizsgálnia a szállítási folyamat különböző oldalait annak megállapítása érdekében, hogy alkalmazzák-e a szállítási eljárásokat.

Az értékelő megközelítési módszere a szállítás alkalmazásának ellenőrzésével kapcsolatban a TOE jellegétől és magától a szállítási folyamattól függ. Az eljárások vizsgálatán túl az értékelőnek valamilyen szinten meg kell győződnie arról, hogy a szabályokat a gyakorlatban is betartják. Lehetséges megközelítési módok az alábbiak:

a) látogatás a szétosztási hely(ek)en, ahol megfigyelhető az eljárások gyakorlati alkalmazása;
b) a TOE átvizsgálása a szállítás valamelyik fázisában vagy a felhasználó telephelyén (például a hamisítás ellen védő pecsétek ellenőrzése);
c) a szállítási folyamat alkalmazásának megfigyelése a gyakorlatban, amikor az értékelő a TOE-t szabályos csatornákon keresztül szerzi be;
d) a végfelhasználók megkérdezése a TOE szállítás folyamatáról.

A helyszíni szemlékre útmutató található a7.2.3 pontban.

Egy újonnan fejlesztett TOE esetén előfordulhat, hogy a TOE szállítási eljárásait még nem vezették be a gyakorlatban. Ekkor az értékelőnek meg kell elégednie azzal, hogy a megfelelő eljárásokat és eszközöket kialakították a jövőbeli szállításokra, és minden érintett alkalmazott tisztában van a felelősségével. Az értékelő kérheti a szállítás egy "száraztesztjét", amennyiben ez célszerűnek tűnik. Amennyiben a fejlesztő már korábban létrehozott hasonló terméket, akkor az ott bevezetett eljárások vizsgálata is segíthet az aktuális termékkel kapcsolatos garancia megállapításában.

6.2.5.3.4. Fejlesztés biztonság: Az ALC_DVS.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztő fejlesztési környezetre vonatkozó ellenintézkedései megfelelők-e, alkalmasak-e a TOE tervek és a TOE megvalósítás bizalmasságának és sértetlenségének megvédésére, biztosítva ezzel, hogy a TOE biztonságos működése ne kompromittálódjon.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) a fejlesztés biztonsági dokumentáció.

Az értékelőnek szüksége lehet egyéb értékelői bizonyíték megvizsgálására is annak megállapítása érdekében, hogy a biztonsági intézkedések jól meghatározottak-e, s követik-e ezeket. Speciálisan, az értékelőnek szüksége lehet a fejlesztő (az ALC_CMC.4 és ALC_CMS.4 altevékenységek bemenetét képező) konfiguráció kezelési dokumentációjának megvizsgálására. Az eljárások alkalmazására vonatkozó bizonyítékokat is megkövetelik.

6.2.5.3.4.1. Az ALC_DVS.1.1E értékelői akció

ALC_DVS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ALC_DVS.1.1C A fejlesztés biztonsági dokumentációnak le kell írnia minden olyan fizikai, eljárásbeli, személyi és egyéb biztonsági intézkedést, mely a TOE tervek és TOE megvalósítás bizalmasságának és sértetlenségének a védelméhez szükséges, fejlesztési környezetében.

ALC_DVS.1-1 Az értékelőnek meg kell vizsgálnia a fejlesztői biztonsági dokumentációt annak megállapítása érdekében, hogy az részletezi-e az összes olyan, fejlesztői környezetben használt biztonsági intézkedést, melyek a TOE tervek és a TOE megvalósítás bizalmasságának és sértetlenségének megőrzését szolgálják.
Az értékelő először azt határozza meg, hogy mire van szükség a kellő védelemhez. Ehhez használja az ST információit, különösen a fejlesztési környezetre vonatkozó biztonsági célokat.

Az ST-ből származó közvetlen információ hiányában az értékelőnek kell meghatároznia a szükséges biztonsági mértéket. Olyan esetben, amikor a fejlesztő alulbecsülte a szükséges

biztonsági mértéket, egy lehetséges sebezhetőséggel való visszaélésen alapuló világos indoklást kell erre adni.

Az értékelőnek az alábbi típusú biztonsági intézkedéseket kell számba vennie a dokumentáció vizsgálatakor:

a) *fizikai*, például fizikai hozzáférés védelmi intézkedések a TOE fejlesztői környezethez való jogosulatlan hozzáférés megakadályozására (munkaidőben és azon kívül);
b) *eljárásbeli*, például:
   ba) a fejlesztői környezethez vagy annak bizonyos elemeihez (pl. fejlesztő berendezésekhez) való hozzáférés biztosítása;
   bb) hozzáférési jogok visszavonása, ha egy személy elhagyja a fejlesztői csoportot;
   bc) védett anyag továbbítása a fejlesztői környezeten belül, kívülre, illetve (a meghatározott elfogadási eljárásokkal összhangban) a különböző fejlesztői környezetek között ;
   bd) látogatók beengedése és kísérése a fejlesztői környezetben;
   be) szerepkörök és felelősségek a biztonsági intézkedések folyamatos betartásában, és a biztonsági szabályszegések észlelésében.
c) *személyi*, például egy új fejlesztő megbízhatóságának ellenőrzése;
d) *egyéb biztonsági intézkedések*, például a fejlesztői eszközök logikai védelme.

A fejlesztői biztonsági dokumentációnak azonosítania kell a fejlesztési helyszíneket, valamint le kell írnia a végrehajtott fejlesztés különböző oldalait, az egyes helyszíneken alkalmazott biztonsági intézkedésekkel együtt. A fejlesztésre sor kerülhet például egyetlen épület több helyszínén, egy telephely több épületében, vagy több telephelyen. TOE részek vagy befejezetlen TOE-k szállítása különböző fejlesztési helyszínek között a Fejlesztés biztonság (ALC_DVC), míg a kész TOE vásárlóhoz továbbítása a Szállítás (ALC_DEL) hatáskörébe tartozik.

A fejlesztés magában foglalja a TOE előállítását is.

ALC_DVS.1-2 Az értékelőnek meg kell vizsgálnia a fejlesztés bizalmasságát és sértetlenségét, annak megállapítása érdekében, hogy az alkalmazott biztonsági intézkedések kielégítők-e.

Az alábbi jellegű szabályok tartoznak ide:

a) a TOE fejlesztéssel kapcsolatos milyen információkat kell bizalmasan kezelni, és a fejlesztői csoport mely tagjai férhetnek hozzá ilyen anyagokhoz;
b) milyen anyagokat kell védeni a jogosulatlan módosítástól a TOE sértetlenségének megőrzése érdekében, és a fejlesztők közül kik jogosultak az ilyen anyagok módosítására.

Az értékelőnek meg kell állapítania, hogy a fejlesztői biztonsági dokumentáció tartalmazza-e ezeket a szabályokat, az alkalmazott biztonsági intézkedések megfelelnek-e a szabályoknak, és a szabályok köre teljes-e.

Amíg a Konfiguráció kezelés képességei (ALC_CMC) követelményei rögzítettek, a Fejlesztés biztonsága (ALC_DVS) csak a szükséges intézkedéseket követeli meg, s ezek függnek a

TOE természetétől, s az ST-ben megadott információktól. Például az ST a fejlesztési környezetre meghatározhat egy olyan biztonsági célt, amely megköveteli, hogy a TOE-t olyan fejlesztők dolgozzák ki, akik biztonsági engedéllyel rendelkeznek. Az értékelőnek ekkor ebben az altevékenységben meg kell állapítania, hogy alkalmaztak-e ilyen szabályt.

6.2.5.3.4.2. Az ALC_DVS.1.2E értékelői akció

ALC_DVS.1.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági intézkedéseket betartják.

ALC_DVS.1-3 Az értékelőnek meg kell vizsgálnia a fejlesztési biztonság dokumentációt és az ahhoz kapcsolódó bizonyítékokat annak megállapítása érdekében, hogy a biztonsági intézkedéseket betartották-e.

Ebben a munkaegységben az értékelőnek meg kell állapítania, hogy a fejlesztési biztonság dokumentációban megfogalmazott biztonsági intézkedéseket alkalmazták-e a TOE sértetlenségének és a kapcsolódó dokumentáció bizalmasságának megfelelő védelme érdekében. Ez meghatározható például a dokumentált bizonyítékok vizsgálatával, melyet kiegészíthet a fejlesztői környezetben tett látogatás. A látogatás során az értékelő:

a) megfigyelheti a biztonsági intézkedések alkalmazását (pl. fizikai védelmi intézkedések);
b) megvizsgálhatja az eljárások alkalmazásának dokumentált bizonyítékát;
c) megkérdezheti, ellenőrizheti a fejlesztőket, hogy tisztában vannak-e a fejlesztés biztonsági szabályaival és eljárásaival, valamint saját felelőségükkel.

A fejlesztői helyszín meglátogatása hasznos módszer az alkalmazott intézkedések megbízhatóságának megítélésében. A látogatás elhagyását meg kell beszélni a tanúsító szervezettel.

A fejlesztői helyszín meglátogatására útmutató található a melléklet 7.2.3 pontjában.

6.2.5.3.5. Életciklus meghatározás: Az ALC_LCD.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztő használ-e dokumentált modellt a TOE életciklusára.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az ST,
b) az életciklus meghatározás dokumentáció.

6.2.5.3.5.1. Az ALC_LCD.1.1E értékelői akció

ALC_LCD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ALC_LCD.1.1C Az életciklus modell dokumentációnak le kell írnia a TOE fejlesztéséhez és karbantartásához használt modellt.

ALC_LCD.1-1 Az értékelőnek meg kell vizsgálnia az alkalmazott életciklus modell dokumentált leírását, annak megállapítása érdekében, hogy az lefedi-e a fejlesztési és karbantartási folyamatot.

Az életciklus modell leírásának az alábbiakat kell tartalmaznia:

a) a TOE életciklus fázisaira (fő folyamataira), illetve az egymást követő fázisok közötti átmenetre vonatkozó információk,
b) a fejlesztő által használt eljárásokra, eszközökre és technikákra (pl. a tervezéshez, kódolásra, tesztelésre, hibajavításra) vonatkozó információk,
c) az eljárások alkalmazását felügyelő átfogó menedzsment szerkezet (pl. az életciklus modell által lefedett fejlesztési és karbantartási folyamatban megkövetelt eljárások mindegyikére az egyedi felelősségi körök azonosítása és leírása),
d) arra vonatkozó információ, hogy a TOE mely részét szállítják alvállalkozók (amennyiben alvállalkozók is érintettek a TOE fejlesztésében).

Az ALC_LCD.1 értékelési altevékenység nem követeli meg az alkalmazott modell egyetlen szabványos életciklus modellnek való megfelelését sem.

ALC_LCD.1.2C Az életciklus modellnek biztosítania kell a TOE fejlesztéséhez és karbantartásához szükséges ellenőrzést.

ALC_LCD.1-2 Az értékelőnek meg kell vizsgálnia az életciklus modellt annak megállapítása érdekében, hogy az életciklus modell által leírt eljárások, eszközök és technikák használata pozitív módon hozzájárul-e a TOE fejlesztéséhez és karbantartásához.

Az életciklus modellben szereplő információ az értékelő számára arról ad bizonyosságot, hogy az alkalmazott fejlesztési és karbantartási eljárások a legkisebb szintre csökkentik a biztonsági hibák valószínűségét. Amennyiben az életciklus modellben szerepel például az ellenőrzési (ávizsgálás) folyamat, de a komponensek módosításának rögzítése nem garantált, akkor az értékelő nem tud megfelelő bizalommal lenni afelől, hogy a TOE-ba nem kerül be újabb hiba. Az értékelő további garanciát kaphat azáltal, hogy összehasonlítja a modell leírását a TOE fejlesztéssel kapcsolatos más értékelői tevékenységek (pl. a Konfiguráció kezelés képességei (ALC_CMC) által lefedett értékelői akciók) során összegyűjtött, a fejlesztési folyamatról szóló ismeretekkel. Az életciklus modellben talált hiányosságokkal foglalkozni kell, ha azok kimutathatóan növelhetik a TOE-ba bekerülő véletlen vagy szándékos hibák számát.

A CC nem tesz kötelezővé egyetlen fejlesztési módszert sem, és bármelyiket is alkalmazzák, a célszerűség szerint ajánlott azt értékelni. A "spirális", a "gyors-prototípus" vagy a "vízesés" tervezési modellek egyaránt alkalmazhatók egy minőségi TOE létrehozására, amennyiben ellenőrzött környezetben használják ezeket.

6.2.5.3.6. Eszközök és technikák: Az ALC_TAT.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztő jól meghatározott fejlesztő eszközökkel dolgozott-e (pl. programozási nyelvek vagy számítógéppel támogatott tervezési /CAD/ rendszerek), amelyek ellentmondásmentes és kiszámítható eredményeket adnak.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) a fejlesztő eszközök dokumentációja,
b) az implementáció reprezentáció egy részhalmaza.

Ez a munkaegység párhuzamosan hajtható végre a „Megvalósítási reprezentáció” (ADV_IMP.1) értékelési altevékenységgel, különös tekintettel az eszközökben lévő olyan tulajdonságok használatára, melyek kihatással vannak a tárgykódra (például fordítási opciók).

6.2.5.3.6.1. Az ALC_TAT.1.1E értékelői akció

ALC_TAT.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ALC_TAT.1.1C A megvalósításhoz használt minden fejlesztő eszköznek jól meghatározottnak kell lennie.

ALC_TAT.1-1 Az értékelőnek meg kell vizsgálnia a rendelkezésére bocsátott fejlesztő eszköz dokumentációt, annak megállapítása érdekében, hogy minden fejlesztő eszköz jól meghatározott-e.

Például egy nyelv, fordító vagy CAD rendszer akkor tekinthető jól meghatározottnak, ha megfelel egy elismert (pl. ISO) szabványnak. Egy nyelv akkor jól meghatározott, ha szintaxisának leírása egyértelmű és teljes, továbbá minden eleméhez tartozik részletes szemantikai leírás.

ALC_TAT.1.2C Minden fejlesztő eszköz dokumentációjának egyértelműen meg kell határoznia a megvalósítás során használt valamennyi utasítás, konvenció és direktíva jelentését.

ALC_TAT.1-2 Az értékelőnek meg kell vizsgálnia minden fejlesztő eszköz dokumentációját, annak megállapítása érdekében, hogy azok egyértelműen adják-e meg a megvalósításban használt összes utasítás konvenció és direktíva jelentését.

A fejlesztő eszköz dokumentációjának (pl. programozási nyelv specifikációk és felhasználói kézikönyvek) le kell fednie a TOE megvalósítási reprezentációjában szereplő minden utasítást, és minden egyes ilyen utasításra meg kell adnia az utasítás céljának és hatásának világos és egyértelmű definícióját. Ez a munkaegység párhuzamosan hajtható végre az ADV_IMP altevékenység során végrehajtott megvalósítási reprezentáció értékelői vizsgálatával. A legfontosabb teszt, melyet az értékelőnek alkalmaznia kell, annak vizsgálata, hogy a dokumentáció kellőképpen világos-e az értékelő számára a megvalósítási

reprezentáció megértéséhez. A dokumentációnak (például) nem szabad feltételeznie, hogy az olvasó a szóban forgó programozási nyelv szakértője.

Egy dokumentált szabvány használatára való hivatkozás elfogadható módszer a követelmény teljesítésére, feltéve, hogy a szabvány az értékelő számára hozzáférhető. A szabványtól való bárminemű eltérést dokumentálni kell.

A kritikus teszt az, hogy az értékelő meg tudja-e érteni a TOE forráskódját, amikor az ADV_IMP altevékenységben szereplő forráskód elemzést hajtja végre. Az alábbi ellenőrző lista további segítséget adhat a problémás területek feltárásában:

a) a nyelv definícióban az olyan kifejezések, mint például: „ennek a nyelvi elemnek a hatása nem definiált”, és az olyan kikötések, mint „megvalósítás-függő” vagy „hibás”, rosszul meghatározott részeket jelezhetnek;
b) az álnevek használata (ugyanazon memóriaterület különböző módokon való hivatkozása) a többértelműségi problémák gyakori forrása;
c) a kivételkezelés (mi történik a memória elfogyása vagy stack túlcsordulás esetén) szintén gyakorta nem kellőképpen meghatározott.

A legtöbb általánosan használt nyelvben, bármennyire is jól meghatározott, található néhány problémás elem. Amennyiben a megvalósítás nyelve nagyrészt jól meghatározott, de léteznek benne problémás elemek, akkor a forráskód elemzésének befejezéséig itt egy „Nem bizonyított” határozatot kell hozni.

Az értékelőnek a forráskód vizsgálata során ajánlott ellenőriznie, hogy a problémás elemek használata nem vezet-e be sebezhetőségeket. Az értékelőnek arról is ajánlott meggyőződnie, hogy a dokumentált szabványban eleve kizárt elemeket nem használtak.
A fejlesztő eszközök dokumentációjának a megvalósításhoz használt minden konvenció és direktíva jelentését is meg kell határoznia.

ALC_TAT.1.3C Minden fejlesztő eszköz dokumentációjának egyértelműen meg kell határoznia valamennyi megvalósítás-függő opció jelentését.

ALC_TAT.1-3 Az értékelőnek meg kell vizsgálnia a fejlesztő eszközök dokumentációját annak megállapítása érdekében, hogy az egyértelműen meghatározza-e az összes megvalósítás-függő opció jelentését.

A szoftver fejlesztő eszközök dokumentációjának tartalmaznia kell az olyan implementáció-függő opciók meghatározását, amelyek befolyásolhatják a végrehajtható kód jelentését, és azokét is, melyek különböznek a szabvány nyelvben dokumentálttól. Amennyiben az értékelő rendelkezésére bocsátják a forráskódot, akkor a fordítási és szerkesztési opciókkal kapcsolatos információkat is meg kell adni.

A hardver tervező és fejlesztő eszközök dokumentációjának le kell írnia az összes olyan opció használatát, melyek az eszközök kimenetét befolyásolják (például részletes hardver specifikációk vagy a tényleges hardver).

6.2.5.4. A Tesztelés garanciaosztály (ATE) értékelése

Ennek a tevékenységnek a célja annak megállapítása, hogy a TOE olyan módon viselkedik-e, ahogyan azt az ST-ben leírták és (az ADV osztályban leírt) értékelési bizonyítékban specifikálták. Ezt a megállapítást a TSF fejlesztő általi funkcionális tesztelése (ATE_FUN) és a TSF értékelő általi független tesztelése (ATE_IND) bizonyos kombinációján keresztül lehet megtenni. További garancia nyerhető azzal, hogy a fejlesztőt növekvő mértékben bevonják a tesztelésbe és a TOE-ra vonatkozó kiegészítő információk nyújtásába, valamint azzal, hogy az értékelő növeli a független tesztelési tevékenységeket.

6.2.5.4.1. Alkalmazási megjegyzések

A TSF tesztelését részben az értékelő, illetve a legtöbb esetben a fejlesztő hajtja végre. Az értékelő tesztelési törekvései nemcsak eredeti tesztek létrehozásából és végrehajtásából állnak, hanem a fejlesztői tesztek megfelelőségének felméréséből és ezek egy részhalmazának újra lefuttatásából is.

Az értékelő megvizsgálja a fejlesztői teszteket annak meghatározása érdekében, hogy azok milyen mértékben elegendőek annak bizonyításához, hogy a TSFI a specifikáltaknak (lásd ADV_FSP) megfelelően működik, és hogy megértse a fejlesztő tesztelési megközelítés módját. Hasonlóan, az értékelő megvizsgálja a fejlesztői teszteket annak meghatározása érdekében, hogy azok milyen mértékben elegendőek a TSF belső viselkedésének és tulajdonságainak a bemutatásához.

Az értékelő végrehajtja a fejlesztői tesztek egy részhalmazát is, ahogyan azokat dokumentálták, abból a célból, hogy megbizonyosodjon a fejlesztői teszteredményekről: az értékelő ennek a vizsgálatnak az eredményeit bemenetként fogja felhasználni a TSF egy részhalmazának független teszteléséhez. Erre a részhalmazra az értékelő egy olyan tesztelési megközelítési módot alkalmaz, amely eltér a fejlesztőétől, különösen akkor, ha a fejlesztői tesztek hiányosak.

A fejlesztői tesztelési dokumentáció helyességének értékeléséhez, illetve új tesztek készítéséhez az értékelőnek meg kell értenie a TSF elvárt, tervezett működését – mind belülről, mind a TSFI-n keresztül látható módon - azon SFR-ek összefüggésében, melyek kielégítésére létrehozták ezeket. Az értékelő választhatja azt az utat, hogy a TSF-et és a TSFI-t alrendszerekre bontja az ST funkcionális területei alapján (napló alrendszer, naplózással kapcsolatos TSFI, hitelesítő modul, hitelesítéssel kapcsolatos TSFI, stb.) ha az ST ezt nem bontotta már fel így, majd egyszerre csak egy alrendszerre összpontosít. Minden alrendszerre megvizsgálja az ST követelményt és a fejlesztői és az útmutató dokumentáció vonatkozó részeit, hogy megértse azt, milyen működést várnak el a TOE-tól. A fejlesztői dokumentációra épülő bizalom aláhúzza a tesztelés lefedettségének (ATE_COV) és mélységének (ATE_DPT) függőségét a fejlesztés (ADV) garanciaosztálytól.

A CC a családok összetevőinek alkalmazásakor elkülöníti a tesztelés lefedettségét és mélységét a funkcionális teszteléstől, a rugalmasság fokozása érdekében. A családok követelményeit azonban együtt kell alkalmazni annak biztosítása érdekében, hogy a TSF a specifikációjának megfelelően működik. A családok e szoros összefonódása az értékelői

munka megduplázódásához vezet a különböző altevékenységek között. Az alábbi alkalmazási megjegyzések az altevékenységek közötti szöveg ismétléseket minimalizálják.

A TOE elvárt működésének megértése

A tesztelési dokumentáció helyességének értékelése, illetve új tesztek készítése előtt az értékelőnek meg kell értenie a biztonsági funkciók elvárt, tervezett működését azon követelmények összefüggésében, melyek kielégítésére létrehozták ezeket.

Mint ahogyan korábban említésre került, az értékelő választhatja a TSF és a TSFI alrendszerekre bontását az ST-ben szereplő SFR-ek (naplózás, hitelesítés, stb.) szerint, majd egyszerre csak egy alrendszerre összpontosíthat. Az értékelő vizsgáljon meg minden ST követelményt, valamint a funkcionális specifikáció és az útmutató dokumentáció vonatkozó részeit, hogy megértse azt, milyen működést várnak el az érintett TSFI-től. Hasonlóan, az értékelő vizsgálja meg a TOE terv és a biztonsági szerkezet dokumentáció vonatkozó részeit, hogy megértse azt, milyen működést várnak el a TSF érintett alrendszereitől és moduljaitól.
A tervezett működés megértése után az értékelő vizsgálja meg a tesztelési tervet, hogy áttekintést kapjon a tesztelés módszeréről. A legtöbb esetben a tesztelési módszer egy TSFI kiváltása, majd a válaszok megfigyelése. A kívülről látható funkcionalitások közvetlenül tesztelhetők, amikor viszont a funkcionalitás a TOE-n kívülről nem látható (például a maradvány információ védelmi funkcionalitás), akkor más eszközöket kell alkalmazni.

A tesztelés, illetve egyéb módszerek a funkcionalitás elvárt működésének ellenőrzésére

Azon esetekben, melyekben nem célszerű, vagy nem lehetséges a tesztelés (amikor nincs kívülről látható TSFI), a tesztelési tervnek alternatívát kell adnia a tervezett viselkedés, működés ellenőrzésére. Az értékelő felelőssége az alternatív módszer alkalmasságának megítélése. A következőket azonban ajánlott figyelembe venni az egyéb módszerek alkalmasságának megállapításakor:

a) elfogadható alternatív módszer a megvalósítási reprezentáció elemzése annak megállapítása érdekében, hogy a megkívánt működést mutatja-e a TOE. Ez jelenthet kód vizsgálatot egy szoftver TOE, vagy chip-maszk vizsgálatot egy hardver TOE esetén.
b) elfogadható a fejlesztő integrációs vagy modul tesztelése által kapott bizonyíték felhasználása is. Amennyiben a fejlesztő integrációs vagy modul tesztelését használják egy biztonsági funkcionalitás elvárt működésének ellenőrzése során, akkor meg kell arról győződni, hogy a tesztelési bizonyíték a TOE aktuális megvalósítását tükrözi-e. Amennyiben az alrendszer vagy a modulok változtak a tesztelés óta, akkor bizonyítékra van szükség arról, hogy a változtatásokat nyomon követték és elemezték, vagy ilyen esetekben általában további teszteket kell elvégezni.

Hangsúlyozni kell, hogy a tesztelési munka kiegészítése alternatív módszerekkel csak akkor járható út, ha mind a fejlesztő, mind az értékelő úgy ítéli meg, hogy nincs más praktikus lehetőség egy biztonsági funkció tervezett működésének tesztelésére.

A tesztek megfelelőségének ellenőrzése

A tesztelés által megkövetelt kezdeti feltételek kialakításához szükség van a tesztelés előfeltételeire. Ezek kifejezhetők beállítandó paraméterekkel, vagy a tesztelés sorrendjének kialakításával, olyan esetekben, amikor az egyik teszt befejezése teremti meg egy másik teszt szükséges előfeltételeit. Az értékelőnek meg kell állapítania, hogy az előfeltételek teljesek és alkalmasak-e, nehogy a megfigyelt teszteredmények az elvárt eredmény irányába befolyásolják a folyamatot.

A tesztelési lépések és várt eredmények meghatározzák a TSFI-re alkalmazandó feladatokat és paramétereket, valamint, hogy a várt eredményeket milyen módon kell ellenőrizni és mik ezek az eredmények. Az értékelőnek meg kell állapítania, hogy a tesztelési lépések és várt eredmények összhangban vannak-e a funkcionális specifikáció TSFI leírásával. Ez azt jelenti, hogy a TSFI működés funkcionális specifikációban közvetlenül leírt minden jellemzőjéhez tartoznia kell tesztnek és várt eredménynek az adott működés ellenőrzése érdekében.

A tesztelési tevékenység fő célja annak megállapítása, hogy minden alrendszert, modult és TSFI-t kellőképpen leteszteltek a funkcionális specifikációban, TOE tervben és a biztonsági szerkezet leírásban megfogalmazott üzemeltetési elvárások szerint. A kiemelt garanciaszinten a tesztelés terhelés teszteket és negatív teszteket is tartalmaz. A tesztelési eljárások betekintést nyújtanak abba, hogy a fejlesztő a tesztelés során hogyan aktivizálta a TSFI-ket, modulokat és alrendszereket. Az értékelő ezt az információt felhasználja, amikor kiegészítő teszteket dolgoz ki a TSF független teszteléséhez.

6.2.5.4.2. Funkcionális tesztek: Az ATE_FUN.1 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztő vajon helyesen hajtotta végre és dokumentálta a tesztelési dokumentációban leírt teszteket.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) teszt dokumentáció.

Annak mértéke, hogy a tesztelési dokumentáció mennyire fedje le TSF-t, függ a lefedettség garanciális összetevőjétől.

A rendelkezésre bocsátott fejlesztői tesztekre az értékelőnek meg kell állapítania a tesztek megismételhetőségét, valamint azt, hogy a fejlesztői tesztek milyen mértékben használhatók az értékelő független teszteléséhez. Az értékelőnek minden olyan TSFI-t, amelyekre a fejlesztői teszt eredmények azt mutatják, hogy esetleg nem a specifikáltnak megfelelően hajtódnak végre, a megfelelőség vagy meg nem felelősség megállapítása érdekében független tesztelés alá kell vetnie.

6.2.5.4.2.1. Az ATE_FUN.1.1E értékelői akció

ATE_FUN.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ATE_FUN.1.1C A tesztelési dokumentációnak tartalmaznia kell a tesztelési terveket, az elvárt teszteredményeket és a tényleges teszteredményeket.

ATE_FUN.1-1 Az értékelőnek ellenőriznie kell, hogy a tesztelési dokumentáció tartalmazza-e a tesztelési terveket, az elvárt eredményeket és a tényleges teszt eredményeket.
Az értékelő ellenőrizze, hogy a tesztelési terveket, az elvárt eredményeket és a tényleges teszt eredményeket belefoglalták-e a tesztelési dokumentációba.

ATE_FUN.1.2C A tesztelési terveknek azonosítaniuk kell a végrehajtandó teszteket, és le kell írniuk minden teszt végrehajtásának forgatókönyvét. Ezen forgatókönyveknek tartalmazniuk kell a más tesztek eredményeitől való minden sorrendbeli függést.

ATE_FUN.1-2 Az értékelőnek ellenőriznie kell, hogy a tesztelési terv leírja-e minden teszt végrehajtásának forgatókönyvét.

Az értékelőnek meg kell állapítania, hogy a teszterv nyújt-e információkat a használt tesztkonfigurációra vonatkozóan: mind a TOE konfigurációra, mind pedig minden használt tesztberendezésre vonatkozóan. Ennek az információnak a tesztkonfiguráció reprodukálhatóságának biztosításához kellően részletesnek kell lennie.

Az értékelőnek azt is meg kell állapítania, hogy a teszterv nyújt-e információt arról, hogy hogyan kell végrehajtani a tesztet: az összes szükséges automatizált indítási eljárásról (és hogy ezek igényelnek-e futási jogosultságot), az alkalmazandó bemenetekről és ezek alkalmazásáról, hogyan lehet megkapni a kimenetet, valamennyi automatikus törlési eljárásról (és hogy ezek igényelnek-e futási jogosultságot), stb. Ennek az információnak a teszt reprodukálhatóságának biztosításához kellően részletesnek kell lennie.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ATE_FUN.1-3 Az értékelőnek meg kell vizsgálnia a tesztelési tervet annak megállapítása érdekében, hogy a TOE teszt konfigurációja megegyezik-e az ST-ben az értékelésre megadott konfigurációval.

A tesztelési tervben ugyanazt az egyedi hivatkozást kell alkalmazni a TOE-ra, mint amit a Konfiguráció kezelési képességek (ALC_CMC) altevékenységekben fektettek le, illetve amit az ST bevezetőjében azonosítottak.

Az ST egynél több konfigurációt is meghatározhat az értékeléshez. Az értékelő ellenőrizze, hogy a fejlesztő által a tesztelési dokumentációban azonosított összes teszt konfiguráció megfelel-e az ST-nek. Például az ST olyan kötelezően beállítandó konfigurációs lehetőségeket határozhat meg, amelyek befolyásolják, hogy a TOE milyen részekből álljon, belefoglalva vagy kizárva egyes részeket. Az értékelő ellenőrizze, hogy a TOE összes ilyen változatát figyelembe vették.

Az értékelő vegye figyelembe azokat az ST-ben leírt, a TOE üzemeltetési környezetére vonatkozó biztonsági céljait, amelyek a teszt környezetre alkalmazhatók. Lehet hogy néhány cél nem alkalmazható a teszt környezetre. Például egy a felhasználói engedélyekkel

kapcsolatos cél nem alkalmazható, míg a „csatlakozás a hálózathoz egyetlen ponton” alkalmazható.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ATE_FUN.1-4 Az értékelőnek meg kell vizsgálnia a tesztelési tervet annak megállapítása érdekében, hogy az elegendő utasítást tartalmaz-e a sorrendi függőségekre.

