e-Közigazgatási Keretrendszer Kialakítása

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

Új Magyarország Fejlesztési Terv

ÖSSZETETT 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 (Title)	Összetett termékekre vonatkozó értékelési módszertan
Kulcsszó (Subject)	IT biztonság; értékelés; módszertan
Leírás (Description)	Az elkészült e-közigazgatási alkalmazásokat használatbavétel előtt meg kell vizsgálni, hogy megfelelnek-e a rájuk vonatkozó biztonsági követelményeknek. A biztonság (termékekre irányuló) értékelési módszertana a követelménytárban megtalálható. A jelen dokumentumban leírtak a termékekre irányuló biztonság értékelés módszertanának kiegészítését jelentik. Olyan összetett termékek értékelésre használható, melyeket már (termékként) értékelt komponensek integrálásával állítottak elő.
Típus (Type)	Szöveg, táblázat, ábra
Forrás (Source)	
Kapcsolat (Relation)	e-Közigazgatási Keretrendszer egyéb dokumentumai
Terület (Coverage)	KOP-ok során megvalósuló projektek, központi IT fejlesztési projektek
Létrehozó (Creator)	e-Közigazgatási Keretrendszer Kialakítása projekt
Kiadó (Publisher)	Miniszterelnöki Hivatal
Résztvevő (Contributor)	Hunguard Kft.
Jogok (Rights)	e-Közigazgatási Keretrendszer
Dátum (Date)	2008.09.19.
Formátum (Format)	.doc
Azonosító (Identifier)	
Nyelv (Language)	Magyar
Verzió	V4
Státusz	Végleges
Fájlnév	EKK_ekozig_osszetett_termek_ertekelese_080919_V4.doc
Méret	
Ár	
Felhasználási jogok	Korlátlan

Verziókövetési táblázat

A dokumentum neve	Összetett 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	179
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.

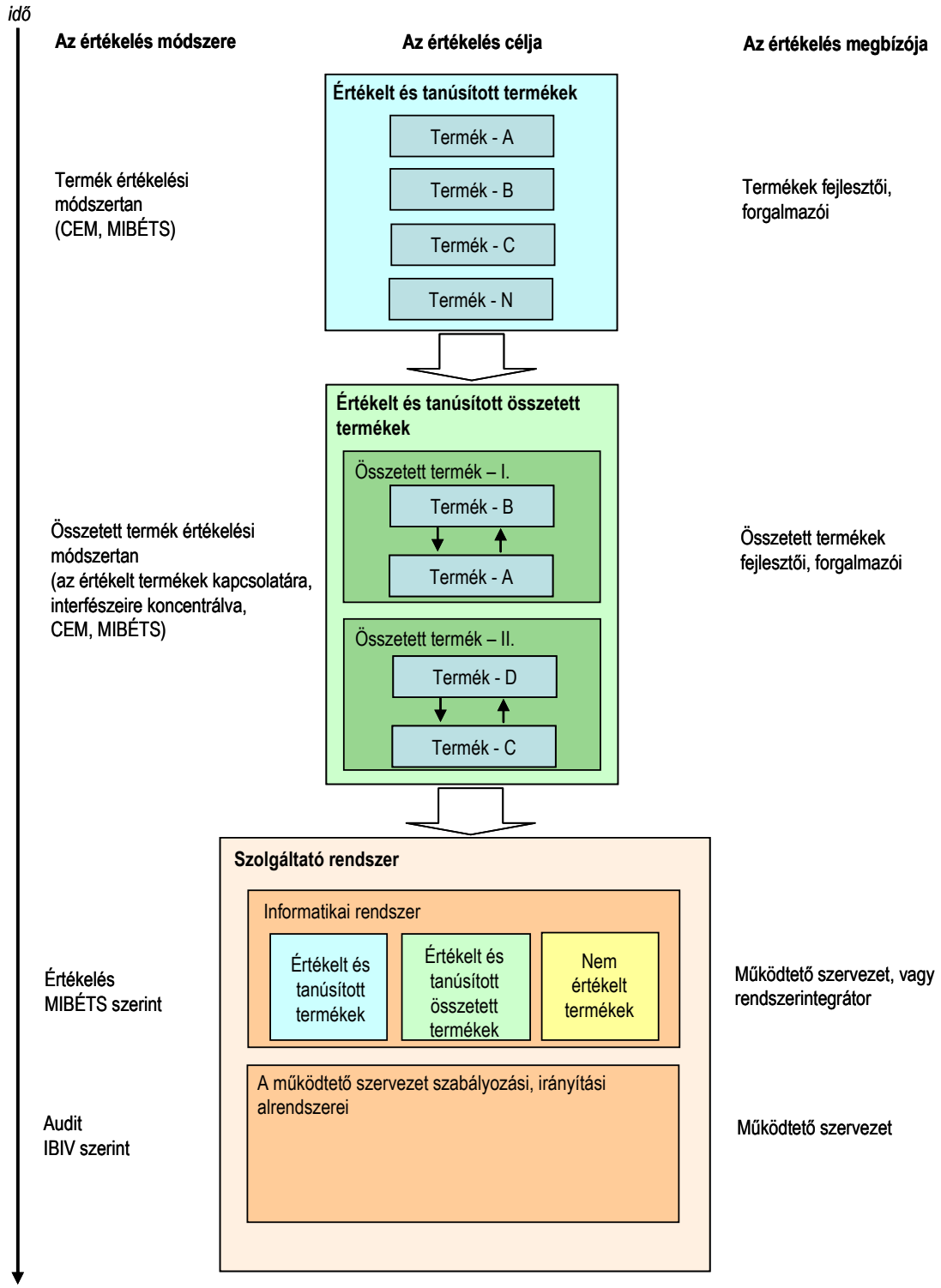
Az informatikai biztonságot technológiai szempontból kezelő értékelői módszertan az alábbi dokumentumokból áll:

- Termékekre vonatkozó értékelési módszertan [3],
- Összetett termékekre vonatkozó értékelési módszertan (jelen dokumentum),
- 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 köztes helyet képvisel:

- a termékekre vonatkozó értékelési módszertanra [3] épül, hiszen az összetett termékeket már (termékként) értékelt komponensek integrálásával állítják elő,
- 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 [9] 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 (ez csak a CC tanúsítványokra vonatkozik), de segítségükkel az adott országban működő szervezetek mégis garanciát szerezhetnek a termékek biztonságáról.

Akár CC szerint, akár a hazai séma egyszerűsített módszertana alapján tanúsított egy termék, ez csak az első lépés a megbízhatóan működő informatikai rendszerek biztosításához.

A végső célt (működő, szolgáltató informatikai rendszerek értékelését) elősegítő következő lépés a már értékelt és tanúsított termékekből integrált bonyolultabb alrendszerek (összetett termékek) értékelési módszertana. Természetesen a termék értékelési módszertan vizsgálati tárgya is lehet nagyon összetett, sok-komponensű. Jelen dokumentumban összetett termék alatt egy (vagy több) szolgáltató komponensből és egy (vagy több kliens alkalmazásból (komponensből) álló egységet értünk, ahol a szolgáltató komponens biztonsági szolgáltatásokat nyújt a kliens komponensnek (a szerepek fel is cserélődhetnek). Az összetett termék értékelése akkor segíti az értékelési folyamatot, ha

- A szolgáltató komponens(ek) már értékelve van, és az értékelés folyamán nem vették vizsgálat alá az összes kliens által aktivizált szolgáltatói interfészt (tipikus példa egy adott, értékelt operációs rendszer és az ennek szolgáltatásait kihasználó alkalmazás együttese);
- A szolgáltató-kliens komponensek adott kapcsolata önálló termékként (nem csak egy adott működő rendszerben) megjelenhet, így azokat nem kell minden szolgáltatói működő rendszerben külön-külön értékelni.

Jelen dokumentumban leírt módszertan a működő rendszerértékelés költség- és időhatékonyságát szolgálja.

Az összetett termékek értékelési módszertanára jelen dokumentum az [1] és [2] által bevezetett megközelítést alkalmazza: már értékelt és tanúsított komponensekből integrált összetett terméket úgy értékel, hogy maximálisan felhasználja a korábbi eredményeket, és az integrálás eredményének csak azokra a belső kapcsolataira koncentrál, amely az eredeti komponens értékelések során nem kapott kellő figyelmet.