Bizonyos lépések végrehajtására szükség lehet a kezdeti feltételek kialakítása érdekében. Például a felhasználói fiókokat fel kell venni, mielőtt azokat törölni lehet. Egy példa a sorrendiségi függőségre: először azokat a tevékenységeket kell végrehajtani, melyek naplóbejegyzéseket állítanak elő, s csak ezt követően lehet a naplóbejegyzéseket kereső és rendező tesztekkel foglakozni. Másik példa a sorrendiségi függőségre: egyik teszteset állítja elő azt az adatállományt, amely egy másik teszt eset számára bemenetként szolgál.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ATE_FUN.1.3C Az elvárt teszteredményeknek be kell mutatniuk a tesztek sikeres végrehajtásából keletkező várható kimeneteket.

ATE_FUN.1-5 Az értékelőnek meg kell vizsgálnia a tesztelési dokumentációt annak megállapítása érdekében, hogy az tartalmazza-e az összes várt teszteredményt.

Az elvárt teszteredmények annak megállapításához szükségek, hogy egy tesztet sikeresen végrehajtottak-e vagy sem. Az elvárt teszteredmények akkor tekinthetők kielégítőnek, ha egyértelműek, és megfelelnek az adott tesztelési módszer alapján várt működésnek.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ATE_FUN.1.4C A tényleges teszteredményeknek összhangban kell állniuk az elvárt teszteredményekkel.

ATE_FUN.1-6 Az értékelőnek ellenőriznie kell, hogy a tesztelési dokumentációban szereplő várt teszteredmények összhangban állnak-e a tényleges teszteredményekkel.

A fejlesztő által átadott tényleges és várt teszteredmények összehasonlítása felfedi a két eredményhalmaz közötti különbségeket. Lehet, hogy a tényleges teszteredmények közvetlen összehasonlítása nem történhet meg bizonyos adatok egyszerűsítése vagy összevonása előtt. Ilyenkor a fejlesztői tesztelési dokumentációban ismertetni kell a tényleges adatokat egyszerűsítő vagy összevonó eljárásokat.

Például a fejlesztőnek tesztelnie kell egy üzenettár tartalmát egy hálózati kapcsolat után, az üzenettár tartalmának megállapítása érdekében. Az üzenettár egy bináris számot tartalmaz, amelyet valamilyen más adatmegjelenítési formába kell átalakítani az értelmezhetőség érdekében. A fejlesztőnek tehát le kell írnia az adat magas szintű ábrázolási formába történő átalakításának módját, hogy az értékelő is végre tudja azt hajtani (szinkron vagy aszinkron átvitel, stop bitek száma, paritás, stb.).

Megjegyzendő, hogy a tényleges adatok egyszerűsítő vagy összevonó folyamatának leírását az értékelő nem a szükséges módosítások tényleges elvégzésére használja, hanem a folyamat megfelelőségének értékelésére. A fejlesztő feladata az elvárt teszteredmények átalakítása olyan formára, amely könnyen összehasonlítható a tényleges teszteredményekkel.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ATE_FUN.1-7 Az értékelőnek jelentést kell készítenie a fejlesztő tesztelési munkájáról, áttekintést adva a tesztelési módszerről, konfigurációról, mélységről és eredményekről.

Az értékelési jelentésben rögzített fejlesztői tesztelésről szóló információ lehetővé teszi az értékelő számára, hogy bemutassa az általános tesztelési módszert és a fejlesztő által a TOE tesztelésébe fektetett munkát. A cél a fejlesztő tesztelési munkájának érdemi áttekintése. Nem cél, hogy az értékelési jelentésben a fejlesztői teszteléssel kapcsolatos információk a specifikus tesztlépések vagy egyedi tesztek eredményeinek pontos megismétlése legyenek. A cél elegendő részletesség biztosítása más értékelők és a tanúsító szervezet számára ahhoz, hogy betekintést kapjanak a fejlesztő tesztelési módszerébe, a végrehajtott tesztek nagyságrendjébe, a TOE teszt konfigurációjába és a fejlesztői tesztelés általános eredményébe.

Az értékelési jelentés fejlesztői tesztekről szóló részében általában az alábbi információk találhatók:

a) TOE teszt konfigurációk. A ténylegesen tesztelt TOE konfigurációk, köztük az, hogy a teszt felállítása vagy a tesztet követő rendteremtés igényelt-e külön jogosultságú kódot.
b) Tesztelési módszer. Az alkalmazott fejlesztői tesztelési stratégia áttekintése.
c) Tesztelési eredmények. A fejlesztői tesztelés eredményének áttekintő leírása.

E lista korántsem teljes, csupán megmutat néhány területet, melyeknek a fejlesztői teszteléssel kapcsolatosan az értékelési jelentésben szerepelni kell.

6.2.5.4.3. Lefedettség: Az ATE_COV.2 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztő letesztelte-e az összes TSFI-t, és hogy a fejlesztő teszt lefedettség elemzése szemlélteti-e a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikációban leírt TSFI-k közötti megfelelést.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) teszt dokumentáció,
d) tesz lefedettség elemzés.

6.2.5.4.3.1. Az ATE_COV.2.1E értékelői akció

ATE_COV.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ATE_COV.2.1C A teszt lefedettség elemzésének szemléltetnie kell a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikációban leírt TSFI-k közötti megfelelést.

ATE_COV.2-1 Az értékelőnek meg kell vizsgálnia a teszt lefedettség elemzését annak megállapítása érdekében, hogy a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikációban leírt interfészek közötti megfeleltetés pontos-e.

A megfeleltetés bemutatására egy egyszerű kereszt-táblázat is elegendő lehet. A teszt lefedettség elemzésben szereplő teszteket és interfészeket egyértelműen kell azonosítani.

Emlékeztetjük az értékelőt arra, hogy nem kell a tesztelési dokumentáció valamennyi tesztjét leképezni a funkcionális specifikációban leírt interfészekre.

ATE_COV.2-2 Az értékelőnek meg kell vizsgálnia a tesztelési tervet annak megállapítása érdekében, hogy a tesztelési módszer minden interfész esetén szemlélteti-e az adott interfész elvárt működését.

Ehhez a munkaegységhez útmutató található az alábbi alkalmazási megjegyzésekben:

a) 6.2.5.4.1.1, A TOE elvárt működésének megértése
b) 6.2.5.4.1.2, A tesztelés, illetve egyéb módszerek a funkcionalitás elvárt működésének ellenőrzésére

ATE_COV.2-3 Az értékelőnek meg kell vizsgálnia a teszt eljárásokat annak megállapítása érdekében, hogy a teszt előfeltételek, a tesztelési lépések és az elvárt eredmény(ek) megfelelően tesztelnek-e minden interfészt.

Ehhez a funkcionális specifikációra vonatkozó munkaegységhez útmutató található az alábbi alkalmazási megjegyzésben:

a) 6.2.5.4.1.3, A tesztek megfelelőségének ellenőrzése.

ATE_COV.2.2C A teszt lefedettség elemzésének szemléltetnie kell, hogy a funkcionális specifikációban leírt összes TSFI-t letesztelték.

ATE_COV.2-4 Az értékelőnek meg kell vizsgálnia a teszt lefedettség elemzését annak megállapítása érdekében, hogy a funkcionális specifikációban leírt interfészek és a tesztelési dokumentációban azonosított tesztek közötti megfeleltetés teljes-e.

A funkcionális specifikációban szereplő valamennyi TSFI-nek meg kell jelennie a teszt lefedettség elemzésében, és ezeket le kell képezni a tesztekre a teljesség kimutatása érdekében, az interfészek teljes körű specifikáció tesztelése ugyanakkor nem követelmény.

Nyilvánvalóan hiányos a lefedettség, ha a funkcionális specifikációban azonosított egyik interfészhez nem rendeltek tesztet.

Emlékeztetjük az értékelőt arra, hogy nem kell a tesztelési dokumentáció valamennyi tesztjét leképezni a funkcionális specifikációban leírt interfészekre.

6.2.5.4.4. Mélység: Az ATE_DPT.2 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztő letesztelte-e az összes TSF alrendszert és SFR-t érvényre juttató modult, a TOE tervnek és a biztonsági szerkezet leírásnak megfelelően.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) TOE terv,
d) biztonsági szerkezet leírása,
e) teszt dokumentáció,
f) tesz mélység elemzés.

6.2.5.4.4.1. Az ATE_DPT.2.1E értékelői akció

ATE_DPT.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ATE_DPT.2.1C A teszt mélység elemzésnek szemléltetnie kell a tesztelési dokumentációban azonosított tesztek és a TOE tervben szereplő TSF alrendszerek, illetve SFR-t érvényre juttató modulok közötti megfelelést.

ATE_DPT.2-1 Az értékelőnek meg kell vizsgálnia a teszt mélység elemzését annak megállapítása érdekében, hogy a tesztelési dokumentáció tartalmazza-e a TSF alrendszerek működésének és egymás közötti kapcsolódásaik leírását.

Ez a munkaegység ellenőrzi a tesztek és a TOE terv megfelelését. Amennyiben a TSF architektúrális helyességének leírása (az ADV_ARC biztonsági szerkezet leírás keretén belül) speciális mechanizmusokra hivatkozik, ez a munkaegység ellenőrzi a tesztek és az ilyen mechanizmusok üzemeltetési leírása közötti megfelelést is.

A megfeleltetés bemutatására egy egyszerű kereszt-táblázat is elegendő lehet. A teszt mélység elemzésben szereplő teszteket és a működéseket, kapcsolódásokat egyértelműen kell azonosítani.

Emlékeztetjük az értékelőt arra, hogy nem kell a tesztelési dokumentáció valamennyi tesztjét leképezni az alrendszerek működésének, illetve egymásra hatásuk leírására.

ATE_DPT.2-2 Az értékelőnek meg kell vizsgálnia a tesztelési tervet, a teszt előfeltételeket, a tesztelési lépéseket és az elvárt eredmény(eke)t annak megállapítása érdekében, hogy a működés leírás tesztelési módszere szemlélteti-e, hogy az alrendszerek működése megfelel-e a TOE tervben leírtaknak.

Ehhez a munkaegységhez útmutató található az alábbi alkalmazási megjegyzésekben:

a) 6.2.5.4.1.1, A TOE elvárt működésének megértése
b) 6.2.5.4.1.2, A tesztelés, illetve egyéb módszerek a funkcionalitás elvárt működésének ellenőrzésére

Amennyiben leírták a TSF alrendszerek interfészeit, az alrendszerek működésének tesztelése végrehajtható közvetlenül ezeken az interfészeken. Egyébként az alrendszerek működése a TSFI interfészeken tesztelendő. Az előzőek kombinációja is alkalmazható. Bármelyik módszert is választotta, az értékelőnek meg kell fontolnia, hogy az adott módszer alkalmas-e az alrendszerek TOE tervben leírt működésnek a tesztelésére.

ATE_DPT.2-3 Az értékelőnek meg kell vizsgálnia a tesztelési tervet, a teszt előfeltételeket, a tesztelési lépéseket és az elvárt eredmény(eke)t annak megállapítása érdekében, hogy a működés leírás tesztelési módszere szemlélteti-e, hogy az alrendszerek egymásra hatása megfelel-e a TOE tervben leírtaknak.

Amíg az előző munkaegység az alrendszerek működésével foglalkozik, ez a munkaegység az alrendszerek egymásra hatásával (az egymás közötti működéssel) foglalkozik.

Ehhez a munkaegységhez útmutató található az alábbi alkalmazási megjegyzésekben:

a) 6.2.5.4.1.1, A TOE elvárt működésének megértése
b) 6.2.5.4.1.2, A tesztelés, illetve egyéb módszerek a funkcionalitás elvárt működésének ellenőrzésére

Amennyiben leírták a TSF alrendszerek interfészeit, az alrendszerek közötti egymásra hatás tesztelése végrehajtható közvetlenül ezeken az interfészeken. Egyébként az alrendszerek közötti egymásra hatásra a TSFI interfészeken keresztül lehet következtetni. Bármelyik módszert is választotta, az értékelőnek meg kell fontolnia, hogy az adott módszer alkalmas-e az alrendszerek közötti, a TOE tervben leírt egymásra hatás tesztelésére.

ATE_DPT.2-4 Az értékelőnek meg kell vizsgálnia a teszt mélység elemzését annak megállapítása érdekében, hogy a tesztelési dokumentáció tartalmazza-e az SFR-t érvényre juttató modulok interfészeinek a leírását.

Ez a munkaegység ellenőrzi a tesztek és a TOE terv megfelelését. Amennyiben a TSF architektúrális helyességének leírása (az ADV_ARC biztonsági szerkezet leírás keretén belül) speciális, modul szintű mechanizmusokra hivatkozik, ez a munkaegység ellenőrzi a tesztek és az ilyen mechanizmusok üzemeltetési leírása közötti megfelelést is.

A megfeleltetés bemutatására egy egyszerű kereszt-táblázat is elegendő lehet. A teszt mélység elemzésben szereplő teszteket és a működéseket, kapcsolódásokat egyértelműen kell azonosítani.

Emlékeztetjük az értékelőt arra, hogy nem kell a tesztelési dokumentáció valamennyi tesztjét leképezni az alrendszerek működésének, illetve az egymásra hatásnak a leírására.

ATE_DPT.2-5 Az értékelőnek meg kell vizsgálnia a tesztelési tervet, a teszt előfeltételeket, a tesztelési lépéseket és az elvárt eredmény(eke)t annak megállapítása érdekében, hogy a tesztelési módszer minden SFR-t érvényre juttató modul interfészre szemlélteti-e az adott interfész elvárt működését.

Amíg az ATE_DPT.2-1 munkaegység az alrendszerek elvárt működésével foglalkozik, ez a munkaegység azokkal az SFR-t érvényre juttató modul interfészek működésével foglalkozik, melyeket az ATE_DPT.2-4 munkaegység fed le.

Ehhez a munkaegységhez útmutató található az alábbi alkalmazási megjegyzésekben:

a) 6.2.5.4.1.1, A TOE elvárt működésének megértése
b) 6.2.5.4.1.2, A tesztelés, illetve egyéb módszerek a funkcionalitás elvárt működésének ellenőrzésére

Egy interfész tesztelése végrehajtható közvetlenül ezen az interfészen, vagy egy külső interfészen, vagy az előzőek kombinációjával. Bármelyik módszert is választotta, az értékelőnek meg kell fontolnia, hogy az adott módszer alkalmas-e az interfészek tesztelésére. Az értékelő különösen azt állapítsa meg, hogy a belső interfészeken való tesztelésre van-e szükség, vagy ezek a belső interfészek megfelelően tesztelhetők (még ha közvetve is) a külső interfészek révén. Ennek eldöntése, csakúgy, mint a döntés indoklása az értékelő hatásköre.

ATE_DPT.2.2C A teszt mélység elemzésnek szemléltetnie kell, hogy a TOE tervben szereplő összes TSF alrendszert letesztelték.

ATE_DPT.2-6 Az értékelőnek meg kell vizsgálnia a teszt eljárásokat annak megállapítása érdekében, hogy a TSF alrendszerek működésének és egymásra hatásának minden leírását tesztelték-e.

Ez a munkaegység az ATE_DPT.2-1 munkaegység teljességét ellenőrzi. A TOE tervben szereplő valamennyi alrendszer működésére, illetve valamennyi alrendszerek egymásra hatására vonatkozó leírást tesztelni kell. Nyilvánvalóan hiányos a tesztelés mélysége, ha a TSF tervben azonosított egyik TSF alrendszer működésre, vagy alrendszerek egymásra hatására vonatkozó leíráshoz nem rendeltek tesztet.

Emlékeztetjük az értékelőt arra, hogy nem kell a tesztelési dokumentáció valamennyi tesztjét leképezni a TOE tervben leírt alrendszer interfészekre.

ATE_DPT.2.3C A teszt mélység elemzésnek szemléltetnie kell, hogy a TOE tervben szereplő SFR-t érvényre juttató modulokat letesztelték.

ATE_DPT.2-7 Az értékelőnek meg kell vizsgálnia a teszt eljárásokat annak megállapítása érdekében, hogy az SFR-t érvényre juttató modulok összes interfészét tesztelték-e.

Ez a munkaegység az ATE_DPT.2-4 munkaegység teljességét ellenőrzi. A TOE tervben szereplő SFR-t érvényre juttató modulok összes interfészét tesztelni kell. Nyilvánvalóan

hiányos a tesztelés mélysége, ha a TSF tervben azonosított egyik SFR-t érvényre juttató modul egyik interfészéhez nem rendeltek tesztet.

Emlékeztetjük az értékelőt arra, hogy nem kell a tesztelési dokumentáció valamennyi tesztjét leképezni a TOE tervben leírt SFR-t érvényre juttató modulok interfészeire.

6.2.5.4.5. Független tesztelés: Az ATE_IND.2 altevékenység értékelése

Ennek az altevékenységnek a célja a TSFI egy részhalmazának független tesztelésével annak megállapítása, hogy a TOE a terv dokumentációban előírt módon működik-e, valamint a fejlesztői tesztek megbízhatóságának ellenőrzése egy azokból vett minta végrehajtásával.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST,
b) funkcionális specifikáció,
c) TOE terv,
d) üzemeltetési felhasználói útmutató,
e) előkészítő felhasználói útmutató,
f) konfiguráció kezelés dokumentáció,
g) tesztelési dokumentáció,
h) a tesztelésre alkalmas TOE.

6.2.5.4.5.1. Az ATE_IND.2.1E értékelői akció

ATE_IND.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ATE_IND.2.1C A TOE-nek tesztelésre alkalmas állapotban kell lennie.

ATE_IND.2-1 Az értékelőnek meg kell vizsgálnia a TOE-t annak megállapítása érdekében, hogy a teszt konfiguráció megegyezik-e az ST-ben meghatározott, értékelés alatt álló konfigurációval.

A fejlesztő által biztosított és a teszt tervben azonosított TOE-nek ugyanazt az egyedi hivatkozást kell alkalmaznia, mint amit a „Konfiguráció kezelés képességei” (ALC_CMC) altevékenységekben fektettek le, illetve amit az ST bevezetőjében azonosítottak.

Az ST meghatározhat egynél több konfigurációt is az értékeléshez. A TOE több különálló hardver és szoftver elemből állhat, melyeket az ST-nek megfelelően kell tesztelni. Az értékelő ellenőrizze, hogy valamennyi teszt konfiguráció ellentmondás mentes-e az ST-vel.

Az értékelő vegye figyelembe azokat az ST-ben leírt, a TOE üzemeltetési környezetére vonatkozó biztonsági célokat, amelyek a teszt környezetre alkalmazhatók. Lehet hogy néhány cél nem alkalmazható a teszt környezetre. Például egy a felhasználói engedélyekkel kapcsolatos cél nem alkalmazható, míg a „csatlakozás a hálózathoz egyetlen ponton” alkalmazható.

Bármilyen tesztelési erőforrás (mérőműszer, elemző készülék) használatakor az értékelő felelőssége annak biztosítása, hogy ezek az erőforrások megfelelően hitelesítve legyenek.

ATE_IND.2-2 Az értékelőnek meg kell vizsgálnia a TOE-t annak megállapítása érdekében, hogy azt megfelelően telepítették-e, és ismert állapotban van-e.

Az értékelő a TOE állapotát többféle módon is megállapíthatja. Például az AGD_PRE.1 altevékenység értékelésének előzetes sikeres befejezése teljesíti ezt a munkaegységet, ha az értékelő még bizonyos abban, hogy a tesztelésre használt TOE-t megfelelően telepítették és ismert állapotban van. Amennyiben nem ez a helyzet, akkor az értékelőnek a fejlesztő eljárásait kell követnie a TOE telepítéséhez és indításához, kizárólag a rendelkezésére bocsátott útmutatókra támaszkodva.

Amennyiben az értékelőnek végre kell hajtania a telepítési lépéseket, mert a TOE ismeretlen állapotban van, akkor e munkaegység sikeres befejezése kielégítheti az AGD_PRE.1-5 munkaegységet is.

ATE_IND.2.2C A fejlesztőnek biztosítania kell a TSF fejlesztői funkcionális tesztelése során használt erőforrás-készlettel azonos eszközkészletet.

ATE_IND.2-3 Az értékelőnek meg kell vizsgálnia a fejlesztő által rendelkezésére bocsátott erőforrás-készletet annak megállapítása érdekében, hogy az azonos-e a TSF fejlesztői funkcionális tesztelése során alkalmazott erőforrásokkal.

A fejlesztő által használt erőforrás-készletet a fejlesztői tesztelési terv dokumentálja, az ATE_FUN funkcionális tesztelés családban meggondolt módon. Az erőforrás-készlet többek között felölelhet laboratóriumi hozzáférést és speciális teszt berendezéseket is. Azokat az erőforrásokat, melyek nem egyeznek meg a fejlesztő által használtakkal, azonossá kell tenni a teszteredményekre gyakorolt lehetséges hatásuk szerint.

6.2.5.4.5.2. Az ATE_IND.2.2E értékelői akció

ATE_IND.2.2E Az értékelőnek végre kell hajtania a tesztelési dokumentációban szereplő tesztek valamely részhalmazát (mintáját) a fejlesztői teszt eredmények ellenőrzése érdekében.

ATE_IND.2-4 Az értékelőnek el kell végeznie a tesztelést a fejlesztői tesztelési tervben és eljárásokban található tesztekből vett mintára.

E munkaegység célja, hogy az értékelő elegendő számú fejlesztői teszt végrehajtásával meggyőződjön a fejlesztői teszteredmények érvényességéről. A minta nagyságáról, és a mintát alkotó fejlesztői tesztekről az értékelő dönt (lásd 7.2.1).

Minden fejlesztői teszt visszavezethető speciális interfészekre. Ezért a mintát alkotó tesztek kiválasztásakor figyelembe vett tényezők hasonlóak az ATE_IND.2-6 munkaegységnél leírtakhoz. Ezen kívül az értékelő alkalmazhat véletlenszerű mintavételezési módszert is a fejlesztői tesztek kiválasztásához, mintába vételéhez.

ATE_IND.2-5 Az értékelőnek ellenőriznie kell, hogy a tényleges teszteredmények összhangban állnak-e az elvárt teszteredményekkel.

A tényleges és az elvárt teszteredmények közti különbségek az ellentmondás feloldására késztetik az értékelőt. Az értékelő által feltárt ellentmondást a fejlesztő is feloldhatja kielégítő magyarázattal vagy az eltérések feloldásával.

Amennyiben nincs kielégítő magyarázat vagy feloldás, akkor az értékelő kevésbé megbízhatónak ítélheti a fejlesztői tesztelést, és növelheti a tesztelési minta nagyságát. Annak megerősítése érdekében, hogy az ATE_IND.2-4 munkaegységben azonosított mintát megfelelően tesztelték, a fejlesztői tesztelésben talált hiányosságokat meg kell szüntetni, akár a fejlesztői tesztelés kijavításával, akár az értékelő által végzett új tesztekkel.

6.2.5.4.5.3. Az ATE_IND.2.3E értékelői akció

ATE_IND.2.3E Az értékelőnek tesztelnie kell a TSF interfészeinek egy részét annak megerősítése érdekében, hogy a TSF a specifikáltaknak megfelelően működik.

ATE_IND.2-6 Az értékelőnek meg kell terveznie egy tesztkészletet.

Az értékelő válassza ki a TOE-nek megfelelő tesztkészletet és tesztelési stratégiát. Egy lehetséges szélsőséges tesztelési stratégia szerint a tesztkészlet annyi interfészt tartalmaz, amennyi csak tesztelhető kevés szigorral. Egy másik lehetséges tesztelési stratégia, hogy a teszt néhány interfészre terjed ki azok fontossága szerint és ezeket igen alapos ellenőrzésnek vetik alá.

Az értékelő által követett tesztelési módszer általában e két szélsőséges eset közé esik. Az értékelőnek ajánlott az interfészek nagy részére legalább egy tesztet végrehajtania, de a tesztelésnek nem kell teljes körű specifikáció-tesztelésnek lennie.

Az értékelőnek a tesztelendő interfész részhalmaz kiválasztásakor az alábbi tényezőket kell figyelembe vennie:

a) A fejlesztői tesztelés bizonyítékai. Ez a következőkből áll: tesztelési dokumentáció, teszt lefedettség elemzés, teszt mélység elemzés. A fejlesztői teszt bizonyíték betekintést nyújt abba, hogy a fejlesztő a tesztelés során hogyan aktivizálta a biztonsági funkciókat. Az értékelő ezt az információt felhasználja a TOE független teszteléséhez szükséges új tesztek tervezésékor. Fokozottan át kell gondolnia a következőket:
   aa) Az interfészekre vonatkozó fejlesztői tesztelés bővítése. Az értékelő végrehajthat ugyanolyan típusú teszteket változó paraméterekkel az interfész szigorúbb tesztelése céljából.
   ab) Az interfészekre vonatkozó fejlesztői tesztelési stratégia kiegészítése. Az értékelő módosíthatja egy adott interfészeknél alkalmazott tesztelési módszert egy új tesztelési stratégiát alkalmazva.
b) Azon interfészek száma, melyekből a tesztkészlet készül. Amennyiben a TOE csak kis számú, viszonylag egyszerű interfészt tartalmaz, célszerű lehet az összes szigorú tesztelése. Más esetekben ez nem költség-hatékony módszer, ekkor mintavételezésre van szükség.

c) Az értékelési tevékenységek egyensúlyának fenntartása. A tesztelésbe fektetett értékelői munka álljon arányban a többi értékelési feladatba fektetett munkával.

Az értékelő válassza ki az interfészek részhalmazát. Ez a kiválasztás több tényezőtől függ, és e tényezők is hatást gyakorolnak a tesztkészlet méretére:

a) Az interfészek fejlesztői tesztelésének szigora. Azokat az interfészeket, melyekre az értékelő további tesztelés szükségességét állapítja meg, ajánlott a tesztkészletbe bevenni.
b) A fejlesztői teszteredmények. Amennyiben a fejlesztői teszteredmény kétséget támaszt az értékelőben egy interfész megfelelő megvalósításával kapcsolatban, az adott interfészt ajánlott a tesztkészletbe bevenni.
c) Az interfészek fontossága. Azokat az interfészeket, amelyek a többieknél fontosabbak, ajánlott a tesztkészletbe bevenni. A „fontosság" egyik jelentős tényezője a biztonsági jelentőség (az SFR-t érvényre juttató interfészek fontosabbak az SFR-t támogató interfészeknél, ezek pedig fontosabbak az SFR-be nem beavatkozó interfészeknél, lásd 6.2.5.1.2 ADV_FSP.4 alfejezet). A „fontosság" másik jelentős tényezője az adott interfészre képezhető SFR-ek száma (ahogyan azt az ADV-beli absztrakciós szintek közötti megfelelés azonosításakor meghatározzák).
d) Az interfészek bonyolultsága. A bonyolult megvalósítást igénylő interfészek bonyolult teszteket követelhetnek meg a fejlesztőktől és az értékelőktől, melyek súlyos, a költség-hatékonysággal ellentétes követelmények. Ugyanakkor a bonyolult interfészeknél nagyobb a hibákra bukkanás valószínűsége, így jó jelöltek lehetnek a tesztkészletbe. Az értékelőnek a fenti két ellentétes szempontot kell mérlegelnie.
e) Közvetett tesztelés. Egyes interfészek tesztelése gyakran más interfészek közvetett tesztelésével is jár, így ezek tesztkészletbe vétele maximalizálja a tesztelt interfészek számát (még ha csak közvetett módon is). Egyes interfészeket általában széleskörű biztonsági funkcionalitásra használnak, így egy hatékony tesztelési megközelítés ezeket megcélozza.
f) Az interfészek típusai (pl. programozott, parancs-soros, protokoll). Az értékelőnek a TOE által támogatott minden TOE által támogatott interfész típusból ajánlott bevennie teszteket.
g) Új vagy szokatlan megoldásokat használó interfészek. Amennyiben a TOE újszerű vagy szokatlan tulajdonságokat tartalmaz, melyek erős üzleti hangsúlyt kaphatnak, az ezeknek megfelelő interfészek is erős jelöltek a tesztelésre.

A fenti útmutató kiemeli a megfelelő tesztkészlet kiválasztási folyamata során figyelembe veendő tényezőket, de semmiképpen nem tekinthető teljesnek.

ATE_IND.2-7 Az értékelőnek el kell készítenie a tesztkészlethez a tesztelési dokumentációt, amely kellőképpen részletes a tesztek megismételhetősége érdekében.

A TSF elvárt működésének az ST-ből, a funkcionális specifikációból és a TOE tervből történő megértése után az értékelőnek meg kell határoznia az interfész tesztelésére leginkább alkalmas módot. Az értékelő különösen az alábbiakat vegye figyelembe:

a) a használni kívánt módszer, például egy külső vagy egy belső interfészt tesztelnek, esetleg egy alternatív teszt módszert (pl. különleges esetben kód vizsgálatot) alkalmaznak,

b) az interfész(ek), melye(ke)t a tesztelésnél és a válaszok megfigyelésénél használnak,
c) a teszteléshez szükséges kezdeti feltételek (például bármely szükséges különleges objektum vagy szubjektum, a szükséges biztonsági tulajdonságokkal),
d) a teszteléshez szükséges speciális berendezések, mely vagy egy interfész aktivizálásához (pl. csomag generátorok), vagy egy interfész megfigyeléséhez (pl. hálózati analizátorok) szükségesek.

Az értékelő tesztelhet úgy is minden interfészt, hogy teszt-esetek sorozatát használja, ahol az egyes teszt-eset az adott interfészt elvárt működésének egy különleges szempontját vizsgálja. Az értékelő tesztelési dokumentációjában ajánlott meghatározni a teszt származtatásokat, visszavezetve azokat az érintett interfész(ek)re.

ATE_IND.2-8 Az értékelőnek végre kell hajtani a tesztelést.

Az értékelő az elkészített tesztelési dokumentációt alapként használja a TOE tesztelésének végrehajtásához. Bár a végrehajtandó tesztelés alapja a tesztelési dokumentáció, az értékelő ad hoc is végezhet teszteket. A tesztelés során feltárt TOE viselkedés alapján az értékelő új teszteket is készíthet. Az új teszteket is le kell írni a dokumentációban.

ATE_IND.2-9 Az értékelőnek jelentésbe kell foglalnia a tesztkészletben szereplő tesztekről az alábbi információkat:
a) a tesztelendő interfész azonosítása;
b) a tesztekhez szükséges berendezések összekapcsolásához és beállításához tartozó utasítások;
c) a teszt előfeltételek kialakítására vonatkozó utasítások;
d) az interfész kiváltására (aktivizálására) vonatkozó utasítások;
e) az interfész működésének megfigyelésére vonatkozó utasítások;
f) az összes elvárt eredmény leírása, valamint a megfigyelt viselkedés és az elvárt eredmények összehasonlításához szükséges elemzések;
g) a tesztek lezárására és a TOE tesztelés utáni állapotának kialakítására vonatkozó utasítások;
h) tényleges teszteredmények.

A leírásnak olyan részletességűnek kell lennie, hogy egy másik értékelő képes legyen megismételni a teszteket és azonos eredményt kapjon. Míg a teszteredmények bizonyos részei eltérhetnek egymástól (pl. naplórekordok dátum és időbejegyzései), az általános eredménynek meg kell egyezni.

Lehetnek olyan esetek, amikor szükségtelen e munkaegységben minden információt megadni (például egy teszt tényleges eredménye nem követeli meg az elemzést, mielőtt az elvárt eredmények összehasonlítása nem történik meg). Ennek eldöntése és a döntés indoklása az értékelő hatásköre.

ATE_IND.2-10 Az értékelőnek ellenőriznie kell, hogy a tényleges teszteredmények megegyeznek-e az elvárt eredményekkel.