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 az összetett termékek fejlesztőinek, integrátorainak ad útmutatást.

A 6.1.1 alfejezet áttekinti az összetett TOE integrálás (komponens-összeállítás) modelljét: a szolgáltatásokat nyújtó „kiszolgáló komponens”, illetve a szolgáltatásokat igénybe vevő „kliens komponens” egyedekből modulárisan összeállítható, bonyolultabb alrendszereket is felépíteni képes eljárást. Az alfejezet leírja a komponens-összeállítás tipikus megvalósítási formáit, valamint az eredményét képező összetett TOE-k értékelésének néhány speciális megközelítési módját.

A 6.1.2 alfejezet előzetesen áttekinti, valamint „ellenőrző lista”-ként használható módon felsorolja azokat a fejlesztői/integrátori feladatokat (a későbbi részletekre való hivatkozással), amelyeket egy összetett termék biztonsági értékelésének előkészítése érdekében kell elvégezni (a különböző garanciacsomagok szerint elkülönített csoportosításban).

A 6.1.3 alfejezet áttekinti az összetett garanciacsomag CC fogalmát, majd ismerteti a hierarchikus kapcsolatban álló 3 összetett garanciacsomagot (alap összetett, fokozott összetett és kiemelt összetett).

A 6.1.4 alfejezet meghatározza az egyik fő értékelés előkészítő feladatot: az összetett termékekre vonatkozó biztonsági előirányzat készítését. Ez több szempontból bonyolultabb feladatot jelent, mint egy termék esetén, ugyanakkor (alap összetett garanciacsomag választása esetén) néhány jelentős egyszerűsítést is megenged.

A 6.1.5 alfejezet meghatározza a másik fő értékelés előkészítő feladatot: az összetett termékekre vonatkozó értékelési bizonyítékokat. Ehhez áttekinti, majd részletesen tárgyalja a kompozíció-összeállítás garanciaosztály 5 garanciacsaládját, meghatározva az ezek által elvárt tartalmi és formai követelményeket.

A 6.1.6 alfejezet azokat a termékértékelésnél már meghatározott kiegészítő garancia-összetevőket határozza meg, melyeket a komponens-összeállítás garanciaosztályon kívül figyelembe kell venni. Ezek a kiegészítő garancia-összetevők mindhárom összetett garanciacsomagban megegyeznek.

A 6.2 alfejezet az összetett termékek értékelőinek ad útmutatást.

Az összetett termékek értékelőinek természetesen valamennyi fejlesztőnek/integrátornak szükséges ismeret birtokában kell lenniük. Az értékelési módszertan leírása ezt a tudást már feltételezi.

A következő alfejezetek a biztonsági előirányzat (6.2.1) és az összetett termék (6.2.2-6.2.4) értékelésére vonatkozó (a választott garanciacsomagtól függően egyre bővülő és szigorodó) követelményeit és módszertani elemeit határozza meg.

A 6.2.5 alfejezet a kiegészítő garancia-összetevők mindhárom garanciacsomagra egységes értékelési módszerét határozza meg.

A 6.2.6 alfejezet néhány olyan kiegészítő szempontot fogalmaz meg, melyeket az összetett termékek garancia folyamatosságának biztosítása esetén kell az értékelőnek kielégítenie.

A 7.1 – 7.3 mellékletek a tesztelés során felhasználható általános útmutatásokat tartalmazzák.

3. Alkalmazási terület

A jelen dokumentumban megfogalmazott irányelvek és követelmények elsődlegesen a közigazgatási fejlesztési operatív programok megvalósítására vonatkoznak, az ezekben felhasznált összetett informatikai termékek biztonságos fejlesztését és vizsgálatát (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 összetett 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) – Part 1: Introduction and general model – Part 2: Security functional components - Part 3: 3: Security assurance components

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

[3]: Termékekre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott tervezet, v1, 2008.05.25)

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

[5]: Magyar Informatikai Biztonsági Ajánlások - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma 3. számú segédlete: Útmutató a fejlesztők számára (v1.0, 2008 június)

[6]: Magyar Informatikai Biztonsági Ajánlások - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma 4. számú segédlete: Útmutató az értékelők számára (v1.0, 2008 június)

[7]: Magyar Informatikai Biztonsági Ajánlások - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma 5. számú segédlete: Értékelési módszertan (v1.0, 2008 június)

[8]: Rendszerekre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott tervezet, v2, 2008.08.01)

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

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) – Part 1: Introduction and general model – Part 2: Security functional components - Part 3: 3: Security assurance components	CCPart1v3.1R1 CCPart2v3.1R1 CCPart3v3.1R1	
Common Methodology for Information Technology Security Evaluation (September 2006 - version 3.1)	CEMv3.1R2	
Termékekre vonatkozó értékelési módszertan		e-Közigazgatási Keretrendszer
Az értékeléssel megszerzett garancia folyamatosságának biztosítása		e-Közigazgatási Keretrendszer
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

5. Fogalom-meghatározások

Jelen dokumentum a [3] által meghatározott termék értékelési módszertan továbbfejlesztése, informatika biztonsági szempontból már értékelt termékekből integrált összetett termékek

biztonsági értékelését és ennek fejlesztői megalapozását határozza meg. Olvasóira nézve feltételezés a [3]-ban megfogalmazott módszertan és az ott használt fogalmak ismerete.

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

Kiszolgáló komponens: Egy összetett TOE olyan entitása, amelyet már értékeltek, s amely szolgáltatásokat és erőforrásokat biztosít egy kliens komponensnek.

Összetett TOE: Két vagy több különálló, már sikeresen értékelt komponensből álló TOE.

Komponens TOE: Egy másik TOE részét képező értékelt TOE.

Kliens komponens: Egy összetett TOE olyan entitása, amely maga is értékelés tárgyát képezi, s amely egy kiszolgáló komponens által biztosított szolgáltatásokra hagyatkozik.

Komponens-összeállítás: Összetett TOE létrehozása különálló, már sikeresen értékelt komponensekből. A komponens-összeállítás szempontjait olyan helyzetekben kívánják alkalmazni, amikor az egyik komponens (kliens komponens) egy másiktól (kiszolgáló komponens) függ a biztonsági szolgáltatások megvalósítása céljából.

Összetett garanciacsomag (CAP): Egy garanciacsomag, mely a CC 3. részéből (döntően az ACO osztályból) származó követelményekből áll, s mely egy pontot képvisel a CC előre meghatározott komponens-összeállítás garancia skáláján.

Funkcionális interfész: Az a (külső) interfész, amely a felhasználó számára hozzáférést biztosít a TOE azon funkcionalitásához, mely közvetlenül nincs érintve a funkcionális biztonsági követelmények érvényre juttatásában. Egy összetett TOE esetében ezek a kiszolgáló komponens azon interfészei, melyet a kliens komponens igényel az összetett TOE működésének támogatásához.

6. Összetett termékekre vonatkozó informatikai biztonsági értékelési módszertan

6.1. Összetett termékek fejlesztése és integrálása

6.1.1. Összetett termékek értékelésének jellemzése

6.1.1.1. Igény összetett termékek értékelésére

Az IT piac általánosságban nézve adott típusú terméket, technológiát kínáló gyártókból áll. Bár vannak kivételek (például amikor egy chip gyártó kizárólagosan fejleszt saját chip-jéhez dedikált operációs rendszert), mégis az a helyzet a tipikus, hogy egy IT megoldást különböző gyártók is megvalósítanak.

Az egyedi IT termékek (melyeket jelen dokumentum komponenseknek nevez) független értékeléséből származó garanciáin kívül a komponensek összeállításából kapott alrendszer (melyeket jelen dokumentum összetett terméknek nevez) garanciáinak bizonyítására is szükség van. A gyártók között van ugyan együttműködés a komponensek integrálásához szükséges bizonyos anyagok megosztásában, a megállapodások azonban ritkán terjednek ki részletes tervezési információkra és a fejlesztési folyamatra, eljárásokra vonatkozó bizonyítékokra. Egy olyan komponens fejlesztője, mely egy másik komponens szolgáltatásaira hagyatkozik működése során, erről az alapot képező komponensről általában nem fér hozzá olyan típusú információkhoz, amelyek szükségesek a két komponens összeállításával létrehozott összetett termék független biztonsági értékeléséhez. Miközben tehát egy komponens értékelését az adott komponens fejlesztője egyedül is képes támogatni, addig az összetett termékek esetén szükség van a különböző komponens fejlesztők együttműködésére, vagy az alapot képező komponensre korábban végrehajtott értékelés eredményeinek és értékelési bizonyítékainak az újrafelhasználására.

6.1.1.2. Az összetett termék integrálás (komponens-összeállítás) modellje

Az összetett termék integrálás (komponens-összeállítás, ACO) szempontjait olyan helyzetekben kívánják alkalmazni, amikor egy IT egyed egy másiktól függ a biztonsági szolgáltatások megvalósítása céljából. A szolgáltatásokat nyújtó egyed a „kiszolgáló komponens”, az azokat igénybe vevő pedig a „kliens komponens”. Ez a kapcsolat számos környezetben fennállhat. Például, egy alkalmazás (kliens komponens) használhatja az operációs rendszer (kiszolgáló komponens) által nyújtott szolgáltatásokat. A kapcsolat lehet egyenrangú is két összekapcsolt alkalmazás tekintetében, amelyek vagy közös operációs rendszer környezetben vagy különálló hardver platformon futnak. Ha van domináns tag, ami szolgáltatást nyújt az alárendelt tagnak, akkor a domináns tekintendő a kiszolgáló komponensnek, az alárendelt pedig a kliensnek. Amennyiben viszont a tagok kölcsönösen biztosítanak egymásnak szolgáltatásokat, akkor mindkettő a kiajánlott szolgáltatások tekintetében kiszolgáló komponensnek tekintendő, és kliensnek az igénybe vett funkciók terén. Ez az ACO komponensek iterációját igényli, minden komponens tag típusra alkalmazva az összes követelményt.

A komponens-összeállításra vonatkozó követelményeket modulárisra tervezték a bonyolultabb kapcsolatokra való általános alkalmazhatóság érdekében.

6.1.1.3. Az összetett termék értékelés jellemzői

Összetett termék (a későbbiekben összetett TOE) értékelése esetén is követelmény, hogy az egyedi komponenseket függetlenül értékeljék, mivel az összeállítás értékelése az egyedi komponens értékelések eredményeire alapoz. A kliens komponens értékelése még folyamatban lehet, amikor az összetett TOE értékelés elkezdődik. A kliens komponens értékelésének azonban be kell fejeződnie az összetett TOE értékelés befejezése előtt.

Az összetett TOE értékelési tevékenységek akár egyidejűleg is történhetnek a kliens komponens értékelésével. Ennek két oka is lehet:

— *Megtakarítás/üzleti megfontolások:* a kliens komponens fejlesztője szponzorálja az összeállítás értékelését is, vagy támogatja ezen tevékenységeket, mivel a kliens komponens értékelésével kapcsolatos értékelési bizonyítékokra szükség van az összetétel értékeléséhez.

— *Technikai szempontok:* a komponensek figyelembe veszik, hogy a kiszolgáló komponens biztosítja-e a szükséges garanciát (például a komponens értékelés befejezése óta a kiszolgáló komponensben történt módosításokat) azzal a megfontolással, hogy a kliens komponens a közelmúltban ment át komponens értékelésen (vagy ez folyamatban van), és az értékeléssel kapcsolatos minden értékelési bizonyíték rendelkezésre áll. Ezért az összetétel kialakítás során nincs olyan tevékenység, ami a kliens komponens értékelési tevékenységek újraellenőrzését igényelné. Továbbá az is ellenőrzött, hogy a kiszolgáló komponens a teszt konfigurációt (vagy azok egyikét) jelenti a kliens komponens teszteléséhez a kliens komponens értékelése során.

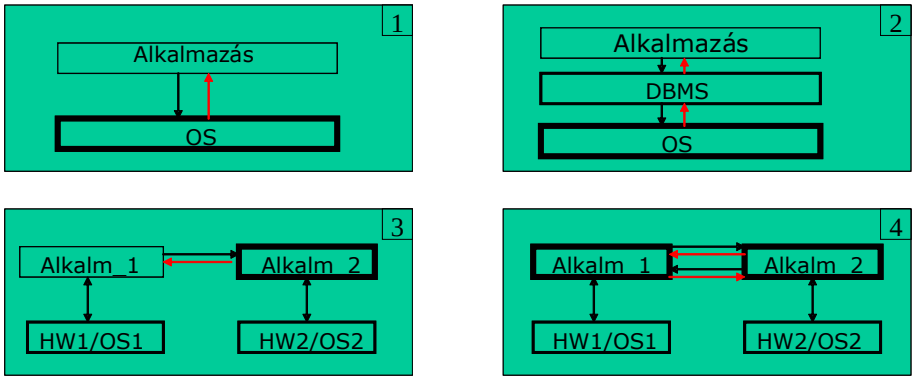
Az összetett TOE értékeléséhez a kliens komponens értékeléséből származó valamennyi értékelési bizonyítékra szükség van.

Az összetett TOE értékeléséhez a kiszolgáló komponens értékeléséből egyetlen anyag szükséges: a kiszolgáló komponenst érintő azon maradvány sebezhetőségek, melyeket a kiszolgáló komponens értékelése során feljegyeztek. /Erre az anyagra az ACO_VUL értékelési tevékenységnél lesz szükség./

Az összetett TOE értékeléséhez a kiszolgáló komponens értékeléséből nincs más értékelési bizonyíték követelmény, mivel a kiszolgáló komponens értékelési eredményeit újra fel lehet használni (azaz el lehet fogadni). A kiszolgáló komponenssel kapcsolatos további információkra csak akkor lehet szükség, ha az összetett TOE biztonsági funkcionalitása (TSF) a kiszolgáló komponensből többet tartalmaz, mint amit TSF-nek tekintettek a kiszolgáló komponens értékelése során.

A kiszolgáló és kliens komponensek értékeléseit egyaránt be kell fejezni, mire az ezekből integrált összetett TOE értékelésénél meghozzák a végső döntést.

6.1.1.4. A komponens összeállítás tipikus megvalósítási formái



2. ábra - Tipikus komponens összeállítások

A 2. ábra négy tipikus komponens összeállítási példát szemléltet. Az ábrán a fekete nyilak jelzik a szolgáltatás kérését, a piros nyilak pedig a szolgáltatás nyújtását. A normál keretezések jelzik a kliens komponenseket, míg a vastag keretezések a kiszolgáló komponenseket.

A 2. ábra 1-es jelzésű példája egy olyan alkalmazás (kliens komponens), ami használja az alapul szolgáló operációs rendszer (kiszolgáló komponens) biztonsági szolgáltatását, például a naplózással és a hozzáférés-ellenőrzéssel kapcsolatosan.

A 2. ábra 2. példája egy 3 elemű komponens összeállítást szemléltet. Egy alkalmazás, mely használja az adatbázis-kezelő rendszert (DBMS), mely adatbázis-kezelő rendszer használja az alapul szolgáló operációs rendszert. Ebben a példában a DBMS egyszerre kliens komponens (az operációs rendszerhez képest) és kiszolgáló komponens (az alkalmazáshoz képest). Ennek a 3 elemű komponens összeállításnak az értékelését két lépésben lehet végrehajtani, első lépésben a DBMS - OS, második lépésben az Alkalmazás – (DBMS-OS) összeállítás értékelhető.

A 2. ábra 3. példája két különböző platformon működő alkalmazás közötti komponens összeállítást szemléltet.

Végül a 2. ábra 4. példájában két különböző platformon működő alkalmazás között kölcsönös függőség áll fenn, mindkettő szolgáltat a másik számára biztonsági szolgáltatást. Ez esetben az értékeléshez mindkét alkalmazás korábbi értékeléséből származó értékelési bizonyítékra szükség van, s az értékelés tetszőleges sorrendben végezhető (például először az 1. Alkalmazás a kliens komponens, majd pedig a 2. Alkalmazás).

6.1.2. Fejlesztői (integrátori) feladatok összetett termékek biztonsági értékelésénél

Ez az alfejezet előzetesen összefoglalja azokat a feladatokat, melyet egy összetett termék biztonsági értékelése esetén az összetett termék integrátorának, illetve részben a megbízónak kell elvégeznie. A feladatok részletezése a további alfejezetekben található.

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

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

Ezt a feladatot a 6.1.2.1 pont részletezi.