Bármilyen különbözőség az elvárt és tényleges eredmények között a TOE helytelen működését vagy a dokumentáció hibáját jelezheti. A nem várt tényleges eredmény a TOE

vagy a tesztelési dokumentáció javítását, esetleg a tesztek összeállításának módosítását, bizonyos tesztek megismétlését igényelheti. Ennek eldöntése és a döntés indoklása az értékelő hatásköre.

ATE_IND.2-11 Az értékelőnek az értékelési jelentésben le kell írnia az értékelői tesztelési munkát, áttekintést adva a tesztelési módszerről, konfigurációról, mélységről és eredményekről.

Az értékelési jelentésben rögzített értékelői tesztelésről szóló információ lehetővé teszi az értékelő számára, hogy bemutassa az általános tesztelési módszert és a tesztelésbe fektetett munkát. A cél a tesztelési munka érdemi áttekintése. Nem cél, hogy az értékelési jelentésben a teszteléssel kapcsolatos információk a specifikus tesztlépések vagy egyedi tesztek eredményeinek pontos megismétlése legyenek. A cél elegendő részletesség biztosítása más értékelők és a tanúsító szervezet számára ahhoz, hogy betekintést kapjanak a választott tesztelési módszerbe, az értékelő által végrehajtott tesztek nagyságrendjébe, a fejlesztő által végrehajtott tesztek nagyságrendjébe, a TOE teszt konfigurációjába és a tesztelés általános eredményébe.

Az értékelési jelentés értékelői tesztekről szóló részében általában az alábbi információk találhatók meg:

a) TOE teszt konfigurációk. A ténylegesen tesztelt TOE konfigurációk.
b) A kiválasztott tesztelési készlet (részhalmaz) nagysága. Az értékelés során tesztelt interfészek mennyisége és ennek indoklása.
c) A részhalmazt alkotó interfészek kiválasztásának szempontjai. Rövid állítások azokról a tényezőkről, melyeket figyelembe vettek az interfészek készletbe választása során.
d) A tesztelt interfészek. Rövid felsorolása a készletbe került interfészeknek.
e) A végrehajtott fejlesztői tesztek. Ezek mennyisége és a kiválasztásukhoz használt szempontok rövid leírása.
f) A tevékenység alapján hozott határozat. Az értékelés során végzett tesztelés eredményének általános elbírálása.

E lista korántsem teljes, csupán megmutat néhány területet, melyeket az értékelői teszteléssel kapcsolatosan az értékelési jelentésben ajánlott szerepeltetni.

6.2.5.5. A Sebezhetőség felmérés garanciaosztály (AVA) értékelése

A sebezhetőség felmérés tevékenység célja a TOE üzemeltetési környezetében lévő hibák vagy gyengeségek kihasználhatóságának megállapítása. Ez a megállapítás az értékelési bizonyíték vizsgálatán, valamint az értékelő által a nyilvánosan elérhető anyagokban való keresésen alapul, és az értékelő áthatolás tesztelése támogatja ezt.

A 7.3 melléklet részletes útmutatót biztosít a sebezhetőség vizsgálat általános fogalmairól és megközelítés módjáról.

6.2.5.5.1. Sebezhetőségi elemzés: Az AVA_VAN.3 altevékenység értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a TOE üzemeltetési környezetében vannak-e megemelt-alap támadó képességgel rendelkező támadók által kihasználható sebezhetőségek.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

e) ST,
f) funkcionális specifikáció,
g) TOE tervek,
h) biztonsági szerkezet leírása,
i)a megvalósítás kiválasztott részhalmaza,
j)az útmutató dokumentáció,
k) a tesztelésre alkalmas TOE,
l)nyilvánosan elérhető információk a lehetséges sebezhetőségek azonosításának támogatására.

Egyéb bemenet ehhez az altevékenységhez:

a) a lehetséges sebezhetőségekre és támadásokra vonatkozó aktuális, nyilvánosan elérhető információk (pl. egy tanúsító szervezettől).

Az értékelési tevékenységek lefolytatása során az értékelő meghatározhat problémás területeket is. Ezek a TOE bizonyítékoknak olyan speciális részei, amelyekkel kapcsolatban az értékelőnek fenntartásai vannak, bár a bizonyíték kielégíti a tevékenységre vonatkozó követelményeket, amelyhez a bizonyíték kapcsolódik. Például úgy tűnik, hogy egy bizonyos interfész specifikáció túlzottan bonyolult, és ennélfogva lehetséges, hogy hibázásra hajlamos vagy a TOE fejlesztése, vagy a TOE üzemelése közben. Nincs ugyan kézzelfogható lehetséges sebezhetőség, de további vizsgálat szükséges.

A lehetséges sebezhetőségek meghatározásának célirányos megközelítési módja az értékelési bizonyítékok olyan célú vizsgálata, amely bármely olyan lehetséges sebezhetőség megállapítására törekszik, amely a bizonyítékokban lévő információk alapján nyilvánvaló. Ez egy nem-strukturált vizsgálat, minthogy a megközelítési mód nincsen előre meghatározva. A célirányos sebezhetőség vizsgálatra vonatkozóan további útmutatás található a 7.3.2.2.2 pontban.

6.2.5.5.1.1. Az AVA_VAN.3.1E értékelői akció

AVA_VAN.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

AVA_VAN.3.1C A TOE-nak alkalmasnak kell lennie tesztelésre.

AVA_VAN.3-1 Az értékelőnek meg kell vizsgálnia a TOE-t annak megállapítása érdekében, hogy a teszt konfiguráció megegyezik-e az ST-ben meghatározott, értékelés alatt álló konfigurációval.

A fejlesztő által biztosított és a teszt tervben azonosított TOE-nek ugyanazt az egyedi hivatkozást kell alkalmaznia, mint amit a „Konfiguráció kezelés képességei” (ALC_CMC) altevékenységekben fektettek le, illetve amit az ST bevezetőjében azonosítottak.

Az ST meghatározhat egynél több konfigurációt is az értékeléshez. A TOE több különálló hardver és szoftver elemből állhat, melyeket az ST-nek megfelelően kell tesztelni. Az értékelő ellenőrizze, hogy valamennyi teszt konfiguráció ellentmondás mentes-e az ST-vel.

Az értékelő vegye figyelembe azokat az ST-ben leírt, a TOE üzemeltetési környezetére vonatkozó biztonsági célokat, amelyek a teszt környezetre alkalmazhatók. Lehet hogy néhány cél nem alkalmazható a teszt környezetre. Például egy a felhasználói engedélyekkel kapcsolatos cél nem alkalmazható, míg a „csatlakozás a hálózathoz egyetlen ponton” alkalmazható.

Bármilyen tesztelési erőforrás (mérőműszer, elemző készülék) használatakor az értékelő felelőssége annak biztosítása, hogy ezek az erőforrások megfelelően hitelesítve legyenek.

AVA_VAN.3-2 Az értékelőnek meg kell vizsgálnia a TOE-t annak megállapítása érdekében, hogy azt megfelelően telepítették-e, és ismert állapotban van-e.

Az értékelő a TOE állapotát többféle módon is megállapíthatja. Például az AGD_PRE.1 altevékenység értékelésének előzetes sikeres befejezése teljesíti ezt a munkaegységet, ha az értékelő még bizonyos abban, hogy a tesztelésre használt TOE-t megfelelően telepítették és ismert állapotban van. Amennyiben nem ez a helyzet, akkor az értékelőnek a fejlesztő eljárásait kell követnie a TOE telepítéséhez és indításához, kizárólag a rendelkezésére bocsátott útmutatókra támaszkodva.

Amennyiben az értékelőnek végre kell hajtania a telepítési lépéseket, mert a TOE ismeretlen állapotban van, akkor e munkaegység sikeres befejezése kielégítheti az AGD_PRE.1-5 munkaegységet is.

6.2.5.5.1.2. Az AVA_VAN.3.2E értékelői akció

AVA_VAN.3.2E Az értékelőnek egy keresést kell végrehajtania nyilvános forrásokban a TOE lehetséges sebezhetőségeinek azonosítása érdekében.

AVA_VAN.3-3 Az értékelőnek tanulmányoznia kell a nyilvánosan rendelkezésre álló információ forrásokat a TOE lehetséges sebezhetőségeinek a meghatározása céljából.

Az értékelő tanulmányozza a nyilvánosan rendelkezésre álló információ forrásokat, amelyek rendelkezésre állnak a TOE lehetséges sebezhetőségei meghatározásainak elősegítéséhez. Sokféle nyilvánosan rendelkezésre álló információ forrás létezik, amelyeket az értékelőnek ajánlatos figyelembe vennie, felhasználva a világhálón elérhető anyagokat, beleértve a következőket:

a) szakértői publikációk (folyóiratok, könyvek);
b) tanulmányok;
c) konferencia kiadványok.

Az értékelő ne korlátozza az általa figyelembevett nyilvánosan rendelkezésre álló információkat a fentiekre, hanem vegyen figyelembe bármely egyéb vonatkozó rendelkezésre álló információt.

Az értékelő az átadott bizonyítékok vizsgálata közben használja fel a nyilvános információkat abból a célból, hogy további vizsgálatokat végezzen lehetséges sebezhetőségek felkutatására. Ha az értékelő problémás területeket határozott meg, vegye figyelembe azokat a nyilvánosan rendelkezésre álló információkat, amelyek az adott problémás területre vonatkoznak.

Az olyan információk elérhetősége, amely azonnal rendelkezésre állhat egy támadó számára, s amely elősegíti támadások meghatározását és megkönnyíti a támadások hatékony végrehajtását, jelentősen megnövelheti egy adott támadó támadási lehetőségeit. A sebezhetőségi információk és kifinomult támadó eszközök hozzáférhetősége az Interneten nagyon valószínűvé teszi, hogy ezeket megpróbálják felhasználni a TOE lehetséges sebezhetőségeinek meghatározására és kihasználására. A modern kereső eszközök az ilyen információkat könnyen elérhetővé teszik az értékelő számára, és a publikált lehetséges sebezhetőségekkel, valamint a jól ismert általános támadásokkal szembeni ellenállóképesség költséghatékony módon meghatározható.

A nyilvánosan rendelkezésre álló információ keresése célirányosan azokra a forrásokra irányuljon, amelyek a TOE alapját képező termék fejlesztésében felhasznált technológiákra vonatkoznak. Az ilyen keresés terjedelme vegye figyelembe a következő tényezőket: a TOE típusa, az értékelő tapasztalatai ezzel a TOE típussal, a feltételezett támadó képesség és a rendelkezésre álló ADV bizonyíték szintje.

A meghatározási folyamat iteratív, ahol egy lehetséges sebezhetőség meghatározása egy másik problémás terület meghatározásához vezethet, amely további vizsgálatokat igényel.

Az értékelőnek jelentést kell készítenie arról, hogy mit tett a bizonyítékokban található lehetséges sebezhetőségek meghatározására. Az ilyen típusú keresésre azonban lehet, hogy az értékelő nem tudja a vizsgálat megkezdése előtt leírni a lehetséges sebezhetőségek meghatározására teendő lépéseket, mivel lehetséges, hogy a módszert a keresés során találtak alakítják.

Az értékelőnek jelentést kell készíteni a megvizsgált bizonyítékokról a lehetséges sebezhetőségekre irányuló keresés befejezésekor. A bizonyítékok kiválasztása származhat az értékelő által meghatározott olyan problémás területekből, amely a támadó által is feltehetően elérhető bizonyítékhoz kapcsolódik, vagy megfelelhet az értékelő által adott valamilyen más magyarázatnak.

6.2.5.5.1.3. Az AVA_VAN.3.3E értékelői akció

AVA_VAN.3.3E Az értékelőnek egy független sebezhetőség vizsgálatot kell végrehajtania a TOE-ra, az útmutató dokumentációt, funkcionális specifikációt, TOE tervet, a biztonsági szerkezet leírást és a megvalósítási reprezentációt használva, a TOE lehetséges sebezhetőségeinek azonosítása érdekében.

AVA_VAN.3-4 Az értékelőnek egy célirányos keresést kell folytatnia az ST-re, az útmutató dokumentációra, a funkcionális specifikációra, a TOE tervre, a biztonsági szerkezet leírásra és a megvalósítási reprezentációra abból a célból, hogy meghatározza a TOE-ban esetlegesen előforduló lehetséges sebezhetőségeket.

Hiba hipotézis módszer használata szükséges, amely a specifikációk, a fejlesztési és útmutató bizonyítékok vizsgálata után a TOE-ban lévő lehetséges sebezhetőségeket feltételezi, illetve ezzel kapcsolatos vizsgálódásokat folytat.

Az értékelő használja fel a TOE-val együtt leszállítandókból szerzett ismeretét a TOE tervére és működésére vonatkozóan, hiba hipotézis módszert alkalmazva, a TOE fejlesztésében, vagy specifikált üzemeltetési módjában lévő lehetséges hibák azonosítása céljából.

A biztonsági szerkezet leírás szolgáltatja a fejlesztő sebezhetőség vizsgálatát, minthogy ez dokumentálja, hogy a TSF hogyan védi saját magát a nem-megbízható szubjektumokkal szemben, és hogyan akadályozza meg a biztonságot érvényre juttató funkcionalitás megkerülését. Ennélfogva az értékelő építsen a TSF védelem megértésére, amelyet ezen bizonyíték vizsgálatából nyert, majd hasznosítsa ezt az egyéb fejlesztésre vonatkozó (ADV) bizonyítékokból nyert ismeretekben.

Az alkalmazott megközelítési módban a problémás területek az irányadók, amelyeket az értékelési tevékenységek során a bizonyítékok vizsgálata közben, illetve az értékelésre átadott fejlesztési és útmutató bizonyítékok reprezentatív mintájában való keresés közben határoztak meg.

A mintavételre vonatkozó útmutatáshoz lásd a 7.2.1 mellékletet. Az útmutató legyen figyelembe véve a részhalmaz kiválasztásakor, és legyenek megindokolva a következők:

a) a kiválasztáskor alkalmazott megközelítési mód;
b) arra vonatkozó alkalmasság, hogy a vizsgált bizonyíték támogatja az adott megközelítési módot.

A problémás területek vonatkozhatnak a biztonsági szerkezet leírásban részletezett speciális védelmi tulajdonságok kielégítőségére.

A sebezhetőség vizsgálat során figyelembevett bizonyítékot ahhoz a bizonyítékhoz lehet kapcsolni, amelyhez a támadó feltételezhetően képes hozzájutni. Például a fejlesztő védheti a TOE tervet és megvalósítási reprezentációt úgy, hogy feltételezi, hogy egy támadó számára az egyedüli hozzáférhető információ a (nyilvánosan rendelkezésre álló) funkcionális specifikáció és útmutató. Mivel ebben az esetben a TOE garanciális céljai biztosítják a TOE tervre és megvalósítási reprezentációra vonatkozó követelmények kielégítését, ezért ezeket a tervezési információkat az értékelő csak további problémás területek felkutatására használhatja.

Ugyanakkor, ha a forrás nyilvánosan elérhető, ésszerű feltételezni, hogy a támadó hozzájut a forráshoz, és felhasználja azt a TOE elleni támadási kísérleteiben. Ezért ekkor az értékelő vegye figyelembe ezt a forrást a célirányos vizsgálati megközelítési módnál.

A következők példákat mutatnak be a bizonyítékok figyelembe veendő részhalmazának kiválasztására:

a) A funkcionális specifikáció és a megvalósítási reprezentáció vizsgálata (mivel a funkcionális specifikáció nyújtja a támadók számára rendelkezésre álló interfészek részleteit, a megvalósítási reprezentáció pedig magában foglalja mindazokat a tervezési döntéseket, amelyeket az összes többi tervezési absztrakciónál tettek meg. Ennélfogva a TOE tervezési információkat a megvalósítási reprezentáció részének tekinthető).
b) Az értékeléshez átadott termék reprezentációk mindegyikében egy meghatározott információs részhalmaz vizsgálata.
c) Az értékeléshez átadott termék reprezentációk mindegyikében meghatározott SFR-ek lefedése.
d) Az értékeléshez átadott termék reprezentációk mindegyikének a vizsgálata, minden egyes termék reprezentációban különböző SFR-ek feltételezése mellett.
e) Az értékeléshez átadott bizonyítékok olyan vonatkozásainak a vizsgálata, amelyek azokkal az aktuális lehetséges sebezhetőségi információkkal vannak kapcsolatban, amelyekhez az értékelő hozzájutott (pl. a tanúsító szervezettől).

A lehetséges sebezhetőségek meghatározásának ez a módja arra szolgál, hogy a megközelítési mód rendezett és tervezett legyen; rendszert képezzen a vizsgálatokhoz. Az értékelőnek le kell írnia a használt módszert (abban az értelemben, hogy milyen bizonyítékot fog figyelembe venni), a bizonyítékban lévő vizsgálandó információt, azt a módot, ahogyan ezt az információt figyelembe kell venni, és a kialakítandó hipotézist.

A következők példákat mutatnak azokra a feltételezésekre, amelyeket egy hipotézis tehet:
a) hibásan megadott input feltételezése a támadók által elérhető külső interfészeknél;
b) a biztonsági szerkezet leírásban említett kulcsfontosságú mechanizmus vizsgálata olyan belső buffer túlcsordulás feltételezése mellett, amely a szétválasztás elromlásához vezethet;
c) kutatás a TOE megvalósítási reprezentációjában létrehozott olyan objektumok meghatározására, amelyeket nem ellenőriz teljes mértékben a TSF, és amelyeket egy támadó felhasználhat az SFR-ek aláaknázására.

Például az értékelő meghatározhatja, hogy a interfészek lehetséges gyenge pontok a TOE-ban, és egy olyan megközelítési módot használhat, hogy „a funkcionális specifikációban és TOE tervben megadott minden interfész specifikáció átvizsgálásra kerül a lehetséges sebezhetőség hipotézisek kialakításához”, majd folytathatja azzal, hogy megmagyarázza a hipotézisben használt módszereket.

A meghatározási folyamat iteratív, ahol egy lehetséges sebezhetőség meghatározása egy másik problémás terület meghatározásához vezethet, amely további vizsgálatokat igényel.

Az értékelőnek jelentést kell készíteni arról, hogy mit tett a bizonyítékokban található lehetséges sebezhetőségek meghatározására. Az ilyen típusú keresésre azonban lehet, hogy az értékelő nem tudja a vizsgálat megkezdése előtt leírni a lehetséges sebezhetőségek meghatározására teendő lépéseket, mivel a feldolgozási mód csak a keresés során találtak eredményeként alakul ki. Ilyen esetekben az értékelőnek a vizsgált bizonyítékokról a lehetséges sebezhetőségekre irányuló keresés befejezésekor kell jelentést készíteni. A bizonyítékok kiválasztása származhat az értékelő által meghatározott olyan problémás

területekből, amely a támadó által is feltehetően elérhető bizonyítékhoz kapcsolódik, vagy megfelelhet az értékelő által adott valamilyen más magyarázatnak.

Azoktól az SFR-ektől függően, amelyeket a TOE-nak teljesítenie kell az üzemeltetési környezetben, az értékelő független sebezhetőség vizsgálata vegye tekintetbe az összes alábbi általános sebezhetőség típust:

a) az értékelés alatt álló TOE típusára vonatkozó általános lehetséges sebezhetőségek, amint ilyeneket a tanúsító szervezet szolgáltathat;
b) megkerülés;
c) hamisítás;
d) közvetlen támadások;
e) megfigyelés;
f) helytelen használat/visszaélés.

A b) - f) tételeket részletesen magyarázza a 7.3 melléklet.

A biztonsági szerkezet leírást a fenti általános lehetséges sebezhetőségek szem előtt tartása mellett kell mérlegelni. Minden lehetséges sebezhetőséget mérlegelni kell azon lehetséges módok felkutatására, amelyekkel a TSF védelmet hatálytalanítani, a TSF-et aláaknázni lehet.

AVA_VAN.3-5 Az értékelőnek az ETR-ben rögzítenie kell a meghatározott lehetséges sebezhetőségeket, amelyek tesztelhetők, és a TOE üzemeltetési környezetében szóba jöhetnek.

Nem szükséges a lehetséges sebezhetőségek további mérlegelése, ha az értékelő azt állapítja meg, hogy az üzemeltetési környezetben meglévő IT vagy nem-IT intézkedések meggátolják a lehetséges sebezhetőségek kiaknázását az adott üzemeltetési környezetben. Például, ha a TOE-hoz való fizikai hozzáférés kizárólag a jogosult felhasználókra van korlátozva, akkor ez a hamisítás lehetséges sebezhetőségét eredményesen nem kihasználhatóvá teheti.

Az értékelőnek minden okot rögzítenie kell a lehetséges sebezhetőségek további mérlegelésből való kizárására, ha azt állapítja meg, hogy a lehetséges sebezhetőség nem kerülhet szóba az üzemeltetési környezetben. Egyéb esetekben az értékelőnek a lehetséges sebezhetőséget további mérlegelésre rögzítenie kell.

Az értékelőnek az ETR-ben meg kell adnia a TOE-val kapcsolatos, annak üzemeltetési környezetében felmerülő lehetséges sebezhetőségek listáját, mely az áthatolás tesztelési tevékenység bemeneteként használható.

6.2.5.5.1.4. Az AVA_VAN.3.4E értékelői akció

AVA_VAN.3.4E Az értékelőnek az azonosított lehetséges sebezhetőségek alapján áthatolás tesztelést kell végrehajtania, annak megállapítása érdekében, hogy a TOE ellenáll egy megemelt-alap támadó képességgel bíró támadó által végrehajtott támadásnak.

AVA_VAN.3-6 Az értékelőnek meg kell terveznie az áthatolás teszteket a lehetséges sebezhetőségekre irányuló független keresés alapján.

Az értékelőnek kellően fel kell készülnie az áthatolás tesztelésre annak megállapítása érdekében, hogy a TOE üzemeltetési környezetében mennyire érzékeny a nyilvános forrásokban való kereséssel azonosított lehetséges sebezhetőségekre. Az értékelőnek figyelembe kell vennie bármely harmadik féltől (pl. tanúsító szervezet) kapott, ismert lehetséges sebezhetőségre vonatkozó aktuális információt, valamint a más értékelői tevékenységek eredményeként talált lehetséges sebezhetőségeket is.

Az értékelőnek szem előtt kell tartania, hogy ugyanúgy, mint a biztonsági szerkezet leírás mérlegelése esetében a sebezhetőségek felkutatásánál (ahogyan az AVA_VAN.3-3-ben részletezve van), tesztelést kell végrehajtania a szerkezeti tulajdonságok megerősítésére. Mivel a kiemelt garanciaszint tartalmaz ATE_DPT-ből származó követelményeket, a fejlesztői tesztelési bizonyíték tartalmazni fog olyan tesztelést, amelyet a biztonsági szerkezet leírásban részletezett speciális mechanizmusok helyes működésének megerősítése céljából hajtottak végre. A fejlesztői fesztelés azonban nem szükségszerűen tartalmaz tesztelést a TSF védelmére szolgáló szerkezeti tulajdonságok minden vonatkozására, minthogy az ilyen tesztelések legtöbbje természetszerűen negatív tesztelés lesz, amely a tulajdonságok megcáfolását kísérli meg. Az áthatolás tesztelés stratégiájának kialakításakor az értékelőnek garantálnia kell, hogy a biztonsági szerkezet leírás minden vonatkozása tesztelésre kerüljön vagy a funkcionális tesztelésnél, vagy az értékelői áthatolás tesztelésnél.

Az áthatolás tesztelést valószínűleg tesztesetek sorozatával célszerű elvégezni, ahol az egyes tesztesetek egy-egy adott lehetséges sebezhetőséget próbálnak ki.

Az értékelőre nézve nem elvárás, hogy teszteket végezzen azokon a lehetséges sebezhetőségeken túl (beleértve a nyilvánosan ismerteket is), melyek kihasználásához legfeljebb megemelt-alap támadó képesség szükséges. Egyes esetekben azonban még a kihasználhatóság meghatározása előtt szükség lehet egy teszt végrehajtására. Amennyiben értékelői tapasztalata segítségével az értékelő egy közepes vagy magas támadó képességgel kihasználható sebezhetőséget tár fel, ezt az értékelési jelentésében maradvány sebezhetőségként szerepeltetnie kell.

Egy adott lehetséges sebezhetőség kihasználásához szükséges támadó képesség meghatározásához útmutató található a 7.3.4 pontban.

Az olyan lehetséges sebezhetőségek, melyek feltételezhetően csak közepes vagy magas támadó képességgel kihasználhatók, nem eredményeznek „nem felelt meg” eredményt erre az értékelői tevékenységre. Amennyiben vizsgálat támogatja a fenti feltételezést, az érintett lehetséges sebezhetőséget a továbbiakban nem szükséges az áthatolás tesztelés bemeneteként kezelni. Ugyanakkor az ilyen sebezhetőséget az értékelési jelentésben maradvány sebezhetőségként szerepeltetni kell.

Az olyan lehetséges sebezhetőségeket, melyek feltételezhetően alap vagy megemelt-alap támadó képességgel kihasználhatók, és a biztonsági célok megsértését eredményezik, a legnagyobb elsőbbséggel ajánlott a lehetséges sebezhetőségek azon listájára felvenni, mely alapján a TOE közvetlen áthatolás tesztelését végzik.

AVA_VAN.3-7 Az értékelőnek a lehetséges sebezhetőségek listáján alapulva el kell készítenie az áthatolás tesztelési dokumentációt, a tesztek megismételhetőségét lehetővé tévő részletességgel. A tesztelési dokumentációnak tartalmaznia kell az alábbiakat:

a) a lehetséges sebezhetőség azonosítását, melyre a TOE-t tesztelik;
b) az áthatolás teszteléshez szükséges minden tesztberendezés csatlakoztatását és beállítását előíró utasítást;
c) az áthatolás tesztelés összes kezdeti előfeltételét kialakító utasításokat;
d) a TSF működését kiváltó utasításokat;
e) a TSF viselkedése megfigyeléséhez szükséges utasításokat;
f) minden várható eredmény leírását, valamint a várható eredményekkel való összehasonlításhoz végrehajtandó, megfigyelt működésre vonatkozó elemzéseket;
g) a tesztek befejezéséhez szükséges és a TOE tesztelés utáni állapotát biztosító utasításokat.

Az értékelőnek a lehetséges sebezhetőségek listáján alapulva el kell készítenie az áthatolás tesztelési dokumentációt, a tesztek megismételhetőségét lehetővé tévő részletességgel.

Az értékelőre nézve nem elvárás, hogy meghatározza a kihasználhatóságát azon lehetséges sebezhetőségeknek, melyek hatásos támadásához közepes vagy magas támadó képesség szükséges. Ugyanakkor értékelői tapasztalata segítségével az értékelő feltárhat olyan lehetséges sebezhetőséget, melyet csak olyan támadó használhat ki, aki közepes vagy magas támadó képességgel rendelkezik. Az ilyen sebezhetőségeket az értékelési jelentésében maradvány sebezhetőségként szerepeltetni kell.

A lehetséges sebezhetőség ismeretében az értékelő határozza meg a leginkább megfelelő módot a TOE érzékenységének kimutatásához. Az értékelő különösen az alábbiakat vegye tekintetbe:

a) a TSFI és más TOE interfészeket, melyeket a TSF kiváltására és a válaszok megfigyelésére használnak (Lehet, hogy az értékelőnek egy TSFI-n kívüli TOE interfészt szükséges használnia a TOE azon tulajdonságainak demonstrálására, melyeket (az ADV_ARC által megkövetelt) biztonsági szerkezet leírás ír le. Megjegyzendő, hogy bár ezek a TOE interfészek lehetőséget adnak a TSF tulajdonságok tesztelésére, nem képezik tárgyát a tesztelésnek);
b) azokat a kezdeti feltételeket, melyek a tesztekhez szükségesek (azaz bármilyen szükséges objektum vagy szubjektum, illetve ezek szükséges biztonsági tulajdonságai);
c) speciális tesztberendezések, amelyek egy TSFI kiváltásához vagy megfigyeléséhez szükségesek (bár nem valószínű, hogy egy megemelt-alap támadó képességet feltételező lehetséges sebezhetőség speciális tesztberendezést igényel);
d) bár elméleti vizsgálat helyettesítheti a fizikai tesztelést, különösen fontos eset, amikor egy kezdeti teszt eredményeként előre jelezhető, hogy egy támadás adott számú megismétlése valószínűleg sikeres lesz.

Az értékelő az áthatolás tesztelést valószínűleg tesztesetek sorozatával találja célszerűnek elvégezni, ahol az egyes tesztesetek egy-egy adott lehetséges sebezhetőséget próbálnak ki.

A tesztelési dokumentáció ilyen szintű részletessége azt hivatott biztosítani, hogy más értékelők is meg tudják ismételni a teszteket, és azonos eredményre juthassanak.

AVA_VAN.3-8 Az értékelőnek végre kell hajtania az áthatolás tesztelést.

Az értékelő az AVA_VAN.3-6 munkaegység eredményeképpen létrejött áthatolás tesztelési dokumentációt a TOE áthatolás tesztelésének alapjaként használja, de ez nem zárja ki, hogy más, ad hoc áthatolás tesztelést ne végezhessen el. Amennyiben szükséges, az értékelő ad hoc teszteket is elvégezhet az áthatolás tesztelés során tapasztaltak következtében, melyeket – ha az értékelő elvégzi azokat - az áthatolás tesztelési dokumentációban rögzítenie kell. E tesztekkel szemben követelmény lehet, hogy a nem várt eredményeket vagy megfigyeléseket ellenőrizzék, vagy hogy a tesztelés előkészítési szakaszában az értékelőnek javasolt lehetséges sebezhetőségeket megvizsgálják.

Amennyiben az áthatolás tesztelés azt mutatja, hogy egy feltételezett lehetséges sebezhetőség nem létezik, az értékelőnek ajánlott megállapítania, hogy a saját elemzése volt téves, vagy az értékelésre átadandók voltak hibásak, hiányosak.

Az értékelőre nézve nem elvárás, hogy teszteket végezzen azokon a lehetséges sebezhetőségeken túl (beleértve a nyilvánosan ismerteket is), melyek kihasználásához legfeljebb megemelt-alap támadó képesség szükséges. Egyes esetekben azonban még a kihasználhatóság meghatározása előtt szükség lehet egy teszt végrehajtására. Amennyiben értékelői tapasztalata segítségével az értékelő egy közepes vagy magas támadó képességgel kihasználható sebezhetőséget tár fel, ezt az értékelési jelentésében maradvány sebezhetőségként szerepeltetnie kell.

AVA_VAN.3-9 Az értékelőnek rögzítenie kell az áthatolás tesztek tényleges eredményeit.
A tényleges eredmények bizonyos részletei különbözhetnek a várható értékektől (pl. idő és dátummezők a naplóban), de az összeredménynek meg kell egyeznie. Javasolt minden váratlan teszteredményt kivizsgálni, valamint ezek értékelésre gyakorolt hatását kimondani és igazolni.

AVA_VAN.3-10 Az értékelőnek az értékelési jelentés keretén belül jelentést kell írnia az értékelői áthatolás tesztelésről, leírván a tesztelési módszert, konfigurációt, mélységet és eredményeket.