A második feladat az összetett termék biztonsági előirányzatának elkészítése. A biztonsági előirányzat az összetett termék informatikai biztonsági követelményeit tartalmazza, illetve előírja azokat a funkcionális és garanciális biztonsági intézkedéseket, amelyeket az összetett 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 az összetett termék biztonsági értékeléséhez szükséges fejlesztői bizonyítékok elkészítése. Ez a feladat a választott garanciaszinttől (CAP-A, CAP-F, CAP-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.

6.1.2.1. Összetett garanciacsomag választás (CAP-A / CAP-F / CAP-K)

A CAP-A (alap összetett garanciacsomag) akkor alkalmazható, ha:
- Mind a kliens, mind a kiszolgáló komponenst legalább MIBÉTS alap értékelési garanciaszinten (vagy legalább CC EAL2-n) már értékelték.
- Biztosított a kliens komponens fejlesztőjének együttműködése a kliens komponens értékeléséből származó tervezési információk és tesztelési eredmények átadására (a kiszolgáló komponens fejlesztőjének bevonása nem szükséges).
- A felhasználók alacsonytól közepes szintig terjedő független biztonsági garanciát igényelnek, a teljes fejlesztési dokumentációhoz való hozzáférés hiányában.

A CAP-F (fokozott összetett garanciacsomag) olyan körülmények között alkalmazható, ha:
- Mind a kliens, mind a kiszolgáló komponenst legalább MIBÉTS fokozott értékelési garanciaszinten (vagy legalább CC EAL3-n) már értékelték.
- Biztosított a kliens komponens fejlesztőjének együttműködése a kliens komponens értékeléséből származó tervezési információk és tesztelési eredmények átadására, valamint biztosított a kiszolgáló komponens fejlesztőjének minimális bevonása is (lásd ACO_DEV.2.2C).
- A felhasználók közepes független biztonsági garanciát igényelnek, valamint az összetett TOE-k és fejlesztésének mélyreható vizsgálatát igénylik, de lényeges technológiai visszaállítási munkák nélkül.

A CAP-K (kiemelt összetett garanciacsomag) olyan körülmények között alkalmazható, ha:
- Mind a kliens, mind a kiszolgáló komponenst legalább MIBÉTS kiemelt értékelési garanciaszinten (vagy legalább CC EAL4-n) már értékelték.
- Biztosított a kliens komponens fejlesztőjének együttműködése a kliens komponens értékeléséből származó tervezési információk és tesztelési eredmények átadására, valamint biztosított a kiszolgáló komponens fejlesztőjének kis mértékű bevonása is (lásd ACO_DEV.3.2C - ACO_DEV.3.4C).
- A felhasználók közepestől magas szintig terjedő független biztonsági garanciát igényelnek és készek további biztonság-specifikus technológiai költségeket vállalni.

6.1.2.2. Biztonsági előirányzat készítése az összetett termékre

Az összetett TOE esetén elkészítendő biztonsági előirányzatokra vonatkozó elvárásokat a 6.1.4 alfejezet tekinti át.

Alap összetett garanciacsomag (CAP-A) választása esetén a biztonsági előirányzat felépítésére, valamint a tartalmára és bemutatására vonatkozó elvárásokat a 6.1.4.1 pont részletezi.

Fokozott összetett garanciacsomag (CAP-F) választása esetén a biztonsági előirányzat felépítésére, valamint a tartalmára és bemutatására vonatkozó elvárásokat a 6.1.4.2 pont részletezi.

Kiemelt összetett garanciacsomag (CAP-K) választása esetén a biztonsági előirányzat felépítésére, valamint a tartalmára és bemutatására vonatkozó elvárásokat a 6.1.4.2 pont részletezi.

6.1.2.3. Fejlesztői bizonyítékok CAP-A választása esetén

6.1.2.3.1. Alap környezetfüggőségi információ (ACO_REL.1)

A fejlesztői feladatok és a bizonyíték elemek tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.2.1 pontban található.

6.1.2.3.2. Funkcionális leírás (ACO_DEV.1)

A fejlesztői feladatok és a bizonyíték elemek tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.3.1 pontban található.

6.1.2.3.3. Komponens-összeállítás indoklás (ACO_COR.1)

A fejlesztői feladatok és a bizonyíték elemek tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.4.1 pontban található.

6.1.2.3.4. Interfész tesztelés (ACO_CTT.1)

A fejlesztői feladatok és a bizonyíték elemek tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.5.1 pontban található.

6.1.2.3.5. Komponens-összeállítás sebezhetőségi áttekintés (ACO_VUL.1)

A fejlesztői feladatok és a bizonyíték elemek tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.6.1 pontban található.

6.1.2.4. Fejlesztői bizonyítékok CAP-F választása esetén

6.1.2.4.1. Alap környezetfüggőségi információ (ACO_REL.1)

A fejlesztői feladatok és a bizonyíték elemek tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.2.1 pontban található.

6.1.2.4.2. Alap tervezési bizonyíték (ACO_DEV.2)

A fejlesztői feladatok és a bizonyíték elemek tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.3.2 pontban található.

6.1.2.4.3. Komponens-összeállítás indoklás (ACO_COR.1)

A fejlesztői feladatok és a bizonyíték elemek tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.4.1 pontban található.

6.1.2.4.4. Szigorú interfész tesztelés (ACO_CTT.2)

A fejlesztői feladatok és a bizonyíték elemek tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.5.2 pontban található.

6.1.2.4.5. Komponens-összeállítás sebezhetőségi elemzés (ACO_VUL.2)

A fejlesztői feladatok és a bizonyíték elemek tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.6.2 pontban található.

6.1.2.5. Fejlesztői bizonyítékok CAP-K választása esetén

6.1.2.5.1. Környezetfüggőségi információ (ACO_REL.2)

A fejlesztői feladatok és a bizonyíték elemek tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.2.2 pontban található.

6.1.2.5.2. Részletes tervezési bizonyíték (ACO_DEV.3)

A fejlesztői feladatok és a bizonyíték elemek tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.3.3 pontban található.

6.1.2.5.3. Komponens-összeállítás indoklás (ACO_COR.1)

A fejlesztői feladatok és a bizonyíték elemek tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.4.1 pontban található.

6.1.2.5.4. Szigorú interfész tesztelés (ACO_CTT.2)

A fejlesztői feladatok és a bizonyíték elemek tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.5.2 pontban található.

6.1.2.5.5. Megemelt alap szintű komponens-összeállítás sebezhetőségi elemzés (ACO_VUL.3)

A fejlesztői feladatok és a bizonyíték elemek tartalmára és bemutatására vonatkozó elvárások részletezése a 6.1.5.6.3 pontban található.

6.1.3. Összetett garanciacsomagok

Az összetett garanciacsomagok (CAP) egy olyan emelkedő szintű skálát jelentenek, amelynek elemeit az összetett TOE-kre vonatkozó garanciaszint és az ennek eléréséhez szükséges költségek egyensúlyát figyelembe véve hozták létre.

Az összetett garanciacsomagok (CAP) szerkezete hasonló a CC értékelési garanciaszintekéhez (EAL). A két csomag típus közötti fő különbség az, hogy az EAL-ok a komponens TOE-kre, míg a CAP-ok az összetett TOE-kre használhatók.

A CAP-okban csak kevés garanciacsalád és garancia-összetevő szerepel a CC 3. részéből. Ez annak köszönhető, hogy jellegüknél fogva a korábban már értékelt egyedek (kiszolgáló komponensek és kliens komponensek) értékelési eredményeire építenek, így e szűkített csomagok is kellő szintű garanciát biztosítanak.

6.1.3.1. Az összetett garanciacsomagok áttekintése

A CAP-okat olyan összetett TOE-kre lehet alkalmazni, amelyek komponens TOE értékelésen átesett (vagy az alatt álló) komponensekből állnak. Az egyes komponenseket egy értékelési garanciaszint szerint tanúsítják (MIBÉTS alap, fokozott vagy kiemelt garanciaszintek, melyek megfelelnek a CC EAL2, EAL3, illetve EAL4 garanciaszintjeinek).

Bár egy kliens komponens a környezetére vonatkozó IT követelmények tekintetében értékelhető egy korábban értékelt kiszolgáló komponenst felhasználva, ez nem ad formális garanciát a komponensek közötti kapcsolatokra vagy az összeállításból eredő esetleges új sebezhetőségekre nézve. Az összetett garanciacsomagok figyelembe veszik ezeket a kapcsolatokat is, és a garancia magasabb szintjein biztosítják, hogy a komponensek közötti interfész is tesztelés tárgya lesz. Az összetett TOE sebezhetőség elemzésére is sor kerül az alkotóelemek összeállításából származó esetleges új sebezhetőségek felismerése céljából.