Az értékelési jelentésben rögzített áthatolás tesztelésről szóló információ lehetővé teszi az értékelő számára, hogy bemutassa az általános tesztelési módszert és az ezen tevékenység végrehajtásába fektetett munkát. A cél az értékelő áthatolás tesztelési munkájának érdemi áttekintése. Nem cél, hogy az értékelési jelentésben az áthatolás teszteléssel kapcsolatos információk a specifikus tesztlépések vagy egyedi áthatolás tesztek eredményeinek pontos megismétlése legyenek. A cél elegendő részletesség biztosítása más értékelők és a tanúsító szervezet számára ahhoz, hogy betekintést kapjanak a választott áthatolás tesztelési módszerbe, a végrehajtott áthatolás tesztek nagyságrendjébe, a TOE teszt konfigurációjába és az áthatolás tesztelési tevékenység általános eredményébe.

Az értékelési jelentés értékelői áthatolás tesztelésről szóló része általában az alábbi információkat tartalmazza:

a) TOE tesztkonfigurációk; az áthatolás tesztelésnél használt konkrét TOE konfigurációk.

b) Az áthatolás teszt során tesztelt TSFI-k. Az áthatolás tesztelés középpontjában álló TSFI-k és egyéb TOE interfészek rövid felsorolása.
c) Az altevékenység alapján született határozat. Az áthatolás tesztelés eredményeinek általános megítélése.

E lista korántsem teljes, csupán felvillant néhány szempontot, melyeknek az értékelő áthatolás tesztelésével kapcsolatosan az értékelési jelentésben ajánlott szerepelniük.

AVA_VAN.3-11 Az értékelőnek meg kell vizsgálnia az összes áthatolás teszt eredményét annak megállapítása érdekében, hogy a TOE üzemeltetési környezetében ellenáll-e egy megemelt-alap támadó képességgel rendelkező támadónak.

Amennyiben az eredmények azt mutatják, hogy a TOE üzemeltetési környezetében kihasználható sebezhetőségeket tartalmaz alap vagy megemelt-alap támadó képességgel rendelkező támadók számára, akkor ez az értékelői akció "Nem felelt meg" határozatot eredményez.

A 7.3.4 mellékletet kell használni egy adott sebezhetőség kihasználásához szükséges támadó képesség meghatározásához, illetve annak eldöntésére, hogy a sebezhetőség a tervezett üzemeltetési környezetben kihasználható-e. Nem feltétlenül kell minden esetben kiszámolni a támadó képességet, csak ha felmerül annak lehetősége, hogy egy alap vagy megemelt-alap támadó képességgel rendelkező támadó kihasználhatja a sebezhetőséget.

AVA_VAN.3-12 Az értékelőnek az értékelési jelentés keretén belül jelentést kell írnia az összes kihasználható sebezhetőségről és maradvány sebezhetőségről, az alábbi adatokkal:
a) forrás (pl. azon CEM tevékenység, melynek végrehajtása során észlelték, az értékelő ismerte, szakirodalomban olvasott róla);
b) a nem kielégített SFR(-ek);
c) leírás;
d) kihasználható-e vagy sem az üzemeltetési környezetben (vagyis kihasználható vagy maradvány sebezhetőségről van szó);
e) az azonosított sebezhetőség kihasználáshoz szükséges felhasznált idő, szakértelem, TOE ismeret, hozzáférési lehetőség, eszköz, valamint az ezekhez rendelt értékek a 7.3.4 melléklet 8. és 9. táblázata alapján.

7. Mellékletek

7.1. Általános fejlesztői útmutató

7.1.1. A CC funkcionális követelmények szerkezete

7.1.1.1. Osztálystruktúra

Minden funkcionális osztály tartalmazza az osztály nevét, az osztály bemutatását és egy vagy több funkcionális családot.

Az osztálynév alfejezet olyan információt biztosít, amely a funkcionális osztály meghatározásához és kategorizálásához szükséges. Minden funkcionális osztálynak egyedi neve van. A kategóriainformáció egy három karakteres rövid névből áll. Az osztály rövid neve az adott osztály rövid családneveinek meghatározására használható.

Az osztálybemutatás kifejezi a családoknak azt az általános szándékát vagy megközelítési módját, hogy a család eleget tegyen a biztonsági céloknak. A funkcionális osztályok meghatározása nem tükröz semmilyen, a követelmények specifikációjában található formális taxonómiát. Az osztálybemutatásban található ábra leírja az osztályban található családokat és minden, a család összetevőin belüli hierarchiát.

7.1.1.2. Családszerkezet

Minden család tartalmazza a család nevét, a családi viselkedést, az összetevő szintekre osztását, az irányítási követelményeket és a naplózási követelményeket

A családnév alfejezet a család meghatározásához és kategorizálásához szükséges információkat biztosít. Minden család egyedi névvel rendelkezik. A kategorikus információ egy hét karakterből álló rövid nevet tartalmaz, amelyből az első három megegyezik az osztály rövid nevével, ezt egy alsó kötőjel követ, majd a család rövid neve, pl.: XXX_YYY. A családnévnek ez az egyedi, rövid alakja biztosítja az összetevő fő hivatkozási nevét.

A családi viselkedés a funkcionális család narratív bemutatása, amely meghatározza a biztonsági célt és a funkcionális követelmények általános leírását.

Az összetevő szintekre osztása bemutatja a családban elérhető összetevőket és azok áttekintő magyarázatát.

Az irányítási követelmények a PP/ST szerzői számára irányítási tevékenységekként tartalmaznak információt egy megadott összetevőhöz. Az irányítási követelményeket az FMT osztály összetevői részletezik.

A naplózási követelmények a PP/ST szerzők számára kiválasztható naplózási eseményeket tartalmazzák.

7.1.1.3. Összetevő szerkezet

Minden összetevő tartalmazza az alábbiakat: összetevő-azonosítás, funkcionális elemek, függések.

Az összetevő-azonosítás rész leíró információkkal szolgál, amelyek az összetevő azonosításához, kategorizálásához, regisztrálásához és kereszthivatkozásokhoz szükségesek. A funkcionális összetevők részeként meghatározásra kerül egy egyedi név (amely tükrözi az összetevő célját), valamint egy rövid név.

Minden összetevőhöz létezik egy sor funkcionális elem. Minden elem önálló és külön került meghatározásra. A funkcionális elem egy tovább már nem bontható, elemi biztonsági funkcionális követelmény.

Függés akkor jelentkezik a funkcionális összetevők között, ha egy összetevő nem önálló, és egy másik összetevő funkcionalitására vagy az azzal való kölcsönhatásra van utalva a saját helyes működésének fenntartása érdekében.

7.1.2. CC műveletek

A CC összetevőket pontosan úgy lehet használni, ahogyan a CC-ben le vannak írva, vagy megengedett műveletek használatával átszabhatók. A műveletek alkalmazásánál a PP/ST szerzőknek ügyelniük kell arra, hogy az adott követelménytől függő többi követelmény függőségi igényei teljesüljenek. A megengedett műveletek az alábbiak lehetnek:

a) **ismétlés**, amely megengedi, hogy egy összetevőt változó működéssel többször használjunk,
b) **értékadás**, amely megengedi a paraméterek meghatározását,
c) **kiválasztás**, amely megengedi, hogy egy listából egy vagy több elemet meghatározzunk,
d) **finomítás**, amely megengedi részletek hozzáadását.

Az ismétlés és finomítás műveletek minden összetevőre alkalmazhatók. Az értékadás és kiválasztás csak azokra az összetevőre alkalmazhatók, melyek ezt külön jelzik.

7.1.3. Védelmi profil (PP) megfelelés

7.1.3.1. Bevezetés

A PP-ket arra szánták, hogy „sablon”-ként szolgáljanak az ST-khez. Vagyis: a PP ismertet egy felhasználói igény halmazt, míg egy ST, amely megfelel ennek a PP-nek, leír egy TOE-t, amely kielégíti a szóbanforgó igényeket.

Meg kell jegyezni, hogy lehetséges az is, hogy egy PP-t egy másik PP-hez használják sablonként Ez az eset teljesen hasonló az ST/PP esethez. Az áttekinthetőség kedvéért ez a fejezet csak az ST/PP esetet írja le, de érvényes a PP esetre is.

Ez a melléklet leírja, hogy mit jelent egy ST PP-nek való megfelelése. A CC kétféle megfelelés típust ismer:

a) ***szigorú megfelelőség***: nagyon szigorú összefüggés áll fenn a PP és az ST között. Ezt az összefüggést nagyjából úgy lehet megfogalmazni, hogy “az ST-nek tartalmaznia kell minden állítást, ami benne van a PP-ben, de tartalmazhat többet”. A szigorú megfelelőséget várhatóan olyan szigorú követelmények esetében fogják használni, amelyeket pontosan be kell tartani egyedi módon;
b) ***kimutatható megfelelőség***: nincsen részhalmaz-bennfoglaló halmaz típusú összefüggés a PP és az ST között. A PP és az ST tartalmazhat teljesen eltérő

állításokat, amelyek különböző entitásokat tárgyalnak, különböző elgondolásokat használnak, stb. Azonban az ST-nek tartalmaznia kell indoklásokat arra, hogy az ST miért tekinthető "azonosnak vagy még jobban korlátozónak", mint a PP. A kimutatható megfelelőség lehetővé teszi, hogy egy PP szerzője általános megoldandó biztonsági feladatokat írjon le, és általános irányelveket adjon meg a feladatok megoldásához szükséges követelményekhez, annak tudatában, hogy feltehetően több módja van egy megoldás megadásnak. A kimutatható megfelelőség az olyan TOE típusoknál is alkalmazható, ahol már több hasonló PP létezik (vagy feltehetően létezni fog a jövőben), így megengedett, hogy az ST szerzője kijelentse, hogy az ST megfelel mindezen PP-knek egyszerre, és ezáltal munkát takarítson meg.

A megfelelőségnek a megengedett típusát a PP határozza meg. Vagyis a PP kijelenti (a PP megfelelőségi nyilatkozatban), hogy milyen típusú megfelelőség van megengedve az ST-k számára:

a) ha a PP kijelenti, hogy szigorú megfelelőség van megkövetelve, akkor az ST-nek kötelezően szigorú módon kell megfelelnie az ST-nek;
b) ha a PP kijelenti, hogy kimutatható megfelelőség van megkövetelve, akkor az ST-nek szigorú vagy kimutatható módon kell megfelelnie az ST-nek;

Más szavakkal megfogalmazva, egy ST számára csak akkor megengedett, hogy kimutatható módon feleljen meg egy PP-nek, ha a PP közvetlenül megengedi ezt.

Ha egy ST több PP-nek való megfelelőséget állít, akkor az ST-nek meg kell felelnie (a fentebb leírtak szerint) minden egyes PP-nek olyan módon, ahogy az egyes PP-k azt előírják. Ez azt jelenti, hogy az ST megfelelhet bizonyos PP-knek szigorúan, más PP-knek pedig kimutathatóan.

Meg kell jegyezni, hogy az ST vagy megfelel egy PP-nek, vagy nem. A CC nem ismer el „részleges" megfelelőséget. Ennélfogva a PP szerzőjének a felelőssége, hogy biztosítsa, hogy a PP nem túlzottan terhes, ami meggátolná a PP/ST szerzőket abban, hogy a PP-nek való megfelelőséget kijelentsék.

7.1.3.2. Szigorú megfelelőség

a) **Biztonsági probléma meghatározás**: az ST-nek tartalmaznia kell a PP-ben megadott biztonsági probléma meghatározást, és specifikálhat további veszélyeket és OSP-ket, de nem specifikálhat további feltételezéseket.
b) **Biztonsági célok**: Az ST:
   ba) tartalmaznia kell a PP-ben megadott, a TOE-ra vonatkozó minden biztonsági célt, és specifikálhat a TOE-ra további biztonsági célokat;
   bb) tartalmaznia kell az üzemeltetési környezetre megadott minden biztonsági célt (egyetlen kivétellel, amit a következő tétel ad meg), de nem specifikálhat további biztonsági célokat az üzemeltetési környezetre;
   bc) specifikálhatja azt, hogy bizonyos célok, amelyeket a PP az üzemeltetési környezetre ír elő, az ST-ben a TOE-ra vonatkozó biztonsági célok. Ezt nevezik a biztonsági cél áthelyezésének.

c) **Biztonsági követelmények:** Az ST-nek tartalmaznia kell a PP-ben megadott minden SFR-et és SAR-t, de kijelenthet további, vagy hierarchikusan erősebb SFR-eket és SAR-okat. Az ST-ben a műveletek elvégzésének összhangban kell lenni a PP-beliekkel; vagy ugyanúgy kell elvégezni egy műveletet, mint a PP-ben, vagy pedig úgy, hogy a követelmény legyen jobban korlátozó (a pontosítás szabályait alkalmazva).

Meg kell jegyezni, hogy bizonyos esetekben lehetséges, hogy a PP szerzője nem akarja, hogy az üzemeltetési környezetre vonatkozó bizonyos vagy összes cél át legyen helyezve a TOE céljai közé. Ebben az esetben ezt ki kell jelenteni a PP-ben.

Meg kell jegyezni azt is, hogy a veszélyek, az OSP-k, a feltételezések és a biztonsági célok olyan szóhasználattal is újra fogalmazhatók, amely sokkal megszokottabb az ST használói számára egy meghatározott ST esetében (pl. egy orvosi rendszerre vonatkozó ST használhat olyan fogalmakat, mint „orvosok”, „orvosi asszisztensek”, „kórházi adminisztrátorok”, még akkor is, ha az ST egy általánosabb PP-nek való megfelelőséget állít, amely olyan szavakat használ, mint „tisztviselők”, „beosztottak” és „adminisztrációs személyzet”). Ebben az esetben a megfelelőség indoklásának az ST-ben ki kell mutatnia kell a különböző szóhasználatok egyenértékűségét.

7.1.3.3. Kimutatható megfelelőség

A kimutatható megfelelőség a PP szerzőjéhez igazodik, aki bizonyítékokat vár el arra, hogy az ST egy megfelelő megoldás a PP által leírt általános biztonsági feladatra. Míg a szigorú megfelelőség esetében egy jól látható részhalmaz-bennfoglaló halmaz típusú összefüggés áll fenn a PP és az ST között, egy kimutatható megfelelőség esetében a kapcsolat kevésbé világos. Az általános megállapítás az, hogy az ST-nek azonosan vagy jobban korlátozónak kell lennie, mint a PP. Egy ST „megegyező vagy szigorúbb”, mint a PP, ha:

a) minden olyan TOE, amely megfelel a PP-nek, megfelel az ST-nek is, és
b) minden olyan üzemeltetési környezet, amely megfelel az ST-nek, megfelel a PP-nek is;

vagy, informálisan, az ST-nek ugyanazokat a megszorításokat vagy még többet kell kirónia a TOE-ra, és ugyanazokat a megszorításokat vagy kevesebbet a TOE üzemeltetési környezetére.

Ez az általános kijelentés speciálisabban is kimondható az ST különböző fejezeteire:

a) **Biztonsági probléma meghatározás:** Az ST-ben a megfelelőség indoklásának szemléltetnie kell, hogy az ST-beli biztonsági probléma meghatározás „megegyező vagy szigorúbb”, mint a PP-beli biztonsági feladat meghatározás. Ez azt jelenti, hogy:
   aa) minden TOE, amely megfelel az ST-ben megadott biztonsági probléma meghatározásnak, megfelel a PP-ben megadott biztonsági probléma meghatározásnak is;
   ab) minden üzemeltetési környezet, amely megfelel a PP-ben megadott biztonsági probléma meghatározásnak, megfelel az ST-ben megadott biztonsági feladat meghatározásnak is.

b) **Biztonsági célok:** Az ST-ben a megfelelőség indoklásának szemléltetnie kell, hogy az ST-beli biztonsági célok „megegyező vagy szigorúbb”, mint a PP-beli biztonsági célok. Ez azt jelenti, hogy:
   ba) minden TOE, amely kielégíti az ST-ben megadott, TOE-ra vonatkozó biztonsági célokat, kielégíti a PP-ben megadott, TOE-ra vonatkozó biztonsági célokat is;
   bb) minden üzemeltetési környezet, amely kielégíti a PP-ben megadott, üzemeltetési környezetre vonatkozó biztonsági célokat, kielégíti az ST-ben megadott, üzemeltetési környezetre vonatkozó biztonsági célokat is.
c) **SFR-ek:** Az ST-ben a megfelelőség indoklásának szemléltetnie kell, hogy az ST-beli SFR-ek „megegyező vagy szigorúbb”, mint a PP-beli SFR-ek. Ez azt jelenti, hogy minden TOE, amely kielégíti az ST-ben megadott SFR-eket, kielégíti a PP-ben megadott SFR-eket is.
d) **SAR-ok:** Az ST-nek tartalmaznia kell a PP-ben megadott minden SAR-t, de kijelenthet további, vagy hierarchikusan erősebb SAR-okat is. Az ST-ben a műveletek elvégzésének összhangban kell lenni a PP-beliekkel; vagy ugyanúgy kell elvégezni egy műveletet, mint a PP-ben, vagy pedig úgy, hogy a követelmény legyen jobban korlátozó (a pontosítás szabályait alkalmazva).

7.2. Általános értékelési útmutató

Ennek a mellékletnek a célja az értékelési eredmények műszaki bizonyítékainak biztosítására használható általános útmutatás. Az általános útmutatás az értékelő által végrehajtott munka objektivitását, megismételhetőségét és újraelőállíthatóságát segíti elérni.
Mintavételezés
Az alábbiak a mintavételezéshez adnak általános útmutatót. Részletesebb és speciális javaslatokat azok a munkaegységek tartalmaznak speciális értékelői akcióelemeikben, melyek során mintavételezést kell végezni.

A mintavétel az értékelő által végzett olyan meghatározott eljárás, melynek során az értékelési bizonyíték megkívánt készletének csak egy részhalmazát vizsgálják, és ezt a teljes készlet tekintetében reprezentatívnak tételezik fel. Ez lehetővé teszi az értékelő számára, hogy a teljes bizonyíték elemzése nélkül elegendő bizonyosságot szerezzen az adott értékelési bizonyíték helyességéről. A mintavétel célja az erőforrásokkal való takarékosság, a garancia megfelelő szintjének fenntartásával. A bizonyíték mintavétele két lehetséges következménnyel járhat:

a) A részhalmaz nem fed fel hibát, így az értékelő valamilyen szintű bizonyosságot szerezhet arra, hogy a teljes készlet is helyes.
b) A részhalmaz hibákat tár fel, ezáltal a teljes készlet helyessége megkérdőjeleződik.

Még az összes megtalált hiba kijavítása is kevésnek bizonyulhat ahhoz, hogy az értékelő elégséges bizonyosságot szerezzen a helyességről, ezáltal lehet, hogy meg kell növelnie a részhalmaz méretét, vagy pedig abba kell hagynia a mintavétel használatát az adott bizonyíték vonatkozásában.

A mintavétel olyan módszer, mely megbízható eredményt szolgáltat, ha a bizonyíték készlete viszonylag homogén jellegű, például ha a bizonyítékot egy jól meghatározott folyamat során állították elő.

A mintavétel CC-ben meghatározott esetei, valamint a CEM munkaegységekbe foglalt esetei az értékelői akciók végrehajtásának költség-hatékony megközelítésének tekinthető. Más esetekben a mintavétel csak kivételes esetben megengedett, ha egy adott tevékenység a maga teljességében a többi értékelési tevékenységhez képest aránytalanul nagy munkát igényelne, és ez a többletmunka nem adna az elvégzendő munkának megfelelő garanciát. Az ilyen esetekben az értékelőnek az értékelési jelentésben meg kell indokolnia az adott területen történő mintavétel alkalmazást. Nem elég magyarázat, hogy az értékelés tárgya nagy és összetett, vagy hogy nagyon sok funkcionális biztonsági követelménye van, hiszen egy nagy és bonyolult értékelés tárgya várhatóan mindenképp nagy értékelői munkát igényel. A kivételek inkább csak olyan esetek lehetnek, melyeknél a TOE fejlesztési megközelítése egy adott CC követelményre nagy mennyiségű anyagot jelent, melynek egészét le kellene ellenőrizni vagy át kellene vizsgálni, de ez a teljes körű elemzés várhatóan nem emelné ennek megfelelő mértékben a garanciát.

A mintavételt indokolni kell a TOE-ra vonatkozó biztonsági célokra és veszélyekre való lehetséges hatás tükrében. A hatás attól függ, hogy a mintavétel révén mi maradhat ki a vizsgálatból. Figyelembe kell venni a mintavétel alapjául szolgáló bizonyíték jellegét is, továbbá az is követelmény, hogy egyetlen biztonsági funkció sem maradhat ki vagy gyengülhet a mintavétel miatt.

TOE megvalósításához közvetlenül kötődő bizonyítékok (pl. fejlesztői teszteredmények) mintavétele eltérő megközelítést igényel, mint az a mintavétel, amikor egy folyamat helyes működését kell megállapítani. Sok esetben az értékelőnek azt kell megállapítania, hogy egy folyamatnak megfelelően helyesen járnak-e el, és javasolt-e mintavételezési módszer alkalmazása. Az ekkor alkalmazott módszer különbözik a fejlesztői tesztek eredményének mintavételétől, hiszen a folyamatok esetén a folyamat meglétét, megtörténtét nézik, míg a másik eset az értékelés tárgya helyes megvalósításával foglalkozik. Általában nagyobb mintaméretre van szükség a TOE helyes megvalósításának elemzésekor, mint egy folyamat megtörténtének ellenőrzésekor.

Bizonyos esetekben helyes lehet, ha az értékelő nagyobb hangsúlyt fektet a fejlesztői tesztek megismétlésére. Például, ha a független tesztek, amelyeknek végrehajtása az értékelőre van bízva, csak kiterjedésben térnének el azoktól, mint ami a fejlesztő széleskörű teszt-halmazában benne van (feltehetően azért, mert a fejlesztő több tesztelést hajtott végre, mint ami szükséges a Lefedettség (ATE_COV) és Mélység (ATE_DPT) szempontokhoz), akkor helyes lehet, ha az értékelő nagyobb hangsúlyt fektet a fejlesztői tesztek megismétlésére. Meg kell jegyezni, hogy ez nem szükségszerűen vonja maga után, hogy a fejlesztői teszteket nagy százalékban kell megismételni; egy széleskörű fejlesztői teszt-halmazt feltételezve, az értékelő számára alkalmas lehet egy alacsony százalékú minta igazolása is.

Azokban az esetekben, amikor a fejlesztő automatizált teszt-készletet használt a funkcionális tesztelés végrehajtására, általában könnyebb lesz az értékelő számára, ha nem csak a fejlesztői tesztek egy mintáját, hanem a teljes teszt-készletet ismétli meg. Annak az ellenőrzése azonban kötelező az értékelő számára, hogy az automatikus tesztelés nem adott-e megtévesztő

eredményeket. Ebből következik, hogy ezt az ellenőrzést feltétlenül végre kell hajtani az automatikus teszt-készlet egy mintájára, s így ebben az esetben mindkét alábbi elv alkalmazásra kerül: tesztek kiválasztása (mintavételezés), illetve megfelelő méretű minta.

A mintavétel végrehajtása során az alábbi elveket kell követni:

a) A mintát nem véletlenszerűen, hanem a teljes bizonyítékra nézve reprezentatív módon kell kiválasztani. A minta méretét és összetételét mindig indokolni kell.
b) Amikor a mintavétel a TOE helyes megvalósításával kapcsolatos, a mintának reprezentatívnak kell lennie minden olyan szempontból, mely lényeges a mintavétel alapjául szolgáló terület számára. A kiválasztásnak különösen a különböző komponenseket, interfészeket, fejlesztői és üzemi telephelyeket (ha több ilyen van) és hardver platform típusokat (ha több is van) kell lefednie. A minta méretének arányban kell állnia az értékelés költségeivel, és a TOE-tól függő számos tényezőt kell figyelembe venni a mintavétel során (pl. a TOE nagysága és összetettsége, a dokumentáció nagysága).
c) Amikor a mintavétel a fejlesztői tesztelés megismételhetőségével és újraelőállíthatóságával kapcsolatos, a mintának elegendőnek kell lennie a fejlesztői tesztelés minden különböző szempontjának, így a különböző teszt előírások megjelenítéséhez. A mintának elegendőnek kell lennie a fejlesztő funkcionális tesztelési folyamatának minden esetleges szisztematikus hibájának észleléséhez. Annak az értékelői közreműködésnek, mely a fejlesztői tesztek megismétlésének és független tesztek végrehajtásának kombinációja, elegendőnek kell lennie ahhoz, hogy lefedje a TOE-re vonatkozó jelentősebb részeket.
d) Amikor a mintavétel folyamattal kapcsolatos (pl. látogatók felügyelete vagy terv átvizsgálás) az értékelőnek elegendő információt kell mintavételeznie ahhoz, hogy hitelt érdemlően meggyőződjön az eljárás betartásáról.
e) Az értékelés megbízójának és a fejlesztőnek nem szabad értesülnie előre a minta pontos kialakításáról, feltéve, hogy biztosított a minta és a kiegészítő átadandó elemek időben történő rendelkezésre bocsátása, például a tesztberendezések értékelőhöz szállítása az értékelési ütemtervnek megfelelően.
f) A mintát a lehető legnagyobb mértékben elfogulatlanul kell kiválasztani (pl. nem szabad mindig az első vagy az utolsó tételt választani). Ideális esetben a minta kiválasztását nem is az értékelő, hanem egy más személy végzi.

A mintában talált hibák szisztematikus, illetve szórványos jellegűként kategorizálhatók. Szisztematikus hiba esetén a problémát ki kell javítani, és teljesen új mintát kell venni. Megfelelően megvitatott, megmagyarázott szórványos hibák kijavíthatók új minta nélkül is, bár a magyarázatot meg kell erősíteni. Az értékelőnek el kell döntenie, hogy növeli-e a minta méretét vagy egy eltérő mintát használ-e.

7.2.1. Függőségek kezelése

Az elvárt értékelői tevékenységek, altevékenységek és akciók általában bármilyen sorrendben vagy párhuzamosan is végezhetők. Léteznek azonban különböző olyan függési viszonyok, melyeket az értékelőnek figyelembe kell vennie. Ez az alfejezet a különböző tevékenységek, altevékenységek és akciók közötti függőségekre vonatkozóan ad általános útmutatást.

7.2.1.1. A tevékenységek közötti függőségek

Bizonyos esetekben a különböző garanciaosztályok a kapcsolódó tevékenységekhez kötött sorrendet ajánlhatnak, vagy akár meg is követelhetnek. Ilyen az ST értékelési tevékenysége. Ezt minden más TOE-vel kapcsolatos értékelési tevékenység előtt el kell kezdeni, mivel az ST biztosítja az alapot és teremti meg a többi tevékenység számára a hátteret, környezetet. Ugyanakkor lehetséges, hogy az ST értékelés végső határozata nem hozható meg a TOE teljes értékeléséig, hiszen az ennek során nyert tapasztalatok akár az ST módosítását is szükségessé tehetik.

7.2.1.2. Az altevékenységek közötti függőségek

Az értékelőnek figyelembe kell vennie a CC 3. részének összetevői közötti függőségeket. A legtöbb függőség egyirányú, pl. AVA_VAN.1 értékelési altevékenység függőséget nyilvánít ki az ADV_FSP.1 és AGD_OPE.1 értékelési altevékenységektől. Vannak példák kölcsönös függőségre is, amikor mindkét összetevő függ egymástól. Erre vonatkozó példa az ATE_FUN.1 és az ATE_COV.1 értékelési altevékenységek.

Egy altevékenységhez általában csak akkor lehet “Megfelelt” határozatot rendelni, ha minden olyan altevékenység sikeresen lezárult, amelytől a szóban forgó altevékenység egyirányú függőségben áll. Például az AVA_VAN.1 értékelési altevékenységhez csak akkor lehet “Megfelelt” határozatot rendelni, ha az ADV_FSP.1 és az AGD_OPE.1 értékelési altevékenységekhez már szintén “Megfelelt” határozatot hoztak. A kölcsönös függőség esetén az értékelőre van bízva, hogy melyik altevékenységet hajtja végre először. Megfelelt” határozat azonban általában csak akkor hozható, ha mindkét altevékenység sikeresen befejeződött.

Annak megállapításakor, hogy egy altevékenység hatással van-e egy másik altevékenységre, az értékelőnek figyelembe kell vennie azt, hogy ezen altevékenység függ-e bármely más altevékenység lehetséges értékelési eredményétől. Lehet olyan eset, amikor egy függőséget okozó altevékenység befolyásolja az adott altevékenységet, és már korábban befejezett értékelői feladat ismételt végrehajtását igényli.

Jelentős függési hatás lép fel az értékelő által felfedezett hibák esetén. Amennyiben egy hibát egy altevékenység végrehajtásának eredményeként azonosítanak, akkor egy ettől függő altevékenységhez nem hozható “Megfelelt” határozat mindaddig, amíg ki nem javították a függőséget okozó altevékenységhez kapcsolódó összes hibát.

7.2.1.3. Az akciók közötti függőségek

Előfordulnak olyan esetek, amikor az egyik akció végrehajtása során kapott eredményt az értékelő egy másik akcióban is felhasználja. Például a teljességgel és ellentmondás mentességgel kapcsolatos akciók nem fejezhetők be mindaddig, amíg az értékelő nem fejezi be a tartalomra és megjelenítésre vonatkozó ellenőrzéseket. Ennek alapján ajánlott például, hogy az értékelő az ST indoklásának értékelését csak az ST alkotórészeinek az értékelése után végezze el.

7.2.2. Helyszíni szemlék

7.2.2.1. Bevezetés

Az ALC garanciaosztály követelményeket tartalmaz a következőkre:

a) konfiguráció kezelés alkalmazása, ami biztosítja, hogy a TOE sértetlensége fennmarad;
b) a TOE biztonságos szállításával kapcsolatos intézkedések, eljárások és szabványok, amelyek biztosítják, hogy a TOE által nyújtott biztonsági védelem nem kerül veszélybe a felhasználóhoz való kiszállítás közben;
c) a fejlesztői környezet védelmére szolgáló biztonsági intézkedések.

A fejlesztői helyszín meglátogatása hasznos eszköz, amelyen keresztül az értékelő megállapítja, hogy az eljárásokat követik-e a dokumentációban leírtakkal összhangban álló módon.

A telephely látogatások okai magukban foglalják a következőket:

a) a CM rendszer használatának megfigyelése, ahogyan azt a CM terv leírja;
b) a szállítási eljárások gyakorlati alkalmazásának megfigyelése, ahogyan azt a szállítási dokumentáció leírja;
c) a biztonsági intézkedések alkalmazásának megfigyelése a TOE fejlesztése és kezelése során, ahogyan azt a fejlesztés biztonsági dokumentáció leírja.

Speciális és részletes információt adnak az olyan tevékenységekre vonatkozó munkaegységek, amelyeknél telephely látogatásokat hajtanak végre:

a) CM képességek (ALC_CMC).n n>=3 esetén (mégpedig az ALC_CMC.3-10 = ALC_CMC.4-13 munkaegység);
b) Szállítás (ALC_DEL) (az ALC_DEL.1–2 munkaegység);
c) A fejlesztés biztonsága (ALC_DVS) (mégpedig az ALC_DVS.1-3 munkaegység).

7.2.2.2. Általános megközelítés

Egy értékelés során gyakran szükséges, hogy az értékelő egynél többször találkozzon a fejlesztővel, és jó szervezés kérdése, hogy a telephely meglátogatását másik találkozóval társítsák a költségek csökkentése érdekében. Például össze lehet társítani a konfiguráció kezelés, a fejlesztés biztonság és a szállítás megfigyelésére szolgáló telephely látogatásokat. Szükség lehet arra is, hogy ugyanazt a telephelyet egynél többször meglátogassák, hogy ellenőrizni lehessen minden fejlesztési fázist. Az is figyelembe veendő, hogy a fejlesztés történhet több létesítményben egyetlen épületen belül, több épületen belül ugyanazon a telephelyen, vagy több telephelyen.