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

2. táblázat - Az összetett garanciacsomagok összegzése

Garanciaosztály	**Garanciacsalád**	**Garancia-összetevők az egyes összetett garanciacsomagokban**		
		CAP-A	CAP-F	CAP-K
Komponens-összeállítás(ACO)	ACO_COR	1	1	1
	ACO_CTT	1	2	2
	ACO_DEV	1	2	3
	ACO_REL	1	1	2
	ACO_VUL	1	2	3
Útmutató dokumentumok (AGD)	AGD_OPE	1	1	1
	AGD_PRE	1	1	1
Életciklus támogatás(ALC)	ALC_CMC	1	1	1
	ALC_CMS	2	2	2
Biztonsági előirányzat értékelés (ASE)	ASE_CCL	1	1	1
	ASE_ECD	1	1	1
	ASE_INT	1	1	1
	ASE_OBJ	1	2	2
	ASE_REQ	1	2	2
	ASE_SPD	-	1	1
	ASE_TSS	1	2	2

A CC (és ezzel összhangban jelen dokumentum is) három hierarchikusan rendezett összetett garanciacsomagot határoz meg egy összetett TOE garancia szintjeire. A csomagok aszerint rendezettek, hogy minden egyes CAP a nála alacsonyabb szinten állónál magasabb garanciát képvisel. A növekvő garancia azáltal valósul meg, hogy ugyanazon garanciacsaládból hierarchikusan magasabb garancia-összetevő áll a magasabb garanciaszintű csomagban (azaz növekvő a szigor, hatókör és/vagy mélység), és más garanciacsaládokból is megjelennek további garanciális összetevők (új követelmények hozzáadása). Ez a bővítés az összetett TOE nagyobb fokú elemzését vonja maga után, hogy azonosítani lehessen a komponens TOE-kre megállapított értékelési eredmények kihatását az összetételre.

Minden CAP minden garanciacsaládból legfeljebb egy összetevőt tartalmaz, és minden összetevő minden garanciafüggése teljesül.

A következő szakaszok az egyes CAP-ok meghatározásait adják meg.

6.1.3.2. Alap összetett garanciacsomag (CAP-A)

A CAP-A (alap összetett garanciacsomag) akkor alkalmazható, ha egy összetett TOE-t integráltak, s az összeállítás eredményének biztonságos működésére vonatkozóan bizonyosságot igényelnek. Ez megköveteli a kliens komponens fejlesztőjének együttműködését a kliens komponens értékeléséből származó tervezési információk és tesztelési eredmények átadására vonatkozóan, de nem igényli a kiszolgáló komponens fejlesztőjének bevonását.

A CAP-A ezért olyan körülmények között alkalmazható, amikor a fejlesztők vagy felhasználók alacsonytól közepes szintig terjedő független biztonsági garanciát igényelnek, a teljes fejlesztési dokumentációhoz való hozzáférés hiányában.

A CAP-A abban az esetben alkalmazható, ha mind a kliens, mind a kiszolgáló komponenst legalább alap értékelési garanciaszinten (vagy legalább CC EAL2-n) értékelték.

A CAP-A egyrészt az összetett TOE-t leíró biztonsági előirányzat elemzésével biztosít garanciát. Másrészt a biztonsági működés megértése érdekében az összetett TOE biztonsági előirányzatában meghatározott SFR-eket elemzik az alkotóelem TOE-k értékelési kimeneteinek (pl. ST, útmutató dokumentációk), és a komponens TOE-k közötti interfészek specifikációja felhasználásával.

Az elemzést a kliens komponensek által használt kiszolgáló komponens interfészeinek független tesztelése segíti, ahogyan azt a környezetfüggőségi információ a környezetfüggőségi információn alapuló fejlesztői tesztelési bizonyíték, a fejlesztési információ, a TOE komponens-összeállítás indoklás és a fejlesztői teszteredmények szelektív független megerősítése leírja. Az elemzést ezen kívül segíti az összetett TOE sebezhetőségi áttekintése is, melyet az értékelő végez el.

A CAP-A az összetett TOE (vagyis a működőképes összetett informatikai termék, kiegészítve az útmutató dokumentumokkal) egyedi azonosításával is garanciát biztosít.

3. táblázat - CAP-A

Garanciaosztály	**Garancia-összetevő**
ACO: Komponens-összeállítás	ACO_COR.1 Komponens-összeállítás indoklás
	ACO_CTT.1 Interfész tesztelés
	ACO_DEV.1 Funkcionális leírás
	ACO_REL.1 Alap környezetfüggőségi információ
	ACO_VUL.1 Kompozíció sebezhetőség áttekintés
AGD: Útmutató dokumentumok	AGD_OPE.1 Üzemeltetési felhasználói útmutató
	AGD_PRE.1 Előkészítő eljárások
ALC: Életciklus támogatás	ALC_CMC.1 A TOE címkézése
	ALC_CMS.2 TOE részek konfiguráció kezelés lefedettsége
ASE: Biztonsági előirányzat értékelés	ASE_CCL.1 Megfelelőségi nyilatkozatok
	ASE_ECD.1 Kiterjesztett összetevő meghatározás
	ASE_INT.1 ST bevezetés
	ASE_OBJ.1 A működési környezetre vonatkozó biztonsági célok
	ASE_REQ.1 Kinyilvánított biztonsági követelmények
	ASE_TSS.1 TOE összefoglaló előírás

6.1.3.3. Fokozott összetett garanciacsomag (CAP-F)

A CAP-F (fokozott összetett garanciacsomag) lehetővé teszi egy fejlesztő számára, hogy az összetett TOE-be integrált TOE komponensek közötti kapcsolatok hatásának alrendszer szintű megértésével maximális garanciát szerezzen, egyben minimalizálja az igényt a kiszolgáló komponens fejlesztőjének bevonására.

A CAP-F olyan körülmények között alkalmazható, amikor a fejlesztők vagy felhasználók közepes független biztonsági garanciát igényelnek, valamint az összetett TOE-k és fejlesztésének mélyreható vizsgálatát igénylik, de lényeges technológiai visszaállítási munkák nélkül.

A CAP-F abban az esetben alkalmazható, ha mind a kliens, mind a kiszolgáló komponenst legalább fokozott értékelési garanciaszinten (vagy legalább CC EAL3-n) értékelték.

A CAP-F egyrészt az összetett TOE-t leíró teljes biztonsági előirányzat elemzésével biztosít garanciát. Másrészt a biztonsági működés megértése érdekében az összetett TOE biztonsági előirányzatában meghatározott SFR-eket elemzik az alkotóelem TOE-k értékelési kimeneteinek (pl. ST, útmutató dokumentációk), a komponens TOE-k közötti interfészek specifikációja, valamint az összetett fejlesztési információ által tartalmazott (TSF alrendszereket leíró) TOE terv felhasználásával.

Az elemzést a kliens komponens által használt kiszolgáló komponens interfészeinek független tesztelése segíti, ahogyan azt a környezetfüggőségi információ (beleértve a TOE tervet), a környezetfüggőségi információn alapuló fejlesztői tesztelési bizonyíték, a fejlesztési információ, a TOE komponens-összeállítás indoklás és a fejlesztői teszteredmények szelektív független megerősítése leírja. Az elemzést ezen kívül segíti az összetett TOE sebezhetőségi elemzése is, melyet az értékelő végez el az alap támadási képességgel rendelkező támadókkal szembeni ellenállóképesség bizonyítása céljából.

A CAP-F a CAP-A-hoz képest jelentős garancianövekedést jelent amiatt, hogy a biztonsági funkcionalitás teljesebb teszt lefedettségét követeli meg.

4. táblázat - CAP-F

Garanciaosztály	**Garancia-összetevő**
ACO: Komponens-összeállítás	ACO_COR.1 Komponens-összeállítás indoklás
	ACO_CTT.2 Szigorú interfész tesztelés
	ACO_DEV.2 Alap tervezési bizonyíték
	ACO_REL.1 Alap környezetfüggőségi információ
	ACO_VUL.2 Kompozíció sebezhetőség elemzés
AGD: Útmutató dokumentumok	AGD_OPE.1 Üzemeltetési felhasználói útmutató
	AGD_PRE.1 Előkészítő eljárások
ALC: Életciklus támogatás	ALC_CMC.1 A TOE címkézése
	ALC_CMS.2 TOE részek konfiguráció kezelés lefedettsége
ASE: Biztonsági előirányzat értékelés	ASE_CCL.1 Megfelelőségi nyilatkozatok
	ASE_ECD.1 Kiterjesztett összetevő meghatározás
	ASE_INT.1 ST bevezetés
	ASE_OBJ.2 Biztonsági célok
	ASE_REQ.2 Származtatott biztonsági követelmények
	ASE_SPD.1 Biztonsági probléma meghatározás
	ASE_TSS.2 TOE összefoglaló előírás architektúra terv összegzéssel

6.1.3.4. Kiemelt összetett garanciacsomag (CAP-K)

A CAP-K (kiemelt összetett garanciacsomag) lehetővé teszi egy fejlesztő számára, hogy az összetett TOE komponensei közötti kapcsolatok tényeken alapuló elemzéséből maximális garanciát szerezzen, ami bár szigorú, de nem követeli meg a kiszolgáló komponens összes fejlesztési bizonyítékához való teljes hozzáférést.

A CAP-K ezért olyan körülmények között alkalmazható, amikor a fejlesztők vagy felhasználók a hagyományos kereskedelmi összetett TOE-kra közepestől magas szintig terjedő független biztonsági garanciát igényelnek és készek további biztonság-specifikus technológiai költségeket vállalni.

A CAP-K abban az esetben alkalmazható, ha mind a kliens, mind a kiszolgáló komponenst kiemelt értékelési garanciaszinten (vagy legalább CC EAL4-n) értékelték.

A CAP-K egyrészt az összetett TOE-t leíró teljes biztonsági előirányzat elemzésével biztosít garanciát. Másrészt a biztonsági elemek működésének megértése érdekében az összetett TOE biztonsági előirányzatában meghatározott SFR-eket elemzik az alkotóelem TOE-k értékelési kimeneteinek (pl. ST, útmutató dokumentációk), a komponens TOE-k közötti interfészek specifikációja, valamint az összetett fejlesztési információ által tartalmazott (TSF modulokat leíró) TOE terv felhasználásával.

Az elemzést a kliens komponens által használt kiszolgáló komponens interfészeinek független tesztelése segíti, ahogyan azt a környezetfüggőségi információ (beleértve a TOE tervet), a környezetfüggőségi információn alapuló fejlesztői tesztelési bizonyíték, a fejlesztési információ, a TOE komponens-összeállítás indoklás és a fejlesztői teszteredmények szelektív független megerősítése leírja. Az elemzést ezen kívül segíti az összetett TOE sebezhetőségi elemzése is, melyet az értékelő végez el a megemelt alap támadási képességgel rendelkező támadókkal szembeni ellenállóképesség bizonyítása céljából.

A CAP-K a CAP-F-hez képest jelentős garancianövekedést jelent amiatt, hogy több tervezési leírást és egy magasabb támadási képesség elleni ellenállóképesség kimutatását követeli meg.

5. táblázat - CAP-K

Garanciaosztály	**Garancia-összetevő**
ACO: Komponens-összeállítás	ACO_COR.1 Komponens-összeállítás indoklás
	ACO_CTT.2 Szigorú interfész tesztelés
	ACO_DEV.3 Részletes tervezési bizonyíték
	ACO_REL.2 Környezetfüggőségi információ
	ACO_VUL.3 Megemelt alap kompozíció sebezhetőség elemzés
AGD: Útmutató dokumentumok	AGD_OPE.1 Üzemeltetési felhasználói útmutató
	AGD_PRE.1 Előkészítő eljárások
ALC: Életciklus támogatás	ALC_CMC.1 A TOE címkézése
	ALC_CMS.2 TOE részek konfiguráció kezelés lefedettsége
ASE: Biztonsági előirányzat értékelés	ASE_CCL.1 Megfelelőségi nyilatkozatok
	ASE_ECD.1 Kiterjesztett összetevő meghatározás
	ASE_INT.1 ST bevezetés
	ASE_OBJ.2 Biztonsági célok
	ASE_REQ.2 Származtatott biztonsági követelmények
	ASE_SPD.1 Biztonsági probléma meghatározás
	ASE_TSS.2 TOE összefoglaló előírás architektúra terv összegzéssel

6.1.4. Összetett termék biztonsági előirányzata

Az összetett termék (kiszolgáló komponens + kliens komponens, a továbbiakban összetett TOE) értékeléséhez a fejlesztőnek ST-t kell benyújtania, ami azonosítja az összetett termékre alkalmazandó garanciacsomagot (CAP-A, CAP-F vagy CAP-K) is.

Az összetett TOE-ra vonatkozó ST legfontosabb célja annak bemutatása, hogy a komponensek mind a környezet, mind a követelmények szempontjából kompatibilisek

egymással, valamint, hogy az összetett TOE ST-je nem mond ellent a komponensek ST-inek és a bennük kifejtett biztonsági szabályzatoknak.

Az összetett TOE biztonsági előirányzatának felépítése egységes, megegyezik a termékre vagy komponensre vonatkozó TOE ST-k felépítésével:

- ST bevezetés
- Megfelelőség nyilatkozatok
- Biztonsági probléma meghatározás
- Biztonsági célokról szóló nyilatkozat
- Kiterjesztett összetevő meghatározás
- Biztonsági követelményekről szóló nyilatkozat
- TOE összefoglaló előírás

Az összetett TOE biztonsági előirányzatra ugyanazok a tartalmi elvárások vannak, mint a termékre vagy komponensre vonatkozó TOE ST-ire, az alábbi két különbség típus mellett:

- Az összetett TOE biztonsági előirányzatra néhány kiegészítő követelmény is vonatkozik (a későbbi leírás ezeket a kiegészítő elvárásokat azonosítja).
- Az összetett TOE biztonsági előirányzatra alap összetett garanciacsomag (CAP-A) választása esetén három lényeges egyszerűsítés könnyíti meg a biztonsági előirányzat készítését (nem kell megadni a biztonsági probléma meghatározást, valamint a biztonsági célok és a biztonsági követelmények indoklását).

Az összetett TOE biztonsági előirányzatra fokozott összetett (CAP-F) és kiemelt összetett garanciacsomag (CAP-K) esetén ugyanazok a követelmények vonatkoznak.
A következő pontok részletesen meghatározzák az egyes összetett garanciacsomagok ST-re vonatkozó elvárásait.

6.1.4.1. A biztonsági előirányzat elvárt szerkezete és tartalma CAP-A esetén

6.1.4.1.1. ST bevezetés (ASE_INT)

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.

Összetett TOE esetén az ST-ben szereplő TOE áttekintésnek az összetett TOE használatát és fő biztonsági tulajdonságait kell leírnia, és nem az összetett TOE egyes elemeire vonatkozó információkat.

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.

Összetett TOE esetén az ST hivatkozhat az összetevő TOE-k logikai határainak leírására, melyek az alkotó TOE-k ST-iben szerepelnek, és az összetett TOE leírásának nagy részét képezik. Az összetett TOE ST-nek azonban egyértelműen le kell írnia, hogy az egyedi komponensek melyik szolgáltatása nem tartozik az összetett TOE-ba, következésképp nem jelenik meg az összetett TOE-ban sem tulajdonságként.

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.

6.1.4.1.2. Megfelelőség nyilatkozatok (ASE_CCL)

Függések: ASE_INT.1, ASE_ECD.1, ASE_REQ.2

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 írni az ST megfelelőségét a CC 2.részéhez képest, hogy az megfelel-e a CC 2. részének vagy kiterjeszti azt.

Összetett TOE esetén, ha egy vagy több komponens TOE CC 2. rész kiterjesztést állít, akkor az összetett TOE-nak szintén CC 2. rész kiterjesztettnek kell lennie.

Összetett TOE esetén a CC megfelelőségi nyilatkozat lehet CC 2. rész kiterjesztett, akkor is, ha a komponens TOE-k megfelelnek a CC 2. résznek. (Ez abban az esetben lehetséges, ha a kiszolgáló TOE-ra további, kiterjesztett SFR-eket állítanak.)

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.1.4C 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.