Az első telephely látogatás legyen az értékelés kezdeti szakaszára ütemezve. Abban az esetben, ha egy értékelés a TOE fejlesztési szakaszában kezdődik, akkor ez szükség esetén hibajavító akciókat fog lehetővé tenni. Abban az esetben, ha egy értékelés a TOE fejlesztése után kezdődik, egy korai telephely látogatás lehetővé teheti hibajavító intézkedések beiktatását, ha az alkalmazott eljárásokban súlyos hiányosságok merülnek fel. Ezzel el lehet kerülni felesleges értékelési erőfeszítéseket.

A megbeszélések ugyancsak hasznos eszközök annak megállapítására, hogy a leírt eljárások tükrözik-e az elvégzett tevékenységeket. Az ilyen megbeszélések során az értékelő arra törekszik, hogy mélyebb megértést szerezzen a vizsgált eljárásokról a fejlesztés helyszínén, arról, hogy ezeket hogyan alkalmazzák a gyakorlatban, és hogy ezeket úgy alkalmazzák-e, ahogyan az átadott értékelési bizonyítékok leírják. Az ilyen megbeszélések kiegészítik, de nem helyettesítik az értékelési bizonyítékok vizsgálatát.

A telephely látogatások előkészítésének első lépéseként az értékelők az ALC garanciaosztályt érintő munkaegységeket hajtsák végre, kivéve a telephely látogatás eredményeinek leírását. A fejlesztői dokumentáció által nyújtott információkon és a dokumentációban meg nem válaszolt nyitott kérdéseken alapulva az értékelő állítson össze egy ellenőrző listát azokból a kérdésekből, amelyeket a telephely látogatásnak kell tisztáznia.

Az ALC osztályra vonatkozó értékelési jelentés első verziója és az ellenőrző lista bemenetként szolgál a tanúsító szervezettel folytatott, telephely látogatásokra vonatkozó konzultációhoz.

Az ellenőrző lista vezérfonalként szolgál a telephely látogatásokhoz, hogy milyen kérdéseket kell megválaszolni a vonatkozó intézkedések, ezek alkalmazásának és eredményeinek a megszemlélésén és a megbeszéléseken keresztül. A megkívánt garanciaszint eléréséhez mintavételezés is használható (lásd 7.2.1).

A telephely látogatások eredményei rögzítésre kerülnek, és bemenetként szolgálnak az ALC osztályra vonatkozó értékelési jelentés végleges verziójához.

Egyéb megközelítési módok is mérlegelendők a bizonyosság megszerzéséhez, amelyek a garancia azonos szintjét biztosítják (pl. az értékelési bizonyítékok vizsgálata). A látogatás során nem meghozott döntéseket a tanúsító szervezettel folytatott konzultációval kell meghozni. A megfelelő biztonsági szempontok és módszertan alapuljon az informatikai biztonsági irányítási rendszerek területének egyéb szabványain.

7.2.2.3. Ellenőrzési lista készítésre vonatkozó útmutatás

A következők néhány kulcsszót adnak meg arra, hogy milyen témák legyenek ellenőrizve egy audit során.

7.2.2.3.1. A konfiguráció kezelés szempontja

Alap

- A konfiguráció lista elemei, beleértve a TOE-t, a forráskódot, a futásidejű könyvtárakat, a tervezési dokumentációt, a fejlesztő eszközöket (ALC_CMC.3-8).
- A tervezési dokumentáció, forráskód, felhasználói dokumentáció nyomon követése a TOE különböző verzióihoz.
- A konfiguráció rendszer beépítése a tervbe és a fejlesztési eljárásba, a teszt tervezés, a teszt vizsgálat és a minőségkezelési eljárások.

Tesztvizsgálat
- A teszt tervek és eredmények nyomon követése a TOE speciális konfigurációihoz és verzióihoz.

A fejlesztési rendszerhez való hozzáférés ellenőrzése
- A hozzáférés ellenőrzésre és naplózásra vonatkozó szabályzatok.
- A hozzáférési jogok projekt-specifikus kijelölésére és megváltoztatására vonatkozó szabályzatok.

Engedélyezés
- A TOE és az üzemeltetési felhasználói útmutató fogyasztó számára történő engedélyezésre vonatkozó szabályzatok.
- A TOE és komponensei használat előtti tesztelésére és jóváhagyására vonatkozó szabályzatok.

7.2.2.3.2. A fejlesztés biztonság szempontja

Infrastruktúra
- Biztonsági intézkedések a fejlesztési helyszínre való fizikai bejutás ellenőrzésére és az adott intézkedések hatékonyságának magyarázata.

Szervezeti intézkedések
- A cég szervezeti intézkedései a fejlesztési környezet biztonságát illetően.
- Szervezeti szétválasztás a fejlesztés, előállítás, tesztelés és minőségbiztosítás között.

Személyzeti intézkedések
- A személyzet képzésére vonatkozó intézkedések a fejlesztés biztonságát illetően.
- Intézkedések és jogi megállapodások a belső információk illetéktelen felfedés elleni védelméről.

Hozzáférés ellenőrzés
- Védett objektumok kijelölése (például TOE, forráskód, futásidejű könyvtárak, tervezési dokumentáció, fejlesztő eszközök, felhasználói dokumentáció) és biztonsági szabályzatok.
- A hozzáférés ellenőrzéssel és a hitelesítési információk kezelésével kapcsolatos szabályzatok és felelősségek.
- A fejlesztési helyszínhez való mindenfajta hozzáférés naplózására és a naplóadatok védelmére vonatkozó szabályzatok.

Adatok bemenete, feldolgozása és kimenete
- Biztonsági intézkedések a kimenet és a kimeneti eszközök (printer, plotter, képernyők) védelmére.
- A helyi hálózatok és kommunikációs kapcsolatok védelme.

Dokumentumok és adathordozók tárolása, továbbítása és megsemmisítése.
- A dokumentumok és adathordozók kezelésére vonatkozó szabályzatok.
- Leselejtezett dokumentumok megsemmisítésére és az ilyen események naplózására vonatkozó szabályzatok és felelősségek.

Adatvédelem
- — Az adat és információvédelemre (pl. háttérmentések végrehajtása) vonatkozó szabályzatok és felelősségek.

Katasztrófaterv
- — A vészhelyzetben folytatandó gyakorlat és felelősségek.
- — A vészhelyzeti intézkedések dokumentációja a hozzáférés ellenőrzést illetően.
- — A személyzet tájékoztatása a különleges esetekben alkalmazandó gyakorlatról, védelemről (pl. háttérmentések végrehajtása).

7.2.2.3.3. Példa ellenőrzési listára

A telephely látogatások ellenőrző listáira vonatkozó példák audit előkészítési táblázatokból és az audit eredményeinek bemutatására szolgáló táblázatokból állnak.

Az ellenőrző lista három részre van osztva a bevezetésben (7.2.3.1) jelzett témaköröknek megfelelően.

a) Konfiguráció kezelés rendszer.
b) Szállítási eljárások.
c) Biztonsági intézkedések a fejlesztés során.

Ezek a részek megfelelnek az ALC garancia osztálynak, mégpedig az ALC_CMC.n (CM képességek) n>=3 mellett, az ALC_DEL (Szállítás) és az ALC_DVS (A fejlesztés biztonsága) családoknak.

Ezek a részek sorokra vannak tovább osztva a CEM vonatkozó munkaegységeinek megfelelően.

Az ellenőrző lista oszlopai rendre a következőket tartalmazzák:
- — folyamatos sorszám,
- — a hivatkozott munkaegység,
- — hivatkozások a megfelelő fejlesztői dokumentációra,
- — a fejlesztői intézkedések közvetlen újraelőállítása,
- — speciális megjegyzések és kérdések, amelyeket a látogatás során kell tisztázni (azon a szokásos értékelői feladaton túlmenően, hogy ellenőrizni kell a jelzett intézkedések alkalmazását),
- — a látogatás során végzett vizsgálatok eredményei.

Ha úgy döntenek, hogy külön ellenőrzőlista készül az audit előkészítésre és az audit jelentésre, akkor az eredmény oszlop kimarad az előkészítési listából és a megjegyzések és kérdések oszlop kimarad a jelentés listából. A többi oszlop legyen azonos mindkét listában.

6. táblázat: Példa ellenőrző listára kiemelt garanciaszinten (kivonat)

A. A konfiguráció kezelés rendszer vizsgálata (ALC_CMC.4 és ALC_CMS.4)					
sor-szám	munkaegység	fejlesztői dokumentáció	intézkedések	Kérdések és megjegyzések	eredmény

A.1	ALC_CMC.4-11	Konfiguráció kezelés dokumentáció	A rendszer automatikusan kezeli a forrás kód állományokat.A rendszer képes felhasználói profilok és különböző hozzáférési jogosultságok adminisztrálására, valamint a felhasználók azonosságának és jogosultságának az ellenőrzésére	A forrás kód állomány olvasása vagy módosítása igényel-e felhasználói hitelesítést?	Amennyiben egy felhasználónak nincs hozzáférési jogosultsága egy bizalmas dokumentumhoz , akkor a fájl listában az meg sem jelenik számára.
…	…				
B. A szállítási eljárások vizsgálata (ALC_DEL.1)					
B.1	ALC_DEL.1-1 ALC_DEL.1-2	Szállítási dokumentáció	A szoftver PGP-vel titkosítva és aláírva, elektronikusan továbbítódik a felhasználóhoz	---	Az értékelő ellenőrizte a folyamatot, s a leírtaknak megfelelőket tapasztalt, kiegészítve azzal, hogy egy ellenőrző összeg is továbbítódik.
…	…				
C. A szervezeti és infrastrukturális fejlesztés biztonság vizsgálata (ALC_DVC.1, ALC_LCD.1 és ALC_TAT.1)					
C.1	ALC_DVS.1-1 ALC_DVS.1-2	Fejlesztés biztonsági dokumentáció (környezet)	A helyszínt kerítés védi.	A kerítés megfelelően erős és magas a könnyű behatolás meg-akadályozására?	A kerítés kellően erős és magas.
C.2	ALC_DVS.1-1 ALC_DVS.1-2	Fejlesztés biztonsági dokumentáció (épület)	Az épületbe a következő bejutások vannak: Főbejárat, melyet porta felügyel, szolgálaton kívül pedig zárva van, illetve egy teherbejáró, melyet dupla legördülő ajtórács véd.	A bejutási módok listája teljes?	A jelzett bejutási lehetőségeken túl van egy vészkijárat is, mely kívülről nem nyitható. Az említett legördülő ajtórács is csak belülről nyitható.
…	…				

7.3. Útmutató a sebezhetőség vizsgálathoz

Ez a melléklet magyarázatot nyújt az AVA_VAN garanciacsalád szempontjaihoz, és példákat ad meg ezek alkalmazására. Két fő részből áll:

a) Útmutató egy független sebezhetőség vizsgálat végrehajtásához. Ez a 7.3.1 alfejezetben van összegezve, részletesebben pedig a 7.3.2 alfejezetben van leírva. Ezek a fejezetek ismertetik, hogy egy értékelő hogyan közelítse meg a független sebezhetőség vizsgálat felépítését.

b) Egy támadó feltételezett támadó képességének jellemzése és kezelése. Ezt a 7.3.3 - 7.3.5-ig alfejezetek ismertetik, példa leírást adva egy támadó képesség jellemzésére és kezelésére.

7.3.1. Mi a sebezhetőség vizsgálat

A sebezhetőség elemzés értékelési tevékenység célja annak megállapítása, hogy a TOE üzemeltetési környezetében van-e kihasználható hiba vagy gyengeség. A megállapítás az értékelő által végzett elemzésre épül, s az értékelő tesztelése támogatja.

A sebezhetőség elemzés (AVA_VAN) legalacsonyabb szintjén az értékelő egy egyszerű keresést hajt végre a nyilvánosan elérhető információkra, hogy azonosítsa a TOE-ban az ismert sebezhetőségeket, míg a magasabb szinteken az értékelő egy strukturált elemzést hajt végre a TOE értékelői bizonyítékaira.

A sebezhetőség elemzés végrehajtásának két fő tényezője van, nevezetesen:
a) a lehetséges sebezhetőségek azonosítása,
b) áthatolás tesztelés annak megállapítása érdekében, hogy a lehetséges sebezhetőségek kihasználhatók-e a TOE üzemeltetési környezetében.

A sebezhetőségek azonosítása tovább bontható a bizonyítékok keresésére, valamint arra, hogy milyen nehéz ezeknek a bizonyítékoknak a keresése a lehetséges sebezhetőségek azonosítására. Hasonló módon az áthatolás tesztelés is felbontható egyrészt a támadási módszerek azonosításra irányuló lehetséges sebezhetőségek vizsgálatára, másrészt a támadási módszerek szemléltetésére.

A két tényező természeténél fogva iteratív, pl. a lehetséges sebezhetőségek áthatolás tesztelése további lehetséges sebezhetőségek azonosításához vezethet. Ezért ezeket egy egységes sebezhetőség vizsgálat tevékenység keretében hajtják végre.

7.3.2. Az értékelő által végzett sebezhetőség vizsgálat

Az értékelői sebezhetőség vizsgálat célja annak megállapítása, hogy a TOE ellenáll-e azoknak az áthatolás támadásoknak, amelyeket egy olyan támadó hajt végre, aki alap (az AVA_VAN.1 és AVA_VAN.2 esetén), megemelt-alap (az AVA_VAN.3 esetén), közepes (az AVA_VAN.4 esetén) vagy magas (az AVA_VAN.5 esetén) támadó képességgel rendelkezik. (A jelen dokumentumban meghatározott értékelési módszertan AVA_VAN.1 – AVA_VAN.3 garancia-összetevőket tartalmazza.) Az értékelő először mérje fel az összes azonosított lehetséges sebezhetőség kiaknázhatóságát. Ez elvégezhető áthatolás tesztelés végrehajtásával. Az értékelő tételezzen fel egy olyan támadói szerepkört, amely rendelkezik alap (az AVA_VAN.1 és AVA_VAN.2 esetén), megemelt-alap (az AVA_VAN.3 esetén), közepes (az AVA_VAN.4 esetén) vagy magas (az AVA_VAN.5 esetén) támadó képességgel, amikor áthatolni próbál a TOE-n.

Az értékelő vegye figyelembe azokat a sebezhetőségeket, amelyekkel az egyéb értékelési tevékenységei végrehajtása közben találta magát szemben. Az értékelői áthatolás tesztelés, amely megállapítja a TOE ellenállóképességét az ilyen lehetséges sebezhetőségekkel

szemben, úgy legyen végrehajtva, hogy egy olyan támadói szerepkört tételez fel, amely alap (az AVA_VAN.1 és AVA_VAN.2 esetén), megemelt-alap (az AVA_VAN.3 esetén), közepes (az AVA_VAN.4 esetén) vagy magas (az AVA_VAN.5 esetén) támadó képességgel rendelkezik.

Ugyanakkor a sebezhetőség vizsgálatot nem egy elszigetelt tevékenységként kell végrehajtani. Ez a vizsgálat szorosan kapcsolódik az ADV és AGD értékelési tevékenységekhez. Az értékelő ezen eltérő tevékenységeket úgy hajtsa végre, hogy közben az érintett területeken a lehetséges sebezhetőségek azonosítására koncentrál. Következésképp az értékelőnek jól kell ismernie az általános sebezhetőségi útmutatót (lásd 7.3.2.1).

7.3.2.1. Általános sebezhetőségi útmutató

Az általános sebezhetőségeket az alábbi öt kategóriával jellemezzük.

7.3.2.1.1. Megkerülés

Ez a támadási mód felölel minden olyan módszert, mely révén egy támadó megkerülheti a biztonság érvényre juttatását, az alábbiakkal:

a) a TOE interfészek vagy a TOE-vel kapcsolatba kerülő kiegészítők (utilities) lehetőségeinek a kihasználása;
b) jogosultságok vagy egyéb lehetőségek öröklése, melyek egyébként tiltva vannak;
c) nem megfelelően védett területekre másolt vagy ott tárolt érzékeny adatok kiolvasása (ha a bizalmasság fontos szempont).

Az alábbiak mindegyikét ajánlott figyelembe venni az értékelő független sebezhetőségi elemzése során:

a) „A TOE interfészek vagy a TOE-vel kapcsolatba kerülő kiegészítők lehetőségeinek a kihasználása” típusú támadások általában az interfészekre szükséges biztonság hiányán alapulnak. Példa: hozzáférés olyan funkcióhoz, melyet alacsonyabb szinten valósítottak meg, mint ahogyan a hozzáférés ellenőrzés érvényre jut. Idevágó elemek:
   aa) a TSFI előre meghatározott meghívási sorrendjének megváltoztatása;
   ab) egy további TSFI meghívása;
   ac) egy összetevő nem várt környezetben vagy nem tervezett céllal történő használata;
   ad) a kevésbé absztrakt megjelenítésben bevezetett megvalósítási részletek kihasználása;
   ae) a hozzáférés ellenőrzés és a használat ideje között eltelt idő kihasználása.
b) „A TSFI előre meghatározott meghívási sorrendjének megváltoztatása”-val akkor kell foglalkozni, amikor van egy olyan sorrend, mely alapján a TOE interfészek (pl felhasználói utasítások) meghívódnak egy TSFI kiváltása érdekében (például egy fájl megnyitása, majd adatok olvasása belőle). Ha egy TSFI a TOE egyik interfészében hívódik meg (pl. hozzáférés ellenőrzés), az értékelőnek ajánlott megvizsgálnia, hogy lehetséges-e az ellenőrzés megkerülése azáltal, hogy a hívás a sorrend egy későbbi pontjában, vagy egyáltalán nem történik meg.

c) „Egy további TSFI meghívása” (az előre meghatározott sorrendhez képest), a fentihez hasonló támadás, csak itt a sorozat valamely pontján a TOE egy más interfésze hívása iktatódik közbe. Ide sorolhatók azok a támadások is, amelyek azon alapulnak, hogy hálózaton továbbított érzékeny adatokat fognak el hálózati forgalom-figyelők használatával (itt a további komponens a hálózati forgalom-figyelő).
d) Egy összetevő nem várt környezetben vagy nem tervezett céllal történő használatán alapuló támadás a TOE egy (a TSF megvalósításában) nem érintett interfészét használja fel a TSF megkerülésére, egy nem tervezett cél elérésére. A rejtett csatornák (lásd részletesebben ezekről 7.3.2.1.4) ebbe a támadási típusba tartoznak. A nem dokumentált (esetleg nem biztonságos) interfészek használata szintén ebbe a kategóriába esik (pl. nem dokumentált kiegészítő és súgó lehetőségek).
e) „A kevésbé absztrakt megjelenítésben bevezetett megvalósítási részletek kihasználása”-t is a maga javára fordíthatja egy támadó, olyan kiegészítő funkciókat, erőforrásokat vagy tulajdonságokat kihasználva, melyeket a TOE-ba a finomítási folyamat eredményeként vezettek be. A kiegészítő funkciók lehetnek a szoftver modulokban maradt tesztkódok, valamint a megvalósítási folyamatban bevezetett kiskapuk is.
f) „A hozzáférés ellenőrzés és a használat ideje között eltelt idő kihasználása” olyan eseteket jelent, melyekben hozzáférés ellenőrzés és jogosultság megadása történik, és a támadó képes olyan feltételeket teremteni, melyeknek a hozzáférés ellenőrzésének idejében való aktivizálása az ellenőrzés sikertelenségéhez vezet. Példa: egy felhasználó létrehoz egy háttérfolyamatot nagyon érzékeny adatok olvasására és elküldésére a felhasználói terminálra, majd kijelentkezik és visszajelentkezik egy alacsonyabb érzékenységi szinten. Ha a háttérfolyamat nem fejeződött be a felhasználó kijelentkezéséig, akkor a támadó kikerülheti a MAC (Mandatory Access Control, kötelező hozzáférés ellenőrzés) ellenőrzéseket.
g) A „jogosultságok vagy egyéb lehetőségek öröklése”-n alapuló támadások általában jogtalanul szerzik meg valamely engedélyhez kötött összetevő jogosultságait vagy lehetőségeit, általában úgy, hogy nem ellenőrzött vagy nem tervezett módon lépnek ki ezekből. Az alábbi lényeges szempontokat kell itt figyelembe venni:
   ga) nem végrehajthatónak szánt adatok végrehajtása vagy végrehajthatóvá tétele;
   gb) nem tervezett bemenet generálása egy komponenshez;
   gc) olyan feltételezések és tulajdonságok érvénytelenítése, melyekre az alacsonyabb szintű komponensek épülnek.
h) A "nem végrehajthatónak szánt adatok végrehajtása vagy végrehajthatóvá tétele” olyan támadásokat jelent, amelyek vírusokat használnak (például végrehajtható kód vagy parancsok elhelyezése egy fájlban, amely automatikusan végrehajtódik, amikor a fájlhoz hozzáférnek vagy szerkesztik azt, és ezáltal a fájltulajdonos minden jogosultságának öröklése is megtörténik).
i) A "nem tervezett bemenet generálása egy komponenshez" típusú támadás váratlan hatásokat hozhat létre, melyeket egy támadó kihasználhat. Például, ha a TSF megkerülhető, amennyiben egy felhasználó hozzáfér az alatta lévő operációs rendszerhez, akkor a hozzáférés megszerzése lehetővé válik a bejelentkezési eljárás után azáltal, hogy a támadó kihasználja a különböző vezérlő vagy kilépő (escape) sorozatok leütésének hatását a jelszó hitelesítés ideje alatt.
j) Az "olyan feltételezések és tulajdonságok érvénytelenítése, melyekre az alacsonyabb szintű komponensek épülnek” típusú támadások azon alapulnak, hogy a támadó

kitör az alkalmazás megszorításaiból, hogy hozzáférjen az alkalmazás alatt lévő operációs rendszerhez, azért, hogy megkerülje egy alkalmazás TSF-jét. Ebben az esetben az érvénytelenített feltételezés az, hogy az alkalmazás felhasználója nem tud ilyen hozzáféréshez jutni. Hasonló támadás képzelhető el, ha a biztonsági funkciókat egy alkalmazás az alatta lévő adatbázis-kezelő rendszeren valósítja meg: a TSF ekkor is megkerülhető, ha a támadó ki tud törni az alkalmazás kereteiből.

k) A „nem megfelelően védett területeken tárolt érzékeny adatok kiolvasásán alapuló támadások” (ha a bizalmasság lényeges szempont) az alábbi, érzékeny adatokhoz hozzáférést lehetővé tevő lehetséges módszereket foglalják magukban:

l)lemez “böngészés”;

la) hozzáférés nem védett memóriához;

lb) megosztott írható állományokhoz vagy más megosztott erőforrásokhoz (pl. swap fájlokhoz) való hozzáférés kihasználása;

lc) A hiba helyreállítás aktiválása annak megállapítása érdekében, hogy ilyen esetben a felhasználó milyen hozzáférésekhez juthat. Egy rendszer összeomlás után például az automatikus állomány helyreállító rendszer felhasználhat egy “talált tárgyak” könyvtárát a fejléc nélküli állományokra, melyek címke nélkül vannak a lemezen. Ha a TOE kötelező hozzáférés ellenőrzést valósít meg, akkor meg kell azt vizsgálni, hogy milyen biztonsági szinten kell ennek a könyvtárnak lennie (például rendszer szinten), és ki férhet hozzá a könyvtárhoz.

Több különböző módszer van arra, amelyen keresztül egy értékelő beazoníthat egy kerülő utat, az alábbi két fő technikát beleértve. Az egyik technika az, hogy az értékelő a tesztelés során nem szándékosan azonosít egy olyan interfészt, amelyet helytelenül lehet használni. A másik technika az, amikor a TSF külső interfészei mindegyikére elvégeznek egy tesztelést debug módban abból a célból, hogy azonosítsanak minden olyan modult, amelyet nem hívtak meg az interfészek dokumentált tesztelésének részeként, majd a nem meghívott kód felülvizsgálatával megfontolják, hogy az nem kerülő út-e.

7.3.2.1.2. Hamisítás

A hamisítás magába foglal minden olyan támadást, mely azon alapul, hogy egy támadó megpróbálja a TSF működését befolyásolni (azaz módosítani vagy hatástalanítani), például az alábbi módokon:

a) olyan adatokhoz való hozzáféréssel, melyek bizalmasságán vagy sértetlenségén alapul a TSF;
b) a TOE-t szokatlan vagy nem várt körülményekkel való szembenézésre kényszerítik;
c) a biztonság érvényre juttatásának kikapcsolásával vagy késleltetésével,
d) a TOE fizikai módosításával.

Az alábbiakat ajánlott számításba venni az értékelő független sebezhetőségi elemzése során:

a) Támadások, melyek "olyan adatokhoz férnek hozzá, melyek bizalmasságán vagy sértetlenségén alapul a TSF":

aa) belső adatok közvetlen vagy közvetett olvasása, írása vagy módosítása;

ab) egy komponens nem tervezett környezetben vagy nem tervezett céllal történő használata;

ac) olyan komponensek közötti kölcsönhatások kihasználása, melyek nem láthatók a magasabb absztrakciós szinteken.

b) A "belső adatok közvetlen vagy közvetett olvasása, írása vagy módosítása" az alábbi támadás-típusokat tartalmazza, melyekkel ajánlott számolni a sebezhetőségi elemzés során:
   ba) belsőleg tárolt “titkok”, például felhasználói jelszavak kiolvasása;
   bb) olyan belső adatok “kijátszása”, hamisítása, melyeken a biztonságot megvalósító mechanizmusok alapulnak;
   bc) környezeti változók (pl. logikai nevek), konfigurációs állományok vagy ideiglenes fájlok adatainak módosítása.

c) Lehetséges egy megbízható folyamat megtévesztése oly módon, hogy az módosít olyan védett állományt, melyhez normál esetben nem fér hozzá.

d) Az értékelőnek az alábbi “veszélyes tulajdonságokat” is ajánlott figyelembe vennie:
   da) a TOE-ben található forráskód, fordítóval együtt (módosítani lehet például a bejelentkezési forráskódot);
   db) interaktív hibakereső és javítási lehetőség (módosítható például a végrehajtható kód képe);
   dc) eszközmeghajtó szinten módosítási lehetőség, ha nincs állományvédelem;
   dd) hibakereső (diagnosztikai) kód a forrásban, melyet opcionálisan bele lehet tenni;
   de) a TOE-ben hagyott fejlesztő eszközök.

e) Az "egy komponens nem tervezett környezetben vagy nem tervezett céllal való használata" olyan eseteket ölel fel, ahol például a TOE egy operációs rendszerre épített alkalmazás, és a felhasználók egy szövegszerkesztő csomag vagy más szerkesztő lehetőségeit használják fel a saját parancsállományaik módosítására (például nagyobb jogosultsági szint megszerzésére).

f) Az "olyan komponensek közötti kölcsönhatások kihasználása, melyek nem láthatók a magasabb absztrakciós szinteken", olyan támadást jelent, melyben a támadó az erőforrásokhoz való közös hozzáférést használja ki. Az egyik komponens által végzett erőforrás módosítás hatással lehet egy másik (megbízható) komponens működésére, például forráskód szinten, a globális adatok vagy közvetett mechanizmusok, közös memória, szemaforok alkalmazása révén.

g) Az olyan támadásoknál, amelyek "a TOE-t szokatlan vagy nem várt körülményekkel való szembenézésre kényszerítik", az alábbiakat kell figyelembe venni:
   ga) egy komponenshez nem várt bemenet generálása;
   gb) az alacsonyabb szintű komponenseket megalapozó feltételezések és tulajdonságok hatástalanítása.

h) Az “egy komponenshez nem várt bemenet generálása” a TOE működésének vizsgálatát jelenti az alábbi esetekben:
   ha) parancssori bemeneti puffer túlcsordulás (a verem összeomlása vagy más tárterület felülírása lehet a következmény, mellyel egy támadó visszaélhet, összeomláskor kiíródhat a memóriatartalom, melyben érzékeny információk, például nyílt jelszavak szerepelhetnek);
   hb) érvénytelen parancsok vagy paraméterek bevitele (pl. csak olvasható paraméter megadása egy interfésznek, amely ezen keresztül akar adatot visszaadni);
   hc) állományvége-jel (pl. CTRL/Z vagy CTRL/D) vagy null karakter beszúrása egy naplóállományba.

i) „Az alacsonyabb szintű komponenseket megalapozó feltételezések és tulajdonságok hatástalanítása" típusú támadások olyan forráskódban található hibákat használnak ki, ahol a kód (közvetlen vagy közvetett módon) feltételezi, hogy a biztonsági szempontból fontos adatok kötött formátumban vannak, vagy csak adott értékkészletbe eshetnek. Ekkor az értékelőnek ajánlott megnéznie, hogy az adatok más formátuma vagy más értéke hatástalanítja-e a feltételezéseket, és amennyiben igen, akkor a támadó rosszindulatú tevékenységét ez mennyiben segíti.

j) A TSF helyes működése függhet olyan feltevésektől, amelyek szélsőséges helyzetekben érvényüket veszítik (például amikor egy erőforrás használata eléri a korlátját, vagy a paraméterek meghaladják maximális értéküket). Az értékelőnek ajánlott megvizsgálnia (ha ez lehetséges) a TOE működését az ilyen korlátok elérése szempontjából, például az alábbi esetekben:
   ja) dátumok módosítása (hogyan viselkedik például a TOE, ha túllép egy kritikus dátumhatárt);
   jb) lemezterület töltése;
   jc) a maximális felhasználói szám túllépése;
   jd) a naplóállomány töltése;
   je) biztonsági riasztási sor telítődése egy terminálon;
   jf) kommunikációs komponensekre erősen támaszkodó, többfelhasználós TOE különböző komponenseinek túlterhelése,
   jg) hálózat vagy egyedi gazdagép forgalom túlterhelése, szerver “elárasztása”';
   jh) pufferek vagy mezők töltése.

k) Az olyan típusú támadás, mely "a biztonság érvényre juttatását kikapcsolja vagy késlelteti" az alábbiakat jelenti:
   ka) megszakítások használata vagy funkciók átütemezése a helyes sorrend megzavarására;
   kb) egyidejű folyamatok megzavarása;
   kc) olyan komponensek közötti kölcsönhatások kihasználása, melyek nem láthatók az absztrakció magasabb szintjén.

l) A "megszakítások használata vagy funkciók átütemezése a helyes sorrend megzavarására” támadás ellen meg kell vizsgálni a TOE működését, amikor:
   la) megszakítanak egy parancsot (CTRL/C-vel, CTRL/Y-al stb.);
   lb) második megszakítás érkezik, mielőtt az első nyugtázásra került volna.

m) A biztonsági szempontból fontos folyamatok (például egy naplózási folyamat) megszakításának hatásait ajánlott feltárni. Hasonlóan, az is lehetséges, hogy a támadó késlelteti a naplórekordok beírását vagy a riasztások elindítását vagy fogadását, miáltal azok az adminisztrátor számára már nem lesznek hasznos és időszerű információk (mivel a támadás már sikeresen lezajlott).

n) Az "egyidejű folyamatok megzavarása" elleni védekezés részeként meg kell vizsgálni a TOE-t akkor, amikor két vagy több egyed párhuzamos hozzáférést kísérel meg. A TOE lehet, hogy képes kezelni a zárolást, amikor két egyed párhuzamos hozzáféréssel próbálkozik, de lehet, hogy a működése már elveszíti jól definiált jellegét egy újabb egyed megjelenésekor. Például egy biztonsági szempontból kritikus folyamat erőforrásra váró állapotba kerülhet, ha két másik folyamat ugyanehhez az erőforráshoz van épp kapcsolódva.

o) Az “olyan komponensek közötti kölcsönhatás használata, melyek nem láthatók az absztrakció magasabb szintjén” típusú támadás időkritikus bizalmi folyamatok késleltetését jelentheti.

p) A „TOE fizikai módosítása” típusú támadások a következőképpen osztályozhatóak: fizikai szondázás, fizikai manipulálás, fizikai módosítás és helyettesítés.
   pa) A fizikai szondázás a TOE-ba való behatolással a TOE belsejét veszik célba; pl. leolvasások a belső kommunikációs csatlakozási felületeken, vezetékeken vagy memóriáknál.
   pb) A fizikai manipulálás érintheti a TOE belsejét úgy, hogy célba veszik a TOE belső módosítását (pl. optikai hiba-előidézés kölcsönhatási folyamatként), a TOE belső csatlakozási felületeit (pl. áram vagy órajel üzemeltetési hibákkal) és a TOE környezetet (pl. a hőmérséklet módosításával).
   pc) A TOE belső biztonságot érvényre juttató jellemzőinek fizikai módosítása abból a célból, hogy olyan jogosultságokat vagy más olyan lehetőségeket örököljenek, amelyeket a szabályos működéskor vissza kellene utasítani. Ilyen módosítások okozhatóak pl. optikai hiba-előidézéssel. A fizikai módosításon alapuló támadások előidézhetik magának a TSF-nek a megváltozását, pl. hibák okozásával a TOE belső program adatátvitelekben a végrehajtás előtt. Meg kell jegyezni, hogy az ilyen fajta, magának a TSF-nek a megváltoztatásával történő megkerülés minden TSF-et veszélyeztethet, hacsak nincsenek egyéb intézkedések (feltehetően környezeti intézkedések), amelyek meggátolják, hogy egy támadó fizikailag hozzáférést nyerjen a TOE-hoz.
   pd) Fizikai helyettesítés azzal a céllal, hogy a TOE-t egy másik entitással cseréljék ki a TOE szállítása vagy működése közben. A TOE helyettesítését a fejlesztői környezetből a felhasználóhoz való szállítás közben biztonságos szállítási eljárások alkalmazásával kell megakadályozni (mint amelyeket a „Fejlesztés biztonsága” (ALC_DVS) vett figyelembe). A TOE működés közbeni helyettesítését a felhasználói dokumentációk és az üzemeltetési környezet kombinációjával lehet figyelembe venni úgy, hogy a felhasználó meggyőződhessen arról, hogy valóban a TOE-val áll kölcsönhatásban.