Összetett TOE esetén csak egy összetett megoldást megkövetelő PP-nek való megfelelést lehet állítani egy ST-ben. Ez csak olyan esetekben lehetséges, amikor az "összetett" PP megengedi az összetételek értékelése megközelítést (ACO összetevők használatát).

Összetett TOE esetén az ST egyértelműen azonosítsa azon komponens TOE-k ST-it, melyekből az összetett ST áll. Az összetett TOE lényegileg a komponens TOE-k ST-inek való megfelelést állít.

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.

Összetett TOE esetén a megfelelőségi nyilatkozat indoklása mutassa meg, hogy a komponens TOE-k TOE típusai összhangban vannak az összetett TOE típusával. Ez nem jelenti azt, hogy az összetett és a komponens TOE típusoknak meg kell egyezniük, de a komponens TOE-knak alkalmasnak kell lenniük az összetett TOE-hez való integrálásra. Az összetett TOE ST-jében egyértelművé kell tenni, hogy melyik SFR-k az összeállítás eredményei, és hogy ezeket nem vizsgálták SFR-ként a kiszolgáló és kliens komponens TOE-k értékelése során.

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.

Összetett TOE esetén az összetett TOE biztonsági probléma meghatározása álljon összhangban a komponens TOE-k ST-iben specifikáltakkal. Az összhangot a kimutatható megfelelés szerint kell értelmezni. Teljesülniük kell az alábbiaknak:

a) Az összetett TOE ST-ben szereplő fenyegetések és szervezeti biztonsági szabályzatok nem mondanak ellent a komponens ST-kben szereplőknek.;

b) A komponens ST-kben leírt feltételezések fennállnak az összetett TOE ST-ben. Azaz, vagy a feltételezésnek kell szerepelnie az összetett TOE-ban, vagy a feltételezést pozitív módon kezelni kell az összetett ST-ben. A feltételezés pozitívan kezelhető az összetett TOE-ban követelmények meghatározásával a feltételezésben megcélzott szempont teljesítését biztosító funkcionalitás biztosításával.

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.

Összetett TOE esetén az összetett TOE biztonsági céljai legyenek összhangban a komponens TOE-k ST-iben specifikáltakkal. Az összhangot a kimutatható megfelelés szerint kell értelmezni. Teljesülniük kell az alábbiaknak:

a) A kliens TOE ST-jében szereplő egyetlen működési környezetben releváns IT vonatkozású biztonsági cél sem mond ellent a kiszolgáló TOE ST-jében szereplő biztonsági céloknak. Az nem elvárás, hogy a kliens TOE ST-jén belül a környezeti biztonsági célok nyilatkozata lefedje a kiszolgáló TOE ST-jében található TOE biztonsági célok minden szempontját.

b) Az összetett ST-ben lévő biztonsági célok nyilatkozata nem mond ellent a komponens TOE-k ST-iben szereplő biztonsági célok nyilatkozatának.

Összetett TOE esetén, amennyiben kimutatható megfelelést követel meg a PP, a megfelelőségi nyilatkozat indoklásának meg kell mutatnia, hogy az ST-ben szereplő biztonsági célokra vonatkozó nyilatkozat tartalmazza a komponens TOE ST-iben szereplő biztonsági célokat.

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.

6.1.4.1.3. Biztonsági probléma meghatározás (ASE_SPD)

CAP-A esetén nincs ilyen garancia-összetevő.

6.1.4.1.4. Biztonsági célok (ASE_OBJ)

Függések: Nincsenek függések.

Fejlesztői akcióelemek:

ASE_OBJ.1.1D A fejlesztőnek biztosítania kell egy biztonsági célokról szóló nyilatkozatot.

A bizonyíték elemek tartalma és bemutatása:

ASE_OBJ.1.1C A biztonsági célokról szóló nyilatkozatnak le kell írnia a működési környezetre vonatkozó biztonsági célokat.

Értékelői akcióelemek:

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

6.1.4.1.5. Kiterjesztett összetevő meghatározás (ASE_ECD)

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.

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.

6.1.4.1.6. Biztonsági követelmények (ASE_REQ)

Függések: ASE_ECD.1

Fejlesztői akcióelemek:

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

ASE_REQ.1.2D A fejlesztőnek biztosítania kell egy biztonsági követelmények indoklást.

A bizonyíték elemek tartalma és bemutatása:

ASE_REQ.1.1C A biztonsági követelményekről szóló nyilatkozatnak le kell írnia az SFR-ket és az SAR-kat.

ASE_REQ.1.2C Az SFR-ekben és SAR-ekben használt minden szubjektumot, objektumot, műveletet, biztonsági tulajdonságot, külső egyedet és egyéb terminológiai egységet definiálni kell.

ASE_REQ.1.3C A biztonsági követelményekről szóló nyilatkozatnak azonosítania kell a biztonsági követelményekben szereplő összes műveletet.

ASE_REQ.1.4C Minden műveletet pontosan és helyesen kell végrehajtani.

ASE_REQ.1.5C A biztonsági követelmények minden függési viszonyát vagy teljesíteni kell, vagy a biztonsági követelmények indoklásának igazolnia kell a függés nem teljesítését.

ASE_REQ.1.6C A biztonsági követelményekről szóló nyilatkozatnak belső ellentmondásoktól mentesnek kell lennie.

Értékelői akcióelemek:

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

6.1.4.1.7. TOE összefoglaló előírás (ASE_TSS)

Függések: ASE_INT.1, ASE_REQ.1

Fejlesztői akcióelemek:

ASE_TSS.1.1D A fejlesztőnek biztosítania kell egy TOE összefoglaló előírást.

A bizonyíték elemek tartalma és bemutatása:

ASE_TSS.1.1C A TOE összefoglaló előírásnak le kell írnia, hogy a TOE hogyan teljesíti az egyes SFR-eket.

Összetett TOE esetén azt is egyértelműen meg kell határozni, hogy melyik komponens gondoskodik az egyes SFR-ekről, vagy az egyes SFR-ek teljesítéséhez a komponensek milyen együttesére van szükség.

Értékelői akcióelemek:

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

ASE_TSS.1.2E Az értékelőnek meg kell erősítenie, hogy a TOE összefoglaló előírás összhangban van a TOE áttekintéssel és a TOE leírással, nem mond ellent azoknak.

6.1.4.2. A biztonsági előirányzat elvárt szerkezete és tartalma CAP-F esetén

6.1.4.2.1. 6.1.4.2.1 ST bevezetés (ASE_INT)

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.

Összetett TOE esetén az ST-ben szereplő TOE áttekintésnek az összetett TOE használatát és fő biztonsági tulajdonságait kell leírnia, és nem az összetett TOE egyes elemeire vonatkozó információkat.

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.

Összetett TOE esetén az ST hivatkozhat az összetevő TOE-k logikai határainak leírására, melyek az alkotó TOE-k ST-iben szerepelnek, és az összetett TOE leírásának nagy részét képezik. Az összetett TOE ST-nek azonban egyértelműen le kell írnia, hogy az egyedi komponensek melyik szolgáltatása nem tartozik az összetett TOE-ba, következésképp nem jelenik meg az összetett TOE-ban sem tulajdonságként.

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.

6.1.4.2.2. Megfelelőség nyilatkozatok (ASE_CCL)

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 írni az ST megfelelőségét a CC 2.részéhez képest, hogy az megfelel-e a CC 2. részének vagy kiterjeszti azt.

Összetett TOE esetén, ha egy vagy több komponens TOE CC 2. rész kiterjesztést állít, akkor az összetett TOE-nak szintén CC 2. rész kiterjesztettnek kell lennie.

Összetett TOE-ra vonatkozó CC megfelelőségi nyilatkozat lehet CC 2. rész kiterjesztett, akkor is, ha a komponens TOE-k megfelelnek a CC 2. résznek. (Ez abban az esetben lehetséges, ha a kiszolgáló TOE-ra további, kiterjesztett SFR-eket állítanak.)

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.1.4C 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.

Összetett TOE-ra csak egy összetett megoldást megkövetelő PP-nek való megfelelést lehet állítani egy ST-ben. Ez csak olyan esetekben lehetséges, amikor az "összetett" PP megengedi az összetételek értékelése megközelítést (ACO összetevők használatát).

Összetett TOE-ra vonatkozó ST egyértelműen azonosítsa azon komponens TOE-k ST-it, melyekből az összetett ST áll. Az összetett TOE lényegileg a komponens TOE-k ST-inek való megfelelést állít.

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.

Összetett TOE esetén a megfelelőségi nyilatkozat indoklása mutassa meg, hogy a komponens TOE-k TOE típusai összhangban vannak az összetett TOE típusával. Ez nem jelenti azt, hogy az összetett és a komponens TOE típusoknak meg kell egyezniük, de a komponens TOE-knak alkalmasnak kell lenniük az összetett TOE-hez való integrálásra. Az összetett TOE ST-jében egyértelművé kell tenni, hogy melyik SFR-k az összeállítás eredményei, és hogy ezeket nem vizsgálták SFR-ként a kiszolgáló és kliens komponens TOE-k értékelése során.

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.

Összetett TOE esetén az összetett TOE biztonsági probléma meghatározása álljon összhangban a komponens TOE-k ST-iben specifikáltakkal. Az összhangot a kimutatható megfelelés szerint kell értelmezni. Teljesülniük kell az alábbiaknak:

a) Az összetett TOE ST-ben szereplő fenyegetések és szervezeti biztonsági szabályzatok nem mondanak ellent a komponens ST-kben szereplőknek.;
b) A komponens ST-kben leírt feltételezések fennállnak az összetett TOE ST-ben. Azaz, vagy a feltételezésnek kell szerepelnie az összetett TOE-ban, vagy a feltételezést pozitív módon kezelni kell az összetett ST-ben. A feltételezés pozitívan kezelhető az összetett TOE-ban követelmények meghatározásával a feltételezésben megcélzott szempont teljesítését biztosító funkcionalitás biztosításával.

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.

Összetett TOE esetén az összetett TOE biztonsági céljai legyenek összhangban a komponens TOE-k ST-iben specifikáltakkal. Az összhangot a kimutatható megfelelés szerint kell értelmezni. Teljesülniük kell az alábbiaknak:

a) A kliens TOE ST-jében szereplő egyetlen működési környezetben releváns IT vonatkozású biztonsági cél sem mond ellent a kiszolgáló TOE ST-jében szereplő biztonsági céloknak. Az nem elvárás, hogy a kliens TOE ST-jén belül a környezeti biztonsági célok nyilatkozata lefedje a kiszolgáló TOE ST-jében található TOE biztonsági célok minden szempontját.
b) Az összetett ST-ben lévő biztonsági célok nyilatkozata nem mond ellent a komponens TOE-k ST-iben szereplő biztonsági célok nyilatkozatának.

Összetett TOE esetén, amennyiben kimutatható megfelelést követel meg a PP, a megfelelőségi nyilatkozat indoklásának meg kell mutatnia, hogy az ST-ben szereplő biztonsági célokra vonatkozó nyilatkozat tartalmazza a komponens TOE ST-iben szereplő biztonsági célokat.

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.

Összetett TOE esetén az összetett TOE biztonsági követelményei legyenek összhangban a komponens TOE-k ST-iben specifikáltakkal. Az összhangot a kimutatható megfelelés szerint kell értelmezni. Teljesülniük kell az alábbiaknak:

a) A kliens TOE ST-jében szereplő egyetlen működési környezetben releváns IT vonatkozású biztonsági követelmény sem mond ellent a kiszolgáló TOE ST-jében szereplő biztonsági követelményeknek. Az nem elvárás, hogy a kliens TOE ST-jén belül a környezeti biztonsági követelményekről szóló nyilatkozata lefedje a kiszolgáló TOE ST-jében található TOE biztonsági célok minden aspektusát, mivel néhány SFR-t valószínűleg hozzá kell adni az összetett TOE ST biztonsági követelményeihez. A kiszolgáló TOE-ben lévő biztonsági követelményekről szóló nyilatkozatának azonban támogatnia kell a kliens komponens működését.

b) A kliens TOE ST-jében szereplő egyetlen működési környezetben releváns IT vonatkozású biztonsági cél sem mond ellent a kiszolgáló TOE ST-jében szereplő biztonsági követelményeknek. Az nem elvárás, hogy a kliens TOE ST-jén belül a környezeti biztonsági célok nyilatkozata lefedje a kiszolgáló TOE ST-jében található TOE biztonsági követelmények minden szempontját.

c) Az összetett TOE-ban a biztonsági követelményekről szóló nyilatkozatának összhangban kell lennie a komponens TOE-kre vonatkozó ST-k biztonsági követelményeivel.

Összetett TOE esetén, amennyiben kimutatható megfelelést követel meg a PP, a megfelelőségi nyilatkozat indoklásnak meg kell mutatnia, hogy az ST-ben szereplő biztonsági követelményekről szóló nyilatkozat tartalmazza a komponens TOE ST-iben szereplő biztonsági követelményeket.

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.

6.1.4.2.3. Biztonsági probléma meghatározás (ASE_SPD)

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 működési 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.**

6.1.4.2.4. Biztonsági célok (ASE_OBJ)

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** a működési 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 működési 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 a működési 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.

6.1.4.2.5. Kiterjesztett összetevő meghatározás (ASE_ECD)

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.

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.

6.1.4.2.6. Biztonsági követelmények (ASE_REQ)

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.

6.1.4.2.7. TOE összefoglaló előírás (ASE_TSS)

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.

Összetett TOE esetén azt is egyértelműen meg kell határozni, hogy melyik komponens gondoskodik az egyes SFR-ekről, vagy az egyes SFR-ek teljesítéséhez a komponensek milyen együttesére van szükség.

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

Összetett TOE-ra az értékelő azt is állapítsa meg, hogy egyértelmű-e, hogy melyik komponens biztosítja a védelmet, vagy a komponensek milyen együttese biztosítja azt.

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

Összetett TOE esetén azt is egyértelműen meg kell határozni, hogy melyik komponens biztosítja a védelmet, vagy a komponensek milyen együttese biztosítja azt.

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.

6.1.4.3. A biztonsági előirányzat elvárt szerkezete és tartalma CAP-K esetén

A kiemelt összetett garanciacsomag (CAP-K) biztonsági előirányzatra vonatkozó elvárásai megegyeznek az fokozott összetett garanciacsomag (CAP-F) megfelelő elvárásaival. Lásd 6.1.4.2 alfejezetet.

6.1.5. Kompozíció-összeállítás garanciaosztály

A komponens-összeállítás (ACO) garanciaosztály öt garanciacsaládja által megfogalmazott garanciális követelmények azt a bizalmat kívánják megteremteni, hogy egy összetett TOE biztonságosan fog működni a korábban már értékelt szoftver, hardver vagy förmver komponensek által nyújtott biztonsági funkcionalitásra támaszkodva.

A komponens-összeállítás két vagy több, a termék értékelési módszertan szerint már sikeresen értékelt IT egyedet (kiszolgáló komponensek és kliens komponensek) kombinál úgy, hogy egyik IT egyedre sem igényel további fejlesztést. A komponens-összeállítás nem fedi le az egyéb IT egyedek fejlesztését (azaz olyan egyedekét, amelyek nem estek át korábban termék értékelésen). Az összetett TOE egy új terméket képvisel, ami a környezetére vonatkozó biztonsági célokat kielégítő specifikus környezeti platformon telepíthető és tovább integrálható.

A fenti megközelítés nem a komponensek értékelésének alternatív módját jelenti. Az ACO értelmében történő komponens-összeállítás egy összetett TOE integrátora számára biztosít egy olyan módszert, amely alkalmas arra, hogy igazolja a megbízhatóságot két vagy több sikeresen értékelt összetevő kombinációjából álló TOE-re, anélkül, hogy újra kellene értékelni az összetett TSF-et. (Az összetett TOE-t integráló személyt az ACO osztály végig “fejlesztőnek” nevezi, és megjelöli, hogy ez hol jelenti a kiszolgáló, és hol a kliens komponensek fejlesztőjét.)

Az összetett garanciacsomagokra azért van szükség, mert egy összetett termék értékelése során az alkotó komponensek értékelési eredményeit ugyan újra fel lehet használni, mégis gyakran felmerülnek olyan egyéb szempontok a komponensekkel kapcsolatban, melyeket figyelembe kell venni az összetett TOE-ban.

Összetett TOE esetén általában az a helyzet, hogy egy komponens támaszkodik egy másik komponens által nyújtott szolgáltatásokra. Az a komponens, amely a szolgáltatást igénybe veszi, a