7.3.2.1.3. Közvetlen támadások

A közvetlen támadások a permutáción vagy valószínűségen alapuló mechanizmusok feltörésére irányulnak (pl. az összes lehetséges eset kipróbálásának elvét alkalmazva).

Például hibás feltételezés lehet, hogy egy pszeudó-véletlenszám generátor megvalósítása rendelkezik a biztonsági mechanizmus kezdeti feltöltéséhez (seed) szükséges entrópiával.

Amikor egy permutációs vagy valószínűségen alapuló mechanizmus a biztonsági tulajdonságok megválasztásán (pl. a jelszó hossz megválasztásán), vagy egy emberi felhasználó adatbevitelén (pl. egy jelszó megválasztásán) alapul, a feltételezéseknek a legrosszabb esetet kell tükrözniük.

Azonosítani kell a permutációs vagy valószínűségen alapuló mechanizmusokat a sebezhetőség vizsgálat altevékenység bemeneteként megkövetelt értékelési bizonyítékok (ST,

funkcionális specifikáció, TOE terv és megvalósítási reprezentáció részhalmaz) vizsgálata során, valamint minden más TOE (pl. útmutató) dokumentáció azonosíthat további permutációs vagy valószínűségen alapuló mechanizmusokat.

Ahol a tervezési bizonyíték vagy az útmutató állításokat vagy feltételezéseket tartalmaz (pl. arra vonatkozóan, hogy hány hitelesítési kísérlet lehetséges percenként), az értékelőnek meg kell erősítenie ezek helyességét. Ez a megerősítés teszteléssel vagy független elemzéssel történhet.

A kriptográfiai algoritmusok gyengeségén alapuló közvetlen támadásokat nem kell figyelembe venni a sebezhetőség vizsgálat (AVA_VAN) során, mivel ez a CC (s így a jelen dokumentum által meghatározott értékelési módszertan) hatókörén kívül áll. A kriptográfiai algoritmus megvalósításának helyességét ugyanakkor a módszer figyelembe veszi, az ADV és ATE tevékenységein keresztül.

7.3.2.1.4. Megfigyelés

Az információ egy absztrakt rálátás arra a kapcsolatra, amely entitások tulajdonságai között áll fenn, pl. egy jel információt tartalmaz egy rendszerre vonatkozóan, ha a TOE képes reagálni erre a jelre. A TOE erőforrások olyan információkat dolgoznak fel és tárolnak, amelyeket a felhasználói adatok képviselnek. Ennélfogva:

a) információ áramolhat a felhasználói adatokkal együtt szubjektumok közötti belső TOE adatátvitel vagy a TOE-ból való export útján;
b) információ előállítható és átadható másik felhasználói adat részére;
c) információ nyerhető az információkat képviselő adatokon végzett műveletek megfigyelésével.

A felhasználói adatok által képviselt információ jellemezhető olyan értéket felvevő biztonsági jellemzővel, mint amilyen a „minősítési szint”, amelynek értékei pl. „nem-minősített, bizalmas, titkos, szigorúan titkos”, abból a célból, hogy az adatokon végzett műveleteket ellenőrizzék. Ez az információ, és ennélfogva a biztonsági jellemzők, műveletek segítségével megváltoztathatóak; pl. az FDP_ACC.2 leírhatja a szint csökkentését „leminősítés” útján, vagy növelheti a szintet adatok összetársításával. Ez az egyik szempontja az információáramlás vizsgálatnak, amely olyan ellenőrzött műveletekre irányul, amelyeket ellenőrzött szubjektumok hajtanak végre ellenőrzött objektumokon.

A másik szempont a jogtalan információ áramlás vizsgálata. Ez a szempont általánosabb, mint a felhasználói adatokat tartalmazó objektumokhoz való közvetlen hozzáférés, amelyet az FDP_ACC család tárgyal. Egy információáramlás ellenőrzési szabályzat ellenőrzése alá tartozó adatokat hordozó nem-kikényszerített jelcsatorna idézhető elő azáltal, hogy megfigyelik egy olyan objektum feldolgozását, amely a szóban forgó információt tartalmazza vagy azzal kapcsolatban áll (pl. oldalcsatornák). Egy kikényszerített jelcsatorna az erőforrásokba beavatkozó szubjektumokkal és a szóban forgó hamisítást észlelő szubjektummal vagy felhasználóval határozható meg. Klasszikus értelemben a rejtett csatornákat időzítő vagy tároló csatornaként határozzák meg, a módosítás vagy modulálás alatt álló erőforrásnak megfelelően. Az egyéb megfigyelési támadásokat illetően a TOE használata összhangban áll az SFR-ekkel.

Rejtett csatornák általában abban az esetben alkalmazhatók, ha a TOE megfigyelhetetlenségi és többszintű szétválasztási követelményekkel rendelkezik. A rejtett csatornákat rutinszerűen fel lehet ismerni a sebezhetőség vizsgálat és a tervezési tevékenységek során, ennélfogva tesztelendők. Az ilyen megfigyelési támadásokat azonban általában csak speciális vizsgálati technikák azonosítanak be, amelyeket közös néven „rejtett csatorna vizsgálatok”-nak neveznek. Ezeket a technikákat sokat tanulmányozták, és számos cikket publikáltak e témakörben. A rejtett csatorna vizsgálat lefolytatásához útmutatás a tanúsító szervezetektől kapható.

A nem-kikényszerített információáramlás megfigyelési támadások passzív vizsgálati technikákat foglalnak magukban, amelyek a TOE érzékeny belső adatainak a felfedését célozzák a TOE olyan üzemeltetésével, amely megfelel az útmutató dokumentumoknak.

Az oldalcsatorna vizsgálat rejtett vizsgálati technikákat is magában foglal, amelyek a TOE fizikai szivárgásán alapulnak. Fizikai szivárgást okozhatnak időzítési információk, egy TSF számítás közbeni áramfelvétele vagy áram kisugárzása. Időzítési információkat távoli támadó is gyűjthet (aki hálózati hozzáféréssel rendelkezik a TOE-hoz), az áramon alapuló információs csatornákhoz azonban szükséges, hogy a támadó a TOE közeli környezetében legyen.

A lehallgatásos technikák magukban foglalják az energia minden formájának elfogását, pl. a számítógépes képernyők elektromágneses vagy optikai kisugárzását, nem szükségszerűen a TOE közeli környezetében.

A megfigyelés magában foglalja a protokoll hibák kiaknázásait, mint amilyen például az SSL (hibás) megvalósításán alapuló támadás.

7.3.2.1.5. Helytelen használat/visszaélés

Helytelen használat (illetve a támadó szempontjából visszaélés) bekövetkezhet az alábbiak miatt:

a) hiányos útmutató dokumentáció,
b) ésszerűtlen útmutatók,
c) a TOE rossz konfigurálása,
d) a TSF kikényszerített kivételes viselkedése.

Ha az útmutató dokumentáció hiányos, a felhasználó nem tudhatja, hogy hogyan működtesse a TOE-t az SFR-ekkel összhangban. Az értékelőnek ajánlott alkalmaznia az egyéb értékelői tevékenységéből nyert ismereteit annak megállapítása érdekében, hogy az útmutató teljes-e. Az értékelőnek különösen a funkcionális specifikációt ajánlott figyelembe vennie. Az ebben leírt TSF-t az útmutatóban is ajánlott leírni az emberi felhasználók számára elérhető TSFI-n keresztüli biztonságos adminisztrálás és használat érdekében. A különböző üzemeltetési módokat is ajánlott figyelembe venni annak biztosítása érdekében, hogy minden üzemeltetési mód esetére legyen útmutatás. Az értékelő segítségképpen egy informális megfeleltetést készíthet az útmutató és a funkcionális specifikáció között. A megfeleltetés minden elmaradása hiányosságot mutathat.

Az útmutató akkor tekintendő ésszerűtlennek, ha a TOE használatára vagy az üzemeltetési környezetre olyan elvárásokat fogalmaz meg, melyek ellentmondanak az ST-nek, vagy alkalmatlanok a biztonság kezelésére.

A TOE számos módszert használhat, hogy segítse a vásárlót a TOE SFR-eknek megfelelő használatában, s hogy megakadályozza a véletlen rossz konfigurálást. Egy TOE funkciót biztosíthat a vásárló riasztására, amennyiben a TOE az SFR-ekkel ellentmondó állapotba kerül, míg más TOE-kat olyan bővített útmutatóval szállítanak, mely javaslatokat, ötleteket, eljárásokat, tartalmaz a létező biztonsági funkciók leghatékonyabb alkalmazására (pl. útmutatás a naplózás tulajdonság felhasználására, az SFR-ek esetleges kompromittálódásának észlelésére). Az értékelő vegye figyelembe a TOE funkcionalitását, célját és az üzemeltetési környezetre vonatkozó biztonsági célokat, hogy következtessen arra, hogy az útmutató használata alapján ésszerűen elvárható vagy sem egy nem biztonságos állapotba kerülés időben történő észlelése. Annak lehetőségét, hogy a TOE egy nem biztonságos állapotba kerül, az értékelési bizonyítékok használatával lehet megállapítani, úgymint az ST, a funkcionális specifikáció és minden egyéb tervezés reprezentáció, mely a TOE garanciaszintje mellett a bizonyítékok között szerepel (pl. TOE/TSF terv előírás, amennyiben az ADV_TDS egy összetevője szerepel).

A TSF kikényszerített kivételes viselkedése magában foglalja többek között az alábbiakat:

a) a TOE működése indítás, lezárás vagy hibából való helyreállás esetén;
b) a TOE működése szélsőséges körülmények esetén (túlterhelésnek vagy aszimptotikus üzemnek is nevezik ezt), különösen ha ez a TSF részeinek hatástalanításához vagy kikapcsolásához vezethet;
c) bármilyen esély véletlen hibás konfigurálásra vagy nem biztonságos használatra, melyek a hamisítás címszó alatt korábban leírt támadásokból erednek.

7.3.2.2. A lehetséges sebezhetőségek meghatározása

A lehetséges sebezhetőségeket az értékelő határozhatja meg különböző tevékenységek során. Ezek nyilvánvalóvá válhatnak egy értékelési tevékenység során, vagy a bizonyítékok sebezhetőség felkutatásra irányuló vizsgálata eredményeképpen lehet meghatározni ezeket.

7.3.2.2.1. Rábukkanás

A rábukkanással történő sebezhetőség meghatározás akkor történik, amikor az értékelő lehetséges sebezhetőséget határoz meg az értékelési tevékenységek végrehajtása során, vagyis olyankor, amikor a bizonyítékokat nem kifejezetten a sebezhetőségek meghatározásának a céljából vizsgálja.

A rábukkanásos meghatározási módszer függ az értékelő tapasztalataitól és ismereteitől, amit a tanúsító szervezet figyel és felügyel. Ez egy nem megismételhető megközelítési mód, de dokumentálva lesz abból a célból, hogy biztosítva legyen a következtetések levonásának megismételhetősége a jelentésben rögzített lehetséges sebezhetőségekből kiindulva.

Erre a módszerre nincs megkövetelve formális vizsgálati szempont. A lehetséges sebezhetőségeket az átadott bizonyítékokból határozzák meg a tudás és tapasztalat

eredményeképpen. A meghatározásnak ez a módszere azonban nem korlátozódik a bizonyítékok valamilyen sajátos részhalmazára.

Az értékelő feltételezetten ismeretekkel rendelkezik a TOE-típus technológiájáról, és ismeri a nyilvánosan dokumentált biztonsági réseket. Az ismeretek feltételezett szintje megszerezhető egy a TOE típusára vonatkozó biztonsági e-mail listából, és az olyan rendszeres közleményekből (hiba, sebezhetőségi és biztonsági hiba listák), amelyeket azok a szervezetek hoznak nyilvánosságra, amelyek a széles körben használt termékek és technológiák biztonsági kérdéseit kutatják. Az AVA VAN.l vagy AVA VAN.2-re vonatkozóan nincs feltételezve, hogy ez a tudás kiterjed az egyetemi kutatások által készített speciális konferencia kiadványokig vagy értekezésekig. Az alkalmazott tudás naprakészségének biztosítása érdekében azonban szükséges, hogy az értékelő felkutassa a nyilvánosan elérhető anyagokat.

Az AVA VAN.3 már feltételezi, hogy a nyilvánosan elérhető információ felkutatása magában foglal konferencia kiadványokat és értekezéseket, amelyeket egyetemek és más érintett szervezetek által végzett kutatás során állítottak elő.

A következők arra példák, hogy az értékelő hogyan tud sebezhetőségekre bukkanni:

a) miközben az értékelő valamilyen bizonyítékot vizsgál, az emlékezetébe ötlik egy lehetséges sebezhetőség, amelyet egy hasonló terméktípusnál határoztak meg, és az értékelő úgy véli, hogy ez az értékelés alatt álló TOE-ban is megvan;
b) miközben az értékelő valamilyen bizonyítékot vizsgál, észrevesz egy rést egy csatlakozási felület specifikációban, amely egy lehetséges sebezhetőséget tükröz.

Ez magában foglalhatja azt is, hogy az értékelő úgy szerez tudomást a TOE-ban meglévő lehetséges sebezhetőségről, hogy egy speciális termék típusban található általános sebezhetőségről olvas az IT biztonsági publikációkban vagy egy biztonsági e-mail listában, amelyre az értékelő feliratkozott.

Ezekből a lehetséges sebezhetőségekből közvetlenül kifejleszthetők támadási módszerek. Ennélfogva a rábukkanással megtalált lehetséges sebezhetőségeket az értékelői sebezhetőség vizsgálaton alapuló áthatolás tesztek kialakításakor egyeztetik. Nincsen közvetlen akció azzal a céllal, hogy az értékelő bukkanjon rá lehetséges sebezhetőségekre. Ennélfogva az értékelőt egy közvetett akció vezeti, amely az AVA_VAN.1.2E-ben és AVA VAN.*.4E-ben van meghatározva.

A nyilvános sebezhetőségeket és támadásokat illetően az értékelőt aktuális információval láthatja el pl. egy tanúsító szervezet. Ezt az információt az értékelőnek figyelembe kell vennie, amikor egyezteti a rábukkanással megtalált sebezhetőségeket és támadási módszereket, az áthatolás tesztek kialakításakor.

7.3.2.2.2. Vizsgálat

Az értékelői akciókban a következő típusú vizsgálatok szerepelnek.

Nem-strukturált vizsgálat

Az értékelő által végrehajtandó nem-strukturált vizsgálat (alap és fokozott garanciaszinten, az AVA_VAN.2 altevékenység értékelésére) lehetővé teszi az értékelő számára, hogy az általános sebezhetőségekre rábukkanjon (a 7.3.2.2.1.-ben tárgyaltaknak megfelelően). Az értékelő használja fel a hasonló technológia típusokban lévő hibákra vonatkozó tapasztalatait és ismereteit is.

Célirányos vizsgálat

Az értékelési tevékenységek során az értékelő meghatározhat problémás területeket is. Ezek a TOE bizonyítékok olyan speciális részei, amelyekkel kapcsolatban az értékelőnek fenntartásai vannak, bár a bizonyíték kielégíti a tevékenységre vonatkozó követelményeket. Például egy bizonyos csatlakozási felület specifikáció túl bonyolultnak tűnik, és így hiba lehetőségre ad okot a TOE fejlesztése vagy működése közben. Nincs kézzelfogható lehetséges sebezhetőség ezen a ponton, további vizsgálat szükséges. Ez túlnyúlik a már számításba vett területen, minthogy további vizsgálatot igényel.

A lehetséges sebezhetőség és a problémás terület közötti különbség a következő:

a) Lehetséges sebezhetőség – Az értékelő ismer egy olyan támadási módszert, amelyet fel lehet használni a gyengeség kiaknázására, vagy az értékelő ismer olyan sebezhetőségi információt, amely a TOE-ra vonatkozik.
b) Problémás terület – az értékelő lehetséges sebezhetőségnek feltételezhet egy problémát, máshol szerzett információkon alapulva. Az értékelő a csatlakozási felület specifikáció olvasása közben megállapítja, hogy egy csatlakozási felület túlzott (szükségtelen) bonyolultsága miatt lehetséges sebezhetőség fordulhat elő az érintett területen, bár ez nem nyilvánvaló a kezdeti vizsgálatokból.

A lehetséges sebezhetőségek meghatározásának célirányos megközelítési módja a bizonyítékok olyan célú vizsgálata, hogy bármely lehetséges sebezhetőséget megállapítsanak, amelyek a tartalmazott információkból nyilvánvalóak. Ez egy nem-strukturált vizsgálat, minthogy a megközelítési mód nincs előre meghatározva. A lehetséges sebezhetőségek meghatározásának célirányos megközelítési módja felhasználható az (AVA_VAN.3) altevékenység értékelése által kiemelt garanciaszinten megkövetelt független sebezhetőség vizsgálat során.

Ez a vizsgálat különböző megközelítési módokon keresztül valósítható meg, melyek összemérhető bizonyossághoz vezetnek. A megközelítési módok egyikénél sem tartozik szigorú formátum az elvégzendő bizonyíték vizsgálatra.

A megközelítési módot az értékelő azon bizonyíték felmérés eredményei vezérlik, amelyeket az AVA/AGD altevékenységek követelményei teljesülésének megállapítására végzett. Ennélfogva a bizonyítékoknak a lehetséges sebezhetőségek létezésére irányuló vizsgálatát a következők valamelyike irányíthatja:

a) a problémás területek, amelyeket az értékelői tevékenységek során a bizonyítékok vizsgálata során határoztak meg;
b) szétválasztást biztosító speciális funkcionalitásra való támaszkodás, amelyet a biztonsági szerkezet leírás vizsgálata során határoztak meg (az ADV_ARC.l altevékenység értékelésénél), és amely további vizsgálatokat igényel annak eldöntésére, hogy megkerülhető-e;

c) a bizonyítékok reprezentatív vizsgálata a TOE lehetséges sebezhetőségeire vonatkozó hipotézisek felállítására.

Az értékelőnek jelentést kell készítenie a bizonyítékokban található lehetséges sebezhetőségek meghatározására tett lépésekről. Ugyanakkor lehet, hogy az értékelő nem képes ezeket a lépéseket a vizsgálat megkezdése előtt leírni, mivel ezek az értékelési tevékenységek eredményeként alakulnak ki.

A problémás területek bármelyik olyan bizonyíték vizsgálatából felmerülhetnek, amelyeket a TOE értékeléshez meghatározott garanciális biztonsági követelmények kielégítésére biztosítottak. A nyilvánosan hozzáférhető információk is figyelembe veendők.

Az értékelő által végrehajtott tevékenységek megismételhetők, és ugyanazon következtetéseket eredményeznek a TOE garanciaszintjére nézve, bár e következtetésekhez vezető lépések változhatnak. Minthogy az értékelő dokumentálja a vizsgálat elvégzésének formáját, a következtetésekhez vezető tényleges lépések is megismételhetők.

Módszeres vizsgálat

A módszeres vizsgálati megközelítési mód formája a bizonyítékok egy strukturált vizsgálata. Ez a módszer megkívánja, hogy az értékelő meghatározza a vizsgálat alkalmazni kívánt struktúráját és formáját (vagyis azt a módot, ahogyan a vizsgálat végrehajtásra kerül, a célirányos vizsgálattól eltérően előre meghatározott). A módszer meghatározza a mérlegelendő információkat, valamint a mérlegelés mikéntjét és okát. A lehetséges sebezhetőségek meghatározásának ezt a megközelítési módját lehet használni az AVA_VAN.4 és AVA_VAN.5 altevékenységek értékelése által megkövetelt független sebezhetőség vizsgálat során. (A jelen dokumentum által meghatározott értékelési módszertan csak AVA_VAN.3-ig tartalmazza a CC sebezhetőség vizsgálat család garancia-összetevőit, a módszeres vizsgálatot tehát még kiemelt garanciaszinten sem várja el.)

A bizonyítékoknak ez a vizsgálata a megközelítési módjában előre átgondolt és előre tervezett, és minden meghatározott bizonyítékot a vizsgálat bemenetének tekint.

Az egyes garanciaszinteken specifikált (ADV) garanciakövetelmények teljesítésére nyújtott minden bizonyíték bemenetként szolgál a lehetséges sebezhetőségek megállapítására szolgáló tevékenységhez.

Ezen vizsgálat esetében a „módszeres” jelző használata azt a jellegzetességet kívánja megragadni, hogy a lehetséges sebezhetőségnek ez a meghatározása rendezett és tervezett megközelítési módra törekszik. „Módszer”-t vagy „rendszer”-t kell alkalmazni a vizsgálatokban. Az értékelőnek le kell írnia a használandó módszert a figyelembevett bizonyítékok szempontjából, a bizonyítékban lévő vizsgálandó információt, azt a módot, ahogyan ezt az információt figyelembe kell venni, és a kialakítandó hipotézist.

A következők példákat mutatnak olyan feltételezésekre, amelyeket egy hipotézis tehet:

a) hibásan megadott bemenet feltételezése olyan csatlakozási felületeken, amelyek egy támadó számára kívülről elérhetők;

b) olyan biztonsági mechanizmus (mint például a tartomány szétválasztás) vizsgálata, mely belső buffer túlcsordulás feltételezése mellett a szétválasztás leromlásához vezethet;
c) olyan objektum meghatározására irányuló vizsgálat, amelyet a TOE megvalósítási reprezentációja hozott létre, így a TSF nem ellenőriz teljes mértékben, s amelyet egy támadó felhasználhat az SFR-ek aláaknázására.

Például az értékelő meghatározhatja, hogy a csatlakozási felületek a TOE lehetséges gyenge pontjai, és egy olyan megközelítési módot specifikálhat, hogy „a funkcionális specifikációban és TOE tervben megadott minden csatlakozási felület specifikáció átvizsgálásra kerül lehetséges sebezhetőség hipotézisek kialakításához”, majd folytathatja azzal, hogy megmagyarázza a hipotézisben használt módszereket.

Ez a meghatározási módszer egy olyan TOE támadási tervet szolgáltat, amelyet egy értékelő végrehajthat a TOE lehetséges sebezhetősége áthatolás tesztelésének kiteljesítésére. A meghatározási módszer magyarázata bizonyítékot szolgáltathat a TOE-n végrehajtandó kiaknázás lefedettségére és mélységére.

7.3.3. Mikor használják a támadó képességet

7.3.3.1. A fejlesztő

A támadó képességet felhasználja az ST szerzője, amikor az ST-t kialakítja a fenyegető környezet figyelembe vételekor és a garanciakomponensek kiválasztásakor. Ez lehet egy egyszerű megállapítása annak, hogy a TOE feltételezett támadói általában alap-, megemelt-alap-, közepes- vagy magas támadó képességgel rendelkeznek.

Az ST szerzője figyelembe veszi a kockázat-felmérés során kifejlesztett veszély-profilt (a CC hatáskörén kívül, de amelyet bemenetként felhasználnak az ST kifejlesztésekor, a „biztonsági probléma meghatározás”-hoz). Ennek a veszély-profilnak a figyelembe vétele a következő fejezetekben tárgyalt valamelyik megközelítési mód szempontjából lehetővé teszi annak a támadó képességnek a meghatározását, amellyel szemben a TOE-nak ellent kell állnia.

7.3.3.2. Az értékelő

A támadó képességet az értékelő főleg két különböző módon veszi figyelembe az ST értékelési és a sebezhetőség vizsgálati tevékenységek során.

Támadó képességet használ az értékelő a sebezhetőségi vizsgálat altevékenység végrehajtása során annak megállapítására, hogy a TOE ellenáll-e olyan támadásoknak, amely meghatározott támadó képességet feltételez egy támadóról. Ha az értékelő azt állapítja meg, hogy egy lehetséges sebezhetőséget ki lehet aknázni a TOE-ben, akkor meg kell hogy erősítse, hogy ez kiaknázható az előirányzott környezet minden vonatkozásának figyelembe vétele mellett, beleértve a támadóról feltételezett támadó képességet.

Ennélfogva, a biztonsági előirányzat veszély megállapításaiban megadott információkat felhasználva, az értékelő határozza meg azt a minimális támadó képességet, amely szükséges ahhoz, hogy a támadó hatásos támadást hajtson végre, és következtessen a TOE támadásokkal szembeni ellenálló-képességéről. A 7. táblázat bemutatja ennek a vizsgálatnak és a támadási lehetőségnek a kapcsolatát.

A 7. táblázat maradék sebezhetőség oszlopában a „magas feletti" bejegyzés azokat a lehetséges sebezhetőségeket jelzi, amelyek azt igénylik, hogy egy támadó magasabb támadó képességgel rendelkezzen, mint amit a „magas" jelent, ha ki akarja használni a szóbanforgó lehetséges sebezhetőséget. Ebben az esetben a maradékként besorolt sebezhetőség azt a tényt tükrözi, hogy létezik egy ismert gyengeség a TOE-ban, de az adott üzemeltetési környezetben a feltételezett támadó képesség mellett a gyengeséget nem lehet kihasználni.

Egy lehetséges sebezhetőséget a támadó képesség bármely szintjénél „nem-megvalósítható"-nak ítélhetnek azon ellenintézkedések következményeként, amelyek az üzemeltetési környezetben meggátolják a sebezhetőség kiaknázását.

Egy sebezhetőség vizsgálat minden TSFI-re vonatkozik, beleértve a valószínűségi vagy permutációs mechanizmusokhoz hozzáférőket is. Nincsenek feltételek sem a TSFI tervének és megvalósításának a helyességére, sem a támadási módszerre vagy a támadó TOE-ra hatására vonatkozó korlátozásokra – ha egy támadás lehetséges, akkor azt figyelembe kell venni a sebezhetőség vizsgálat során. Ahogy az a 7. táblázatban látható, ha egy sebezhetőségi garancia-összetevőt sikeresként értékeltek, akkor ez azt tükrözi, hogy a TSF-et úgy tervezték és valósították meg, hogy védve van a veszély megadott szintjével szemben.

7. táblázat - A sebezhetőség tesztelése és a támadó képesség

sebezhetőségi összetevő	**a TOE ellenáll az alábbi támadó képességgel rendelkező támadónak**	**a maradvány sebezhetőség csak az alábbi támadó képességgel rendelkező támadó számára kihasználható**
VAN.5	magas	magas feletti
VAN.4	közepes	magas
VAN.3	megemelt-alap	közepes
VAN.2	alap	megemelt-alap
VAN.1	alap	megemelt-alap

Nem szükséges, hogy egy értékelő támadó képesség számításokat végezzen minden egyes lehetséges sebezhetőségre. Bizonyos esetekben a támadási módszerek kifejlesztésénél nyilvánvaló, hogy a támadási módszer kifejlesztéséhez és futtatásához szükséges támadó képesség összemérhető-e azzal, amellyel a támadó feltehetően rendelkezik az üzemeltetési környezetben. Ugyanakkor az értékelő végezzen támadó képesség számítást minden kiaknázhatónak ítélt sebezhetőségre, annak megállapítása érdekében, hogy a kiaknázhatóság szóba jöhet-e a támadóra feltételezett támadó képesség szintjén.

Az alábbiakban ismertetett megközelítési módot kell alkalmazni mindenütt, ahol támadó képesség számításra van szükség. A 8. és 9. táblázatban megadott értékek nincsenek matematikailag bizonyítva. Ennélfogva lehetséges, hogy az ezekben a példa-táblázatokban megadott értékeket ki kell igazítani a technológia típusnak és az adott környezeteknek megfelelően. Az értékelő útmutatásért a tanúsító szervezethez fordulhat.

7.3.4. A támadó képesség kiszámítása

7.3.4.1. A támadó képesség alkalmazása

A támadó képesség szakértelem, erőforrások és motiváció függvénye. Különböző módszerek vannak ezen tényezők megjelenítésére és megmérésére. Bizonyos TOE típusokra egyéb tényezők alkalmazása is lehetséges.

7.3.4.1.1. A motiváció figyelembe vétele

A motiváció a támadó képesség olyan tényezője, mellyel egy támadó és az általa megszerezni kívánt értékek több szempontja is jellemezhető. A motiváció egyrészt jelentheti egy támadás valószínűségét. Egy olyan veszély, melynek magasan motivált támadó a forrása, vélhetően bármikor bekövetkezhet, míg egy nem motivált veszélyforrásból az a következtetés adódhat, hogy nem várható felőle támadás. A fenti két szélsőséges motivációs szint kivételével nehéz meghatározni a motivációból egy támadás előfordulási valószínűségét.

A motiváció másrészt utalhat a védendő érték pénzben vagy egyéb módon kifejezhető jelentőségére, a támadó vagy az érték tulajdonosa számára. Nagyon nagy érték nagyobb késztetést jelent egy támadónak, mint egy kisebb jelentőségű érték. Konkrétan azonban nehéz valamely vagyon értékét a motivációhoz kötni, mert az érték megítélése szubjektív: nagyrészt a tulajdonos megítélésétől függ.

Harmadszor a motiváció utalhat egy támadó szakértelmére és erőforrásaira is, melyeket felhasználhat támadásához. Egy nagymértékben motivált támadó valószínűleg megszerzi a szükséges tudást és szakértelmet a megszerzendő értékek védelmi rendszerének sikeres áttörése érdekében. Ennek fordítottja is igaz lehet, vagyis egy nagy szakértelemmel és erőforrással bíró támadó alacsony motiváltság esetén nem fogja ezen eszközeit felhasználni egy támadás kivitelezéséhez.

Az értékelésre készülés és annak végzése során a motiváció mindhárom fenti oldalát figyelembe kell venni. Az első szempont (a támadás valószínűsége) az, ami egy fejlesztőt arra ösztönöz, hogy értékelést végeztessen. Ha a fejlesztő úgy véli, hogy a támadók kellőképpen motiváltak egy támadás végrehajtásához, akkor az értékelés megállapíthatja, hogy a TOE képes garantálni a támadó erőfeszítéseinek visszaverését. Jól meghatározott környezetben, például egy rendszer értékelésénél, egy támadás motivációs szintje ismert lehet, és ez befolyásolhatja az ellenintézkedések kiválasztását.

A második szempont (a védendő érték nagysága) esetén az érték tulajdonosa vélheti azt, hogy a védendő vagyon megléte (bármilyen mértékkel mérve is) elegendő ahhoz, hogy valakit támadásra ösztönözzön. Amennyiben szükségesnek ítélik az értékelést, a támadó motiváltsága szerepet játszik a támadási módszerek számbavételénél, illetve a támadások lefolytatásában felhasznált erőforrások és szakértelem felmérésénél. A fejlesztő kiválaszthatja azt a megfelelő garanciaszintet, különösen az AVA követelmény összetevőit, amely arányban áll a veszélyekkel kapcsolatos támadó képességgel. Az értékelés során, és főleg a sebezhetőségi elemzés tevékenység eredményeként, az értékelő megállapítja, hogy a TOE a célkörnyezetben

kielégítő módon megakadályozza-e a megadott szakértelemmel és erőforrásokkal rendelkező támadók támadását.

Egy PP szerzője számszerűsítheti egy támadó motiváltságát, minthogy a PP szerzője szélesebb ismeretekkel rendelkezik az üzemeltetési környezetről, amelybe a TOE-t (a PP követelményeivel összhangban) el kell helyezni. Ennélfogva a motiváltság a támadó képesség kifejezésének közvetlen részét képezheti a PP-ben, a motiváltság számszerűsítésére szolgáló szükséges módszerek és intézkedések mellett.

7.3.4.2. A támadó képesség jellemzése

Ez a pont azokat a tényezőket veszi számba, amelyek a támadó képességet határozzák meg, egyben útmutatót ad ahhoz, hogy hogyan lehet az értékelési folyamat néhány szubjektív szempontját kiküszöbölni.

7.3.4.2.1. A támadó képesség meghatározása

Egy támadásra vonatkozó támadó képesség megállapítása megegyezik annak az erőfeszítésnek a meghatározásával, amely egy támadás kialakításához szükséges, és annak szemléltetésével, hogy ez sikeresen alkalmazható a TOE-ra (beleértve minden szükséges tesztelési eszköz összeállítását vagy felépítését), és hogy ezáltal a TOE-ban meglévő sebezhetőség kiaknázható. Annak szemléltetéséhez, hogy a támadás sikeresen alkalmazható, számításba kell venni minden olyan nehézséget, mely a laboratóriumi eredményből egy sikeres támadáshoz vezet. Például, ha egy kísérlet felfedi egy bizalmas adat (például kulcs) bizonyos bitjeit vagy byte-jait, számításba kell venni, hogy az adat többi részét hogyan lehetne megszerezni (ebben a példában bizonyos bitek közvetlenül kimérhetőek további kísérletekkel, míg egyéb bitek esetleg különböző technikákkal, például a teljes kipróbálással megtalálhatók). Nem szükséges minden kísérletet végrehajtani a teljes támadás beazonosításához, feltéve, ha világos, hogy a támadás ténylegesen bizonyítja, a hozzáférést egy TOE értékhez, és hogy a teljes támadás reálisan végrehajtható a sebezhetőség kiaknázására a vizsgált AVA_VAN összetevőnek megfelelően. Bizonyos esetekben az egyetlen mód annak igazolására, hogy egy támadás reálisan végrehajtható a sebezhetőség kiaknázására a vizsgált AVA_VAN összetevőnek megfelelően, az, hogy teljes egészében végre kell hajtani a támadást, és ezt követően ki kell értékelni ezt a ténylegesen szükséges erőforrások alapján. Egy lehetséges sebezhetőség azonosításából származó egyik kimenet feltehetően egy olyan forgatókönyv, amely lépésről-lépésre leírja, hogy hogyan kell végrehajtani egy olyan támadást, amely felhasználható a sebezhetőség kiaknázására a TOE egy másik példányán.

Sok esetben az értékelők a teljes kiaknázás végrehajtása helyett mérlegeljék a kiaknázásra vonatkozó paramétereket. A mérlegelések és ezek indoklásait dokumentálják az értékelési jelentésben.

7.3.4.2.2. Figyelembe veendő szempontok

Az alábbi tényezőket ajánlott figyelembe venni egy sebezhetőség kihasználásához szükséges támadó képesség elemzése során:

a) Az azonosításhoz és kihasználáshoz szükséges idő (***felhasznált idő***);
b) A szükséges speciális műszaki tudás (***szakértelem***);
c) A TOE terveinek és működésének az ismerete (***TOE ismeret***);
d) Alkalom (***lehetőség***);
e) A kihasználáshoz szükséges informatikai hardver/szoftver vagy más berendezés (***eszköz***).

Számos esetben ezek a tényezők nem függetlenek, hanem valamilyen mértékben helyettesíthetik egymást. A szakértelem vagy hardver/szoftver például pótolhatja az időt. Az alábbiak ezeket a tényezőket veszik számításba. (Az egyes szempontok szintjeit növekvő fontossági sorrendben tárgyalják.) A kiaknázási fázisban a legkevésbé „költséges" összetételt veszik figyelembe.

A ***felhasznált idő*** annak az időnek a teljes mennyisége, amelyet egy támadó fordít arra, hogy előbb meghatározza egy adott lehetséges sebezhetőség előfordulását a TOE-ban, majd kifejlesszen erre egy támadási módszert, végül pedig végrehajtsa a TOE elleni támadást. Ennek a szempontnak a figyelembe vételekor a legrosszabb esetet képviselő forgatókönyv legyen felhasználva a szükséges idő mennyiségének a megbecslésére.

A meghatározott idő mennyiség a következők egyike:
a) kevesebb, mint egy nap,
b) egy nap és egy hét között,
c) egy és két hét között,
d) két hét és egy hónap között,
e) minden újabb hónap 6 hónapig egy emelt értékhez vezet,
f) több, mint 6 hónap.

A ***szakértelem*** az alkalmazási területhez vagy terméktípushoz kötődő általános ismeretekre utal (például internet protokollok, Unix operációs rendszer, buffer túlcsordulás). A meghatározott szintek a következők:
a) hozzá nem értők, akiknek nincs különleges szakértelmük, és a szakértőkhöz és hozzáértő személyekhez képest kevesebb tudással rendelkeznek.
b) hozzáértő személyek, akik ismerik a termék vagy rendszer típus biztonsági működését;
c) szakértők, akik ismerik a rendszerhez/termékhez az alapvető algoritmusokat, protokollokat, hardvert, struktúrákat, biztonsági viselkedést, az alkalmazott biztonsági elveket és elgondolásokat, új támadások meghatározásához szükséges technikákat és eszközöket, kriptográfiát, a termék típusra irányuló klasszikus támadásokat, támadási módszereket, stb.;
d) a „többszörös szakértő" szintet arra a helyzetre vezették be, amikor különböző területek szakértő szintű tudása szükséges egy támadás különböző lépéseihez.

Előfordulhat, hogy bizonyos fajta szakértelem szükséges. Alapértelmezés szerint a különböző szakértelem elemek közül a legmagasabb fokút kell kiválasztani. Nagyon speciális esetekben használható a „többszörös szakértő" szint, de legyen megjegyezve, hogy a szakértelemnek ekkor olyan területeket kell érintenie, amelyek szigorúan eltérnek, mint például a hardver manipuláció és a kriptográfia.

A ***TOE ismeret*** a TOE-hez kapcsolódó speciális szakértelemre vonatkozik. Ez eltér az általános ismeretektől, de nem független azoktól. A meghatározott szintek a következők:

a) nyilvános információ a TOE-ról (pl. az internetről);
b) korlátozott információ a TOE-ról (pl. a fejlesztő szervezeten belül ellenőrzött tudás, melyet más szervezetekkel csak titoktartási megállapodás keretében osztanak meg);
c) érzékeny információ a TOE-ról (pl. a fejlesztő szervezeten belül különböző csoportok között megosztott tudás, melyhez csak az érintett csoportok tagjai férhetnek hozzá).
d) kritikus információ a TOE-ról (pl. csak néhány személy által ismert tudás, melyhez való hozzáférés nagyon szoros ellenőrzés alatt áll szigorúan a „szükséges tudás" és az „egyéni elbírálás" elve alapján).

A TOE ismeretet a tervezési absztrakciónak megfelelően lehet fokozatokra osztani, még ha ezt csak TOE-nként különböző módon is lehet megtenni. Bizonyos TOE tervek lehetnek nyilvános forrásúak (vagy erősen támaszkodhatnak nyilvános forrásra), és ennélfogva még a terv reprezentáció is besorolható nyilvánosként vagy legfeljebb korlátozott hozzáférésűként, ugyanakkor más TOE-k esetében a megvalósítási reprezentáció nagyon szoros ellenőrzés alatt áll, minthogy olyan információkat adhat egy támadónak, amely elősegíthet egy támadást, és ennélfogva érzékenynek, sőt kritikusnak tekintik.

Előfordulhat, hogy többféle típusú ismeret szükséges. Ilyen esetekben a különböző ismeret elemek közül a legmagasabb fokút kell kiválasztani.

A ***lehetőség*** (alkalom) szintén fontos szempont, és összefüggésben áll a felhasznált idő szemponttal. Egy sebezhetőség azonosításához vagy kiaknázásához szükség lehet nagy mennyiségű hozzáférésre a TOE-hoz, ami növelheti a leleplezés valószínűségét. Bizonyos támadási módszerek a kiaknázás céljából tekintélyes erőfeszítéseket igényelhetnek off-line, és csak rövid idejű hozzáférést a TOE-hoz. Lehetséges, hogy a hozzáférés folyamatosan, vagy számos munkaszakaszon keresztül szükséges.

Bizonyos TOE-k esetében az alkalom egyenlőnek tekinthető a támadó által megszerzett TOE mintadarabok számával. Ez különösen akkor fontos, amikor a TOE-n való áthatolási kísérletek és az SFR-ek aláaknázása a TOE tönkretételéhez vezethetnek, meggátolva a szóbanforgó TOE mintadarab további tesztelését (pl. hardver készülékeknél). Az ilyen esetekben gyakran előfordul, hogy a TOE szétosztása ellenőrzött, így a támadónak erőfeszítéseket kell tennie a TOE további mintadarabjainak a megszerzésére.

Ennek a fejtegetésnek az esetében:

a) a szükségtelen/korlátlan hozzáférés azt jelenti, hogy a támadás nem igényli semmilyen fajta alkalom megvalósulását, minthogy nem áll fenn a leleplezés kockázata a TOE-hoz való hozzáférés során, és nem jelent problémát, ha számos TOE mintadarabhoz kell hozzájutni a támadás céljából;

b) a könnyű azt jelenti, hogy a hozzáférés egy napnál rövidebb ideig szükséges, és hogy a támadás végrehajtásához szükséges TOE mintadarabok száma tíznél kevesebb;
c) a mérsékelt azt jelenti, hogy a hozzáférés egy hónapnál rövidebb ideig szükséges, és hogy a támadás végrehajtásához szükséges TOE mintadarabok száma száznál kevesebb;
d) a nehéz azt jelenti, hogy a hozzáférés legalább egy hónapig szükséges, és hogy a támadás végrehajtásához szükséges TOE mintadarabok száma legalább száz;
e) a semmiképpen azt jelenti, hogy az alkalom nem elegendő a támadás végrehajtásához (az az időtartam, amíg a kiaknázandó érték rendelkezésre áll vagy érzékelhető, rövidebb a támadás végrehajtásához szükséges alkalomnál– például ha egy kulcs érték minden héten megváltozik, és a támadás két hetet igényelne); illetve a másik eset az, amikor a TOE mintadarabok nem állnak kellő számban rendelkezésre a támadás végrehajtásához a támadó számára – például, ha a TOE egy hardver, és nagyon magas annak a valószínűsége, hogy a TOE tönkremegy a támadás során, ahelyett, hogy a támadás sikeresen végződne, és a támadó a TOE-nak csak egy mintadarabjához fér hozzá.

Ennek a szempontnak a figyelembevétele arra a megállapításra vezethet, hogy nem lehetséges befejezni a kiaknázást az időigény miatt, amely nagyobb, mint az alkalom időtartama.

Az ***eszköz*** egy sebezhetőség azonosításához vagy kihasználásához szükséges informatikai hardver/szoftver vagy más berendezéseket jelenti.

a) A szabványos eszközök a támadó számára készen állnak, egy sebezhetőség azonosítására vagy egy támadáshoz. Ez az eszköz lehet TOE része (például operációs rendszerben egy debugger), vagy készen hozzáférhető (pl. Internet letöltés, egyszerű támadási scriptek).
b) A speciális eszközök olyan eszközök, amelyek nem állnak készen a támadó számára, de viszonylag könnyen meg tudja szerezni azokat. Megvásárolhat néhány eszközt (pl. áramfelvétel vizsgáló eszközök, az interneten keresztül összekapcsolt több száz PC ebbe a kategóriába tartoznak), vagy kifejleszthet, vehet nagyobb tudású támadási scripteket vagy programokat. Amennyiben egy támadás különböző lépései teljesen különböző speciális berendezéseket igényelnek, akkor ez „testre szabott eszközök” szintet jelent.
c) A testre szabott eszközök a nyilvánosság számára nem hozzáférhetőek, mivel előállításuk speciális módon történik (pl. nagyon kifinomult tudású szoftver), vagy az eszköz terjesztése különlegessége miatt ellenőrzött, esetleg korlátozott, illetve az ára nagyon magas. A nagyon drága eszközök is ebbe a kategóriába tartoznak.
d) A többszörösen testre szabott eszközök szintet arra a helyzetre vezették be, amikor különböző testre szabott eszközök szükségesek egy támadás különböző lépéseihez.

A TOE-vel kapcsolatos szakértelem és TOE ismeret azon személyek számára szükséges információkat jelenti, akik képesek a TOE támadására. Általában közvetett kapcsolat van egy támadó szakértelme (ahol a támadó több személy is lehet kiegészítő tudással) és egy támadásban az eszköz hatékony felhasználásának képessége között. Minél kisebb a támadó szakértelme, annál alacsonyabb a lehetősége a berendezés használatára (eszközök). Hasonlóan, minél nagyobb a szakmai tudása, annál nagyobb a lehetősége, hogy a berendezést a támadás során felhasználja. A szakértelem és az eszköz használata közötti fenti kapcsolat

nem mindig érvényes, például amikor környezeti intézkedések akadályozzák meg a szakértő támadó eszköz használatát, vagy amikor kevés szakértelmet igénylő, de hatékony támadó eszközök jelennek meg nyilvánosan hozzáférhető helyeken (például az interneten).

7.3.4.2.3. A támadó képesség számítása

A 8. táblázat az előző szakaszban ismertetett tényezőket azonosítja és kapcsolja számértékekhez.

Ahol egy tényező közel esik egy tartomány határához, ott az értékelőnek ajánlott megfontolnia egy közbülső érték használatát a 8. táblázatban. Ha például 20 minta szükséges egy támadás végrehajtásához, akkor egy 1 és 4 közötti érték választható erre a tényezőre, vagy ha a terv nyilvánosan elérhető, de a tervező néhány változtatást végzett ezen, akkor egy 0 és 4 közötti érték választható, attól függően, hogy az értékelő hogyan ítéli meg a terv változtatások hatását. A 8. táblázat útmutatás jellegű.

A 8. táblázatban a "**" jelölést az alkalom vonatkozásában nem kell úgy tekinteni, mintha az az előző sorokban megadott időintervallumoknak egy természetes sorrendben növekvő folytatása lenne. Ez a megjelölés azt jelenti, hogy bizonyos egyedi okok miatt a lehetséges sebezhetőséget nem lehet kihasználni a TOE-ban, a tervezett üzemeltetési környezetben. Például, a TOE-hoz való hozzáférést észlelni lehet egy bizonyos idő elteltével egy olyan ismert környezetben (vagyis egy rendszer esetében), ahol rendszeres járőrözést végeznek, és a támadó nem tud észrevétlenül hozzáférni a TOE-hoz a szükséges két hétig. Ez azonban nem vonatkozik egy hálózathoz csatolt TOE-ra (ahol távoli hozzáférés lehetséges), vagy ahol a TOE fizikai környezete ismeretlen.

Ahhoz, hogy megállapítsák a TOE ellenállóképességét a beazonosított lehetséges sebezhetőségekkel szemben, a következő lépéseket kell alkalmazni:

a) Meg kell határozni az {TF1, TF2, ..., TFn} lehetséges támadási forgatókönyveket a TOE-ra, annak az üzemeltetési környezetében.
b) Minden forgatókönyvre végre kell hajtani egy elméleti vizsgálatot, és ki kell számítani a vonatkozó támadó képességet a 8. táblázat felhasználásával.
c) Minden forgatókönyvre, ahol ez szükséges, végre kell hajtani az áthatolás tesztelést az elméleti vizsgálat megerősítése vagy megcáfolása céljából.
d) Az {TF1, TF2, ..., TFn} támadási forgatókönyveket két csoportra kell osztani:
   da) a sikeres támadási forgatókönyvek (vagyis azok, amelyek használatával aláaknázták az SFR-eket), és
   db) azok a támadási forgatókönyvek, amelyeknek az esetében szemléltetve lett, hogy sikertelenek.
e) Minden forgatókönyvre alkalmazni kell a 9. táblázatot, és meg kell állapítani, hogy van-e ellentmondás a TOE ellenálló-képessége és a megválasztott AVA_VAN garancia-összetevő között (lásd a 9. táblázat utolsó oszlopát).
f) Ha ellentmondás áll fenn, a sebezhetőség vizsgálat eredménye sikertelen; például amikor az ST szerzője az AVA_VAN.5 komponenst választotta ki, és egy 21-pontos (magas) támadó képességgel rendelkező támadási forgatókönyv feltörte a TOE biztonságát. Ebben az esetben a TOE a „mérsékelt” támadó képességgel rendelkező támadóval szemben ellenálló, ami ellentmond az AVA_VAN.5-nek, és emiatt a sebezhetőség vizsgálat eredménye sikertelen.

A 9. táblázatban az „érték” oszlop jelzi egy támadási forgatókönyvre vonatkozóan a támadó képesség értékek azon tartományát (amelyet a 8. táblázat felhasználásával számítottak ki), amely az SFR-ek aláaknázását eredményezi.

8. táblázat - A támadó képesség számítása

Tényező	**Érték**
Felhasznált idő	
<= 1 nap	0
<= 1 hét	1
<= 2 hét	2
<= 1 hónap	4
<= 2 hónap	7
<= 3 hónap	10
<= 4 hónap	13
<= 5 hónap	15
<= 6 hónap	17
> 6 hónap	19
Szakértelem	
hozzá nem értő	0
hozzáértő	3
szakértő	6
többszörös szakértő	8
TOE ismeret	
nyilvános	0
korlátozott	3
érzékeny	7
kritikus	11
Lehetőség	
Szükségtelen/korlátlan	0
Könnyű	1
Mérsékelt	4
Nehéz	10
semmiképpen	**
Eszköz	
szabványos	0
speciális	4
testre szabott	7
többszörösen testre szabott	9

9. táblázat - A sebezhetőség és a TOE ellenállás besorolása

érték	**a kihasználáshoz szükséges támadó képesség**	**a TOE ellenáll az alábbi támadó képességgel rendelkező támadónak**	**teljesített garancia-összetevő**	**nem teljesített garancia-összetevő**
0-9	alap	nincs besorolás	-	AVA_VAN.1 AVA_VAN.2 AVA_VAN.3 AVA_VAN.4 AVA_VAN.5
10-13	megemelt-alap	alap	AVA_VAN.1 AVA_VAN.2	AVA_VAN.3 AVA_VAN.4 AVA_VAN.5

érték	a kihasználáshoz szükséges támadó képesség	a TOE ellenáll az alábbi támadó képességgel rendelkező támadónak	teljesített garancia-összetevő	nem teljesített garancia-összetevő
14-19	Közepes	megemelt-alap	AVA_VAN.1 AVA_VAN.2 AVA_VAN.3	AVA_VAN.4 AVA_VAN.5
20-24	magas	közepes	AVA_VAN.1 AVA_VAN.2 AVA_VAN.3 AVA_VAN.4	AVA_VAN.5
>=25	magas feletti	magas	AVA_VAN.1 AVA_VAN.2 AVA_VAN.3 AVA_VAN.4 AVA_VAN.5	.

A bemutatott módszer nem tud figyelembe venni minden körülményt és tényezőt, de a szabványos besorolás eléréséhez szükséges támadással szembeni ellenállás szintjét viszonylag jól mutatja. Egyéb tényezők, például nem valószínű véletlen történések, vagy egy támadás befejeződés előtti észlelésének valószínűsége nem szerepel az alapmodellben.

Amíg több, egyedileg besorolt sebezhetőség magas szintű támadással szembeni ellenállást jelezhet, más sebezhetőségek megléte módosíthatja a táblázat értékeit úgy, hogy a sebezhetőségek kombinációja alacsonyabb végső besoroláshoz vezet. Egy sebezhetőség jelenléte megkönnyítheti mások kihasználását.

Ha egy ST szerzője fel akarja használni a támadó képesség táblázatot annak a támadási szintnek a meghatározásához, amelynek a TOE ellenáll (az AVA_VAN sebezhetőség vizsgálat komponens kiválasztásához), akkor a következőképpen járjon el: minden eltérő támadási forgatókönyvre (vagyis minden különböző típusú támadóra és/vagy különböző támadásra, amelyről a szerző tud), amelyeknek nem szabad megsérteniük az SFR-eket, menjen végig többször a 8. táblázaton a támadó képesség azon különböző értékeinek a meghatározásához, amelyeket az egyes ilyen sikertelen támadási forgatókönyvek felvehetnek. Ezután az ST szerzője válassza ki ezek közül a legmagasabb értéket abból a célból, hogy megállapítsa a TOE ellenálló-képességének azt a szintjét, amit a 5. táblázat alapján el kell várni: a TOE ellenálló-képességének legalább akkorának kell lennie, mint ez a megállapított legmagasabb érték. Például, ha minden olyan támadási forgatókönyvet figyelembe vettek, amelynek nem szabad aláaknáznia a TOE biztonsági szabályzatát, és a támadó képesség ilyen módon megállapított legmagasabb értéke „mérsékelt”, akkor a TOE ellenálló-képességének legalább „mérsékelt”-nek kell lennie (vagyis vagy „mérsékelt”, vagy „magas”), ennélfogva az ST szerzője vagy az AVA_VAN.4-et (mérsékelt esetén) vagy pedig az AVA_VAN.5-öt (magas esetén) választhatja megfelelő garancia-összetevőként.

7.3.5. Példa számítás közvetlen támadásra

A közvetlen támadásoknak kitett mechanizmusok gyakran létfontosságúak a rendszer biztonsága szempontjából, és a fejlesztők gyakran erősítik ezeket a mechanizmusokat. Például egy TOE felhasználhat egy egyszerű szám-kódot (belépési kódot) alkalmazó hitelesítési mechanizmust, amelyet legyőzhet egy támadó, akinek lehetősége van arra, hogy ismétlődően találgassa más felhasználók szám-kódjait. A rendszer erősítheti ezt a mechanizmust azzal,

hogy különféle módokon korlátozza a belépési kódokat és ezek használatát. Az értékelés végrehajtása során egy ilyen közvetlen támadásnak a vizsgálata a következőképpen folyhat le: Az ST-ből és a tervezési bizonyítékokból kitűnik, hogy a széles körben elérhető terminálokról a hálózati erőforrásokhoz való hozzáférés ellenőrzését az azonosítás és hitelesítés alapozza meg. A terminálokhoz a fizikai hozzáférést hatékonyan nem felügyelik, és nem ellenőrzik a terminálhoz való hozzáférés időtartamát sem. A rendszer jogosult felhasználói az első belépésükkor adják meg a belépési kódjukat, amely később módosítható felhasználói kérésre. A rendszer az alábbi követelményeket állítja a felhasználói belépési kóddal szemben:

a) a belépési kód legalább négy, legfeljebb hat számjegy lehet;
b) egymás utáni számsor nem megengedett (pl. 7,6,5,4,3);
c) ismétlődő számjegyek nem lehetnek (minden szám különböző legyen).

A belépési kód kiválasztásához a felhasználók annyi útmutatót kapnak, hogy a kód a lehető legvéletlenszerűbb legyen, és ne legyen társítható a felhasználóhoz semmilyen módon (ne legyen születési idő például).

A belépési kód tartománya az alábbiak szerint számítható:

a) Az emberi felhasználáshoz kötődő minták fontos szempontok, melyek befolyásolhatják a jelszó-tér vizsgálatának módját. Feltételezve a legrosszabb esetet (vagyis amikor a felhasználó csak négy számjegyből álló számot választ), minden jegy egyedisége esetén a belépési kód permutációinak száma: *7*8*9*10=5040*
b) A lehetséges növekvő sorozatok száma hét (0123, 1234,…6789), csakúgy, mint a csökkenő sorozatoké. A nem megengedett sorozatok számát az előző értékből levonjuk: *5040-14=5026*

A tervezési bizonyítékokban szereplő egyéb információk alapján ismert, hogy a belépési kód mechanizmusba terminál zárolási tulajdonságot építettek be. A hatodik sikertelen hitelesítési kísérlet után a terminál egy órára lezár. A sikertelen hitelesítési kísérlet számláló értéke öt perc után törlődik, így egy támadó minden öt percben legfeljebb öt kódot próbálhat ki (vagyis óránként 60-at).

Átlagban egy támadónak 2513 belépési kódot kell beütnie a helyes kód beírásához (mert ez az 5026 összes eset véletlenszerű kipróbálása esetén a várható érték), ami 2513 percet igényel. Ezért az átlagos sikeres támadás ideje így kicsit kevesebb, mint: *2513 perc (42 óra)*.

Azzal a megközelítési móddal, hogy kiszámítjuk a támadó képességet az előző fejezetben leírt módon, kimutatja, hogy egy nem hozzáértő személy hatálytalaníthatja a mechanizmust néhány nap alatt (feltéve a TOE-hoz való könnyű hozzáférést), szabvány berendezések használatával és semmiféle TOE ismeret mellett, azzal, hogy egy 1-es értéket ad eredményül. Mivel az eredmény 1, a sikeres támadás megvalósításához szükséges támadó képesség nincs besorolva, minthogy ez alacsonyabb tartományba esik, mint amit „alap”-nak tekintenek.

7.4. A CC/CEM v2.3 és v3.1 verzióinak összehasonlítása

Az alábbiak a v2.3 és v3.1 verziók közötti változások közül a MIBÉTS módszertant is érintő részeket tekintik át (biztonsági előirányzat, illetve EAL1 – EAL4).

7.4.1. A garanciaosztályok változásainak áttekintése

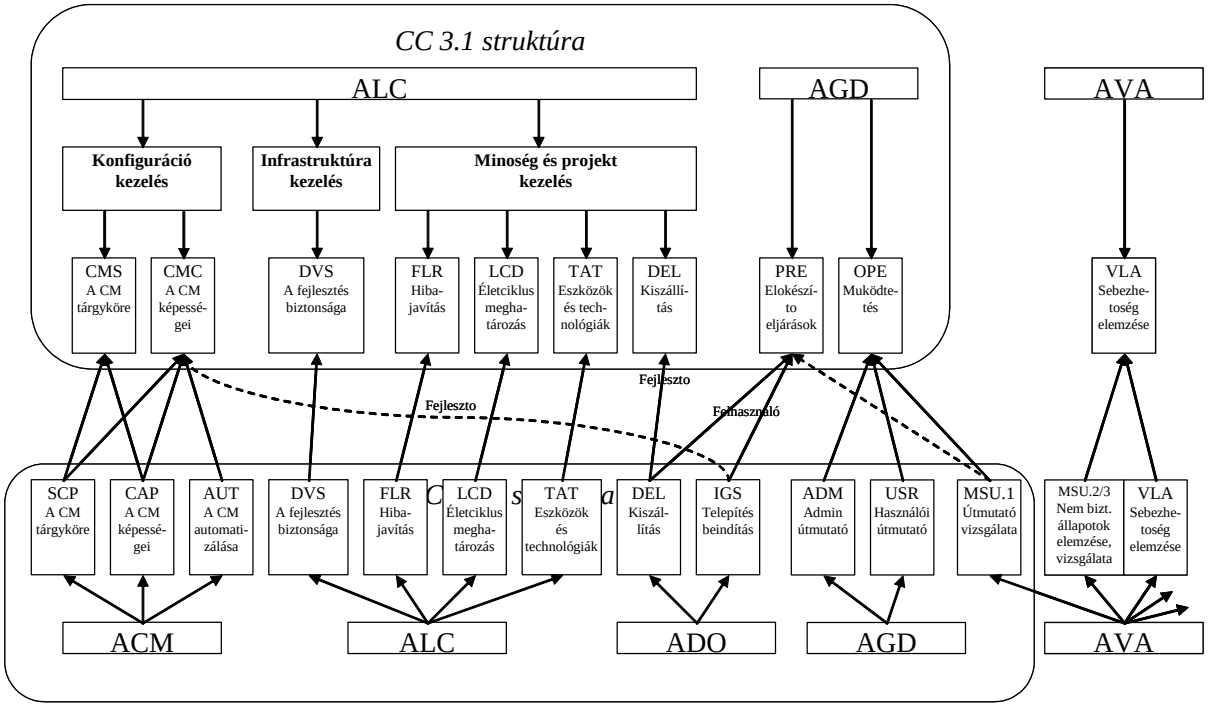
Az 10. táblázat a v2.3 és v3.1 verziók közötti változásokat a garanciaosztályok szintjén mutatja.

A táblázatból látható, hogy a korábbi 8 osztályból 6 lett, s többségük jelentősen változott.

10. táblázat - A garanciaosztályok változásainak áttekintése

Garanciaosztályok CC v2.3	**Garanciaosztályok CC v3.1**	**A változás jellemzése**
Biztonsági előirányzat értékelés (ASE)	Biztonsági előirányzat értékelés (ASE)	**Változott**, de csak az osztályon belül
Fejlesztés (ADV)	Fejlesztés (ADV)	**Változott**, de csak az osztályon belül
Útmutató dokumentumok (AGD)	Útmutató dokumentumok (AGD)	**Jelentősen változott,** a v3.1 AGD osztály a v2.3 AGD, ADO és AVA osztályok egyes elemeit tartalmazza
Konfiguráció kezelés (ACM)	---	**Jelentősen változott,** a v2.3 ACM osztály elemei a v3.1 ALC osztályba kerültek át
Szállítás (ADO)	---	**Jelentősen változott,** a v2.3 ADO osztály elemei a v3.1 ALC és AGD osztályba kerültek át
Életciklus támogatás (ALC)	Életciklus támogatás (ALC)	**Jelentősen változott,** a v3.1 ALC osztály lefedi a v2.3 ACM, és ALC elemeit, és az ADO egy részét
Tesztelés (ATE)	Tesztelés (ATE)	**Lényegében nem változott**
Sebezhetőség felmérés (AVA)	Sebezhetőség felmérés (AVA)	**Jelentősen változott,** a v2.3 AVA osztály MSU családja a v3.1 AGD-be került, a SOF család pedig megszűnt.

A további leírások szemléltetésére a 13. ábra a jelentősen megváltozott garanciaosztályokra család szinten bemutatja a v2.3 és v3.1 módosításait.



13. ábra - A 2.3 verzió osztályainak és családjainak leképezése a 3.1 verzió osztályaira és családjaira

7.4.2. A „Biztonsági előirányzat értékelés” (ASE) garanciaosztály változásai

11. táblázat - A Biztonsági előirányzat értékelés garanciaosztály változásai

Garanciaosztály	Garanciacsalád	EAL1	EAL2	EAL3	EAL4
v2.3 ASE	ASE_INT	1	1	1	1
	ASE_DES	1	1	1	1
	ASE_ENV	1	1	1	1
	ASE_OBJ	1	1	1	1
	ASE_REQ	1	1	1	1
	ASE_TSS	1	1	1	1
	ASE_PPC	1	1	1	1
	ASE_SRE	1	1	1	1
v3.1 ASE	ASE_INT	1	1	1	1
	ASE_ECD	1	1	1	1
	ASE_CCL	1	1	1	1
	ASE_OBJ	1	2	2	2
	ASE_REQ	1	2	2	2
	ASE_SPD	-	1	1	1
	ASE_TSS	1	1	1	1

A Biztonsági előirányzat értékelés garanciaosztály változásai egyrészt az ST szerkezetére vonatkozó elvárások módosulásából (egyszerűsítéséből) következnek, amit a 12. táblázat szemléltet:

12. táblázat - A biztonsági előirányzat elvárt szerkezetének változásai

A biztonsági előirányzat elvárt szerkezete **v2.3**	A biztonsági előirányzat elvárt szerkezete **v3.1**
ST bevezetés (ASE_INT) a) ST azonosítás b) Áttekintés c) CC megfelelés	ST bevezetés (ASE_INT) a) ST hivatkozás b) TOE hivatkozás c) TOE áttekintés d) TOE leírás
A TOE leírása (ASE_DES)	
	Megfelelőségi állítások (ASE_CCL) a) CC megfelelőség aa) CC verzió (melyhez az ST és TOE megfelelőséget állít) ab) ST megfelelőség a CC 2. részéhez képest (megfelel vagy kiterjeszti) ac) ST megfelelőség a CC 3. részéhez képest (megfelel vagy kiterjeszti) b) PP megfelelőség c) Biztonsági követelmény csomag megfelelőség (megfelel vagy szigorítja) d) A megfelelőségi állítások indoklása
A TOE biztonsági környezete (ASE_ENV) a) Feltételezések b) Fenyegetések c) Szervezeti biztonsági szabályzatok	Biztonsági probléma meghatározás (ASE_SPD) a) Fenyegetések b) Szervezeti biztonsági szabályzatok c) Működési környezetre vonatkozó feltételezések
Biztonsági célok (ASE_OBJ) a) A TOE biztonsági céljai b) A környezet biztonsági céljai	Biztonsági célok (ASE_OBJ) **ASE_OBJ.1:** a) Működési környezetre vonatkozó biztonsági célok **ASE_OBJ.2:** a) TOE-ra vonatkozó biztonsági célok b) Működési környezetre vonatkozó biztonsági célok c) A biztonsági célok indoklása
Közvetlenül kinyilvánított IT biztonsági követelmények (ASE_SRE)	Kiterjesztett biztonsági követelmények (ASE_ECD) a) Kiterjesztett funkcionális biztonsági követelmények b) Kiterjesztett garanciális biztonsági követelmények
IT biztonsági követelmények (ASE_REQ) a) TOE biztonsági követelmények aa) funkcionális követelmények ab) garanciális követelmények b) A környezet biztonsági követelményei	Biztonsági követelmények (ASE_REQ) **ASE_REQ.1**: a) funkcionális biztonsági követelmények b) garanciális biztonsági követelmények **ASE_REQ.2**: a) funkcionális biztonsági követelmények b) garanciális biztonsági követelmények c) indoklás (az SFR-ek teljesítik a TOE összes biztonsági célját) d) indoklás (miért az adott SAR-t választották.)

TOE összefoglaló előírás (ASE_TSS) a) TOE biztonsági funkciók b) garanciális intézkedések	TOE összefoglaló előírás (ASE_TSS) **ASE_TSS.1**: a) leírás (a TOE hogyan teljesíti az egyes SFR-eket) **ASE_TSS.2**: a) leírás (a TOE hogyan teljesíti az egyes SFR-eket) b) leírás (a TOE hogyan védi meg magát a beavatkozás és a logikai meghamisítás ellen) c) leírás (a TOE hogyan védi meg magát a megkerülés ellen)
PP megfelelőségi nyilatkozat (ASE_PPC)	

A biztonsági előirányzat értékelés garanciaosztály változásai másrészt abból következnek, hogy a v2.3 egységes követelményeit a v3.1-ben felváltja a két szintű garancia:

- EAL1 esetén az alacsony garanciát biztosító ST (ASE_OBJ.1, ASE_REQ.1, ASE_TSS.1)
- EAL2 - EAL4 esetén a normál ST (ASE_OBJ.2, ASE_REQ.2, ASE_TSS.2)

7.4.3. A „Fejlesztés” (ADV) garanciaosztály változásai

13. táblázat - A Fejlesztés garanciaosztály változásai

Garanciaosztály	Garanciacsalád	EAL1	EAL2	EAL3	EAL4
v2.3 ADV	ADV_FSP	1	1	1	2
	ADV_HLD	-	1	2	2
	ADV_LLD	-	-	-	1
	ADV_IMP	-	-	-	1
	ADV_RCR	1	1	1	1
	ADV_SPM	-	-	-	1
v3.1 ADV	ADV_ARC	-	1	1	1
	ADV_FSP	1	2	3	4
	ADV_TDS	-	1	2	3
	ADV_IMP	-	-	-	1

A 3.1 verzióban megjelenő ADV_ARC család a biztonsági architektúra leírásával kapcsolatban fogalmaz meg új követelményeket, melyek a TOE önvédelmének, tartomány szétválasztásnak, a biztonsági funkciók megkerülhetetlenségének leírására vonatkoznak, ideértve azt is, hogy ezeket az elveket miként támogatják a TSF inicializálásához használt TOE elemek.

Az ADV_FSP család a TSF interfészeivel kapcsolatban fogalmaz meg követelményeket. A 2.3 verzióhoz képest az összetevők elnevezése és szerkezete, jelentése is módosult. Az új verzió megkülönböztet:

- **SFR-t érvényre juttató interfészt:** ha az ST-ben szereplő SFR-re visszavezethető interfészen keresztül rendelkezésre álló műveletet jelent;
- **SFR-t támogató interfészt:** olyan műveletek interfészei, amelyektől SFR-t érvényre juttató funkcionalitás függ, de csak a TOE biztonsági szabályzatának a fenntartása érdekében szükséges a helyes működésük;
- **SFR-be nem beavatkozó interfészt:** olyan műveletek interfészei, amelyektől nem függ SFR-t érvényre juttató funkcionalitás.

Az új verzióban megjelenő ADV_TDS család (TOE terv) a v2.3 magas-szintű (ADV_HLD) és alacsony-szintű (ADV_LLD) terveit helyettesíti. Követelményeinek célja, hogy kielégítő mennyiségű és minőségű információ szülessen annak megállapításához, hogy a funkcionális biztonsági követelmények valóban megvalósulnak. Az EAL szintek emelésével a tervezés elvárt részletessége is nő, alrendszer majd modulszintű lebontást megkövetelve.

Az ADV_IMP család változatlan (mindkét verzióban azt tűzi ki célul, hogy rendelkezésre kell bocsátani a TOE implementációs reprezentációját az értékelő számára vizsgálható formában).

7.4.4. Az „Útmutató dokumentumok” (AGD) garanciaosztály változásai

14. táblázat - Az Útmutató dokumentumok garanciaosztály változásai

Garanciaosztály	Garanciacsalád	EAL1	EAL2	EAL3	EAL4
v2.3 AGD	AGD_ADM	1	1	1	1
	AGD_USR	1	1	1	1
v2.3 ADO	ADO_DEL	-	1	1	2
	ADO_IGS	1	1	1	1
v2.3 AVA	AVA_MSU	-	-	1	2
v3.1 AGD	AGD_PRE	1	1	1	1
	AGD_OPE	1	1	1	1

7.4.4.3. Felhasználói működtetési útmutató (AGD_OPE)

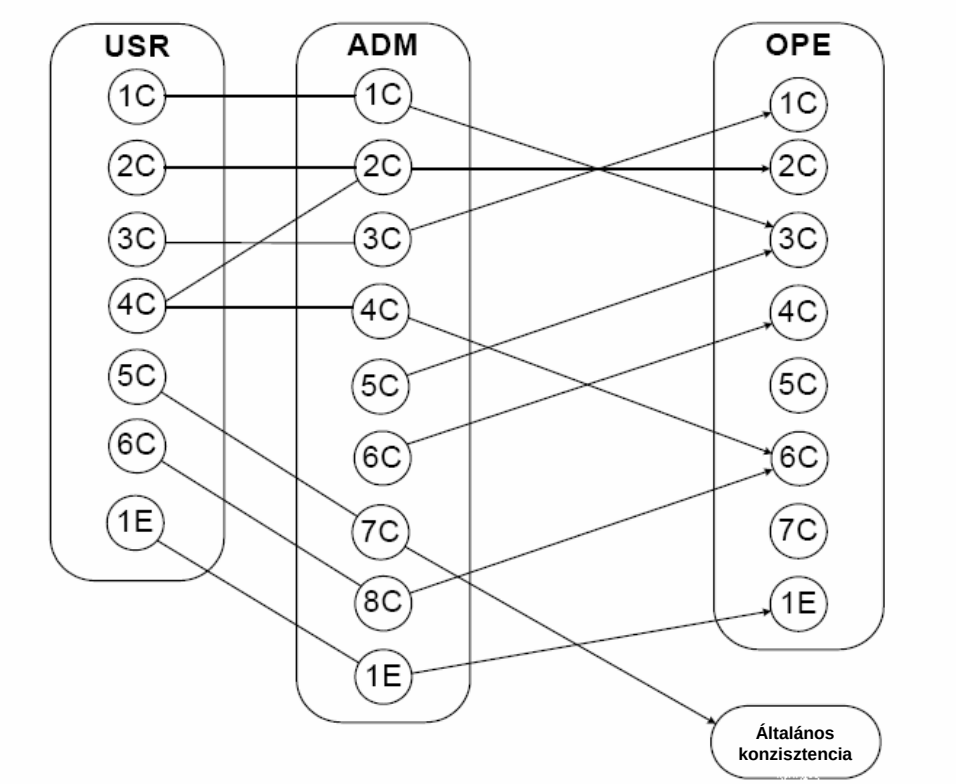
A v2.3 AGD osztálya két családot tartalmazott: AGD_ADM (Adminisztrátori útmutató) és AGD_USR (Felhasználói útmutató). Mivel a két család elemei és munkaegységei igen hasonlóak voltak, és csupán különböző felhasználói körhöz kapcsolódtak, ezért az új verzióban egy család fogja össze a követelményeiket, és ahogy a neve is mutatja, a család a TOE-t működés közbeni állapotában vizsgálja.

A különböző felhasználói körökkel a most bevezetett szerepkör elv foglalkozik. Az értékelések nagy részénél a „végfelhasználó” és az „adminisztrátor” szerepkörök fordulnak elő, melyek tovább finomíthatók szükség esetén.

A CC korábbi verziójában az AGD nyilvánvalóan a TOE működési szakaszához kötődött, az ADO_IGS pedig az előkészítő szakaszhoz. Elképzelhető, hogy a TOE-hoz szükség van utasításokra a telepítési fázisban, de nem a végfelhasználói szakaszban a karbantartáshoz. Ezért az új verzióban az AGD_OPE nem függ az AGD_PRE család összetevőjétől, ellentétben a korábbi verzióval, ahol az ADO_IGS.1 függősége volt az AGD_ADM.1.

Az AGD_OPE elemek az új verzióban nem hivatkoznak kifejezetten az adminisztrátorra vagy a felhasználókra, hanem minden felhasználói szerepkörre vonatkoznak. Az új AGD_OPE elemek szövegezésére történt kihatás oka, hogy az ASE is változott az új verzióban. A követelmények nem az ST-ben szereplő feltételezésekre, hanem a biztonsági célokra vonatkoznak, másészt nem különböztetik meg az IT és nem-IT környezetet. Az új struktúrában magasabb szintű konzisztencia (ellentmondás-mentességi) követelményt vezettek be.

A 14. ábra a korábbi és az új AGD osztály elemeit ábrázolja.



14. ábra: A Felhasználói üzemeltetési útmutató család elemeinek megfeleltetése

7.4.4.4. Előkészítő eljárások (AGD_PRE)

Az előkészítés folyamata megköveteli, hogy a TOE leszállított példányát a felhasználó átvegye, konfigurálja és aktiválja annak bizonyítása céljából, hogy a TOE működtetése során aktívak lesznek a szükséges védelmi tulajdonságok. Az előkészítő eljárások biztosítják azt a garanciát, hogy a felhasználó tisztában lesz a TOE konfigurációs paramétereivel és hogy ezek hogyan befolyásolják a TSF-et.

A CC v3.1 AGD_PRE családjában a korábbi verzió ADO osztályának összetevői realizálódnak a CC revíziók során tapasztalt észrevételek alapján.

A v2.3-as ADO_DEL család követelményei között a szállítással kapcsolatban vannak felhasználóra vonatkozó tevékenységek is, nevezetesen a leszállított TOE átvételi eljárásai. Ezeket az új AGD_PRE családban kell kezelni, hiszen a TOE működésének előkészítésével kapcsolatosak.

Kétféle átvételi eljárás különböztethető meg:

- Alap szintű átvételi eljárások: a felhasználónak meg kell állapítania, hogy a leszállított TOE valóban az értékelt példány-e. Ez valószínűleg a TOE tanúsítvány címkéjének ellenőrzésével állapítható meg.
- Emelt szintű átvételi eljárások: ha a szállítási eljárások megkövetelik a módosítás/megszemélyesítés észlelését is, ekkor a felhasználónak végre kell hajtania a

vonatkozó átvételi eljárás lépéseit a leszállított TOE-ra a fejlesztői intézkedések végrehajtása céljából.

A felhasználói telepítés, generálás és indítási eljárások a 2.3-as verzió ADO_IGS családjának a fő szempontjai. Az új szerkezet ezeket is az AGD_PRE család keretén belül kezeli. A régi ADO_IGS.1 az AGD_PRE.1-be került, a másik összetevő, az ADO_IGS.2 pedig egyik EAL szinten sem jelenik meg, így nem szerepel az új szerkezetben.

7.4.5. Az „Életciklus támogatás” (ALC) garanciaosztály változásai

15. táblázat - Az Életciklus támogatás garanciaosztály változásai

Garanciaosztály	Garanciacsalád	EAL1	EAL2	EAL3	EAL4
v2.3 ACM	ACM_CAP	1	2	3	4
	ACM_SCP	-	-	1	2
	ACM_AUT	-	-	-	1
v2.3 ADO	ADO_DEL	-	1	1	2
v2.3 ALC	ALC_DVS	-	-	1	1
	ALC_LCD	-	-	-	1
	ALC_TAT	-	-	-	1
v3.1 ALC	ALC_CMC	1	2	3	4
	ALC_CMS	1	2	3	4
	ALC_DEL	-	1	1	1
	ALC_DVS	-	-	1	1
	ALC_LCD	-	-	1	1
	ALC_TAT	-	-	-	1

7.4.5.5. CM hatáskör és CM képességek (ALC_CMS, ALC_CMC)

A CC v2.3 verziójában az ACM (Konfiguráció kezelés) osztályon belül a CM képességek család (ACM_CAP) tartalmazott hatáskörre vonatkozó megfontolásokat is, és fordítva, a CM hatáskör család (ACM_SCP) képességekre vonatkozó követelményeket is tartalmazott. Az új struktúra e két családot az alábbi módon különíti el:

- A hatáskörnek le kell írnia a konfiguráció lista minimális tartalmát (a konfiguráció lista adja meg a konfiguráció tételeket, amelyek a CM hatálya alatt kezelendők), és nem ró követelményt a CM rendszer képességeire.
- A képességeknek le kell írniuk a CM rendszer minimális képességeit, és nem szabad feltételezéssel élniük a CM rendszer hatáskörérével kapcsolatban.

Ez az elkülönítés növeli az egyértelműséget (így csökkentve a fejlesztői és értékelői erőfeszítéseket, és növelve az átláthatóságot harmadik felek számára), valamint a rugalmasságot is, mivel a hatáskörre és képességre vonatkozó követelmények egymástól függetlenül választhatók.

Az új családok a 3.1 verzióban az ALC osztály alá kerültek:

- ALC_CMS (CM hatáskör);
- ALC_CMC (CM képesség).

Az új verzió bevezetett egy új hatáskör összetevőt (A TOE részeinek CM lefedettsége) és a CMC követelményekben az absztraktabb “konfiguráció tételek” szerepelnek a “TOE-t alkotó komponensek” helyett.

7.4.5.6. Szállítás (ALC_DEL)

A szállítás az életciklus azon szakasza, amikor a kész TOE az előállítási környezetből a felhasználó hatáskörébe kerül. Beletartozhat a csomagolás és tárolás a fejlesztői telephelyen, de nem terjed ki a befejezetlen TOE vagy részeinek különböző fejlesztői színhelyek közötti továbbítására. Ennek a családnak a fókuszában a befejezett TOE-nak a felhasználóhoz való biztonságos továbbítása áll.

A 2.3 CC verzió ADO_DEL családja szinte kizárólag a fejlesztői szállítási eljárásokkal foglalkozott. Az új struktúra ezeket a követelményeket az ALC osztály különálló családjába, az ALC_DEL-be mozgatta át. Az ALC_DEL a kész TOE-nak a fejlesztői környezetből a felhasználóhoz való biztonságos továbbításának folyamatával foglalkozik. A szállítási fázis végén a TOE a felhasználó felügyelete alá kerül, ő a felelős érte. Ez nem feltétlenül esik egybe a TOE-nak a felhasználó telephelyére való érkezésével.

Az új verzió a három DEL összetevőt egybeolvasztotta, és megköveteli, hogy a fejlesztő vegye figyelembe mindazon biztonsági szempontokat, melyeket a PP/ST megkövetel a szóban forgó TOE-ra, és a választott AVA_VAN-nal arányban álló védelmet biztosítson hozzá.

7.4.5.7. A fejlesztés biztonsága (ALC_DVS)

A család a fejlesztői környezetben használt fizikai, eljárásrendi, személyi és egyéb biztonsági intézkedéseket fedi le. Tartalmazza a fejlesztői helyszín(ek) fizikai biztonságát, és felügyeli a fejlesztői állomány kiválasztását és szerződtetését. Az ALC_DVS két összetevője megmaradt, kisebb változások történtek csak az összetevőkön belül.

7.4.5.8. Az életciklus meghatározása (ALC_LCD)

Az életciklus definíció annak alapját teremti meg, hogy a fejlesztő által a TOE előállításához használt fejlesztés, gyártás gyakorlata terjedjen ki a fejlesztési folyamatban és a működtetési támogatás követelményeiben azonosított szempontokra és tevékenységekre.
Az új verzióban a család első és utolsó összetevője megmaradt, a szabványosított életciklussal foglalkozó második kikerült a követelményrendszerből.
A fejlesztői környezet értékeléséhez az értékelőnek meg kell ismernie a fejlesztő által használt életciklus modellt. Ezért ésszerű, hogy a fejlesztő megadja az értékelő számára az alkalmazott életciklus modellt. Mivel a fejlesztői környezetre vonatkozó értékelés EAL3 szinten történik, az ALC_LCD.1 az EAL4-ről EAL3 szintre került.

7.4.5.9. Eszközök és technikák (ALC_TAT)

Az eszközök és technikák család a TOE fejlesztéséhez, vizsgálatához és implementálásához használt eszközök kiválasztásának szempontjaival foglalkozik. Jól meghatározott, konzisztens és helyesen működő eszközök használatát követeli meg a TOE fejlesztéséhez.
A család három összetevője és ezek jelentése nem változott, csupán az összetevőkön belül történtek kisebb módosítások.

7.4.6. A „Tesztelés" (ATE) garanciaosztály változásai

16. táblázat - A Tesztelés garanciaosztály változásai

Garanciaosztály	Garanciacsalád	EAL1	EAL2	EAL3	EAL4
v2.3 ATE	ATE_FUN	-	1	1	1
	ATE_COV	-	1	2	2
	ATE_DPT	-	-	1	1
	ATE_IND	1	2	2	2
v3.1 ATE	ATE_FUN	-	1	1	1
	ATE_COV	-	1	2	2
	ATE_DPT	-	-	1	2
	ATE_IND	1	2	2	2

A Tesztelés garanciaosztály követelményei lényegében nem változtak.

Az egyetlen különbség az EAL4-es szintű tesztelés mélységével kapcsolatos. A v3.1 ATE_DPT.2 nemcsak azt várja el, hogy a tesztelés mélységi elemzés megmutassa, hogy a TOE tervben szereplő minden TSF alrendszert leteszteltek, hanem azt is, hogy az SFR-t érvényre juttató modulokat (azaz a TOE tervben leírt SFR-t érvényre juttató modulok minden interfészét) letesztelték.

7.4.7. A „Sebezhetőség felmérés" (AVA) garanciaosztály változásai

17. táblázat - A Sebezhetőség felmérés garanciaosztály változásai

Garanciaosztály	Garanciacsalád	EAL1	EAL2	EAL3	EAL4
v2.3 AVA	AVA_MSU	-	-	1	2
	AVA_SOF	-	1	1	1
	AVA_VLA	-	1	1	2
v3.1 AVA	AVA_VAN	1	2	2	3

Szemben a CC v2.3 AVA-n belüli családszerkezettel, a 3.1-es verzió csupán egy családot tartalmaz: AVA_VAN (Sebezhetőségi elemzés) jelöléssel, és azt a fenyegetést fedi le, amit egy támadó jelent olyan hibák felfedezésével, amelyek jogosulatlan hozzáférést adnak számára adatokhoz és funkcionalitáshoz, lehetővé teszik, hogy beavatkozzon a TSF-be vagy módosítsa annak működését, illetve beavatkozzon jogosult felhasználók műveleteibe.
A család összetevőinek szintjei az értékelő által elvégzendő sebezhetőségi elemzés emelkedő szigora, illetve a lehetséges sebezhetőségek támadó általi azonosításához szükséges támadási potenciál szintjei szerint különböznek.

A korábbi CC verziókkal ellentétben, a 3.1 verzió nem írja elő, hogy a fejlesztő végezzen sebezhetőségi elemzést és dokumentálja azt. Ezen osztály összes követelménye az értékelő által végrehajtandó elemzési, dokumentálási és tesztelési tevékenységekkel foglalkozik.

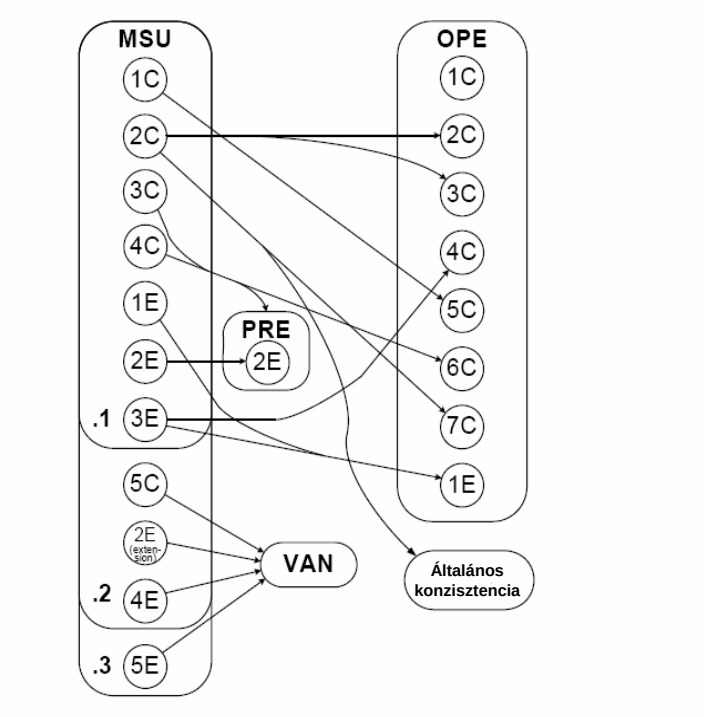
A v3.1 ADV_ARC teljesítéséhez elvégzendő biztonsági szerkezet leírás azonban egyfajta fejlesztői sebezhetőségi elemzésnek tekinthető, abban az értelemben, hogy ennek indokolnia kell, hogy a TSF miért megbízható, és miért juttatja érvényre az összes funkcionális biztonsági követelményt.

Mivel az AVA_MSU és AGD_OPE családok között tekintélyes redundancia állt fenn a korábbi verzióban, ezért az AVA_MSU család az új verzióban beleolvadt az AGD osztályba, míg a nem redundáns információi más családokba kerültek.

Az első MSU összetevő szorosan kapcsolódik az AGD_OPE családhoz, mely utóbbi követelményei lefedik az MSU.1-et, illetve kiegészültek a többletinformációkkal.

A régi magasabb MSU összetevők nem illenek az AGD-be, mivel az útmutató dokumentáció fejlesztő általi elemzését igénylik. Ez tekinthető a sebezhetőségi elemzés speciális esetének, így ez a két összetevő számára a megfelelő hely az AVA_VAN család.

A 15. ábra a v2.3 verzió AVA_MSU családjának beépülését szemlélteti a v3.1 verzióba.



15. ábra - A Visszaélés/helytelen használat család elemeinek megfeleltetése

8. Bibliográfia

9. Rövidítésgyűjtemény

A 18. táblázat a dokumentumban használt rövidítéseket mutatja be.

18. táblázat – A dokumentumban használt rövidítések

Rövidítés	Angol	Magyar
A	-	Alap (értékelési) garanciaszint
ACO	Assurance: Composition	“Kompozíció-összeállítás” garanciaosztály
ADV	Assurance: Development	“Fejlesztés” garanciaosztály
ADV_ARC	ADV: Functional specification	Funkcionális specifikáció garanciacsalád
ADV_FSP	ADV: Functional specification	Funkcionális specifikáció garanciacsalád
ADV_IMP	ADV: Implementation representation	Megvalósítási reprezentáció garanciacsalád
ADV_TDS	ADV: TOE design	TOE terv garanciacsalád
AGD	Assurance: Guidance documents	“Útmutató dokumentumok” garanciaosztály
AGD_OPE	AGD: Operational user guidance	Üzemeltetési felhasználói útmutató garanciacsalád
AGD_PRE	AGD: Preparative procedures	Előkészítő eljárások garanciacsalád
ALC	Assurance: Life cycle support	“Életciklus támogatás” garanciaosztály
ALC_CMC	ALC: CM capabilities	A konfiguráció kezelés (CM) képességei garanciacsalád
ALC_CMS	ALC: CM scope	A konfiguráció kezelés (CM) hatásköre garanciacsalád
ALC_DEL	ALC: Delivery	Szállítás garanciacsalád
ALC_DVS	ALC: Development security	A fejlesztés biztonsága garanciacsalád
ALC_FLR	ALC: Flaw remediation	Hibajavítás garanciacsalád
ALC_LCD	ALC: Life cycle definition	Életciklus meghatározás garanciacsalád
ALC_TAT	ALC: Tools and techniques	Eszközök és technikák garanciacsalád
ASE	Assurance: Security Target evaluation	“Biztonsági előirányzat értékelés” garanciaosztály
ASE_INT	ASE: Introduction	ST bevezetés garanciacsalád
ASE_CCL	ASE: Conformance claims	Megfelelőségi nyilatkozatok garanciacsalád
ASE_SPD	ASE: Security problem definition	Biztonsági probléma meghatározás garanciacsalád
ASE_OBJ	ASE: Security objectives	Biztonsági célok garanciacsalád
ASE_ECD	ASE: Extended components definition	Kiterjesztett összetevő meghatározás garanciacsalád
ASE_REQ	ASE: IT security requirements	IT biztonsági követelmények garanciacsalád
ASE_TSS	ASE: TOE summary specification	TOE összefoglaló előírás garanciacsalád
ATE	Assurance: Tests	“Tesztelés” garanciaosztály
ATE_COV	ATE: Coverage	Lefedettség garanciacsalád
ATE_DPT	ATE: Depth	Mélység garanciacsalád
ATE_FUN	ATE: Functional tests	Funkcionális tesztek garanciacsalád
ATE_IND	ATE: Independent testing	Független tesztelés garanciacsalád
AVA	Assurance: Vulnerability assessment	“Sebezhetőség felmérés” garanciaosztály
AVA_VAN	ATE: Vulnerability analysis	Sebezhetőségi elemzés garanciacsalád
CC	Common Criteria	Közös szempontok
CEM	Common Evaluation Methodology	Közös értékelési módszertan
CM	Configuration Management	Konfiguráció kezelés
EAL	Evaluation Assurance Level	Értékelési garanciaszint
ETR	Evaluation Technical Report	Értékelési jelentés
F	-	Fokozott (értékelési) garanciaszint
FAU	Functionality: Security audit	„Biztonsági naplózás” funkcionális osztály
FCO	Functionality: Communication	„Kommunikáció” funkcionális osztály
FCS	Functionality: Cryptographic support	„Kriptográfiai támogatás” funkcionális osztály
FDP	Functionality: User data protection	„A felhasználói adatok védelme” funkcionális osztály

Rövidítés	Angol	Magyar
FIA	Functionality: Identification and authentication	„Azonosítás és hitelesítés” funkcionális osztály
FMT	Functionality: Security management	„Biztonsági menedzsment” funkcionális osztály
FPR	Functionality: Privacy	„A magántitok védelme” funkcionális osztály
FPT	Functionality: Protection of the TOE Security Functions	„A TOE biztonsági funkciók védelme” funkcionális osztály
FRU	Functionality: Resource utilisation	„Erőforrás gazdálkodás” funkcionális osztály
FTA	Functionality: TOE access	„TOE hozzáférés” funkcionális osztály
FTP	Functionality: Trusted path/channels	„Megbízható útvonal/csatornák” funkcionális osztály
IT	Information Technology	Információs technológia, informatika
K	-	Kiemelt (értékelési) garanciaszint
MIBÉTS		Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma
OSP	Organisational Security Policy	Szervezeti biztonsági szabályzat
OR	Observation Report	Észrevételezési jelentés
PP	Protection Profile	Védelmi profil
SAR	Security Assurance Requirement	Garanciális biztonsági követelmény
SFR	Security Functional Requirement	Funkcionális biztonsági követelmény
ST	Security Target	Biztonsági előirányzat
TOE	Target of Evaluation	Értékelés tárgya
TSF	TOE Security Functionality	A TOE biztonsági funkcionalitása
TSFI	TOE Security Functions Interface	A TOE biztonsági funkcionalitás interfésze

10. Fogalomtár

11. Ábrák

12. Képek

13. Táblázatok

14. Verziószám

V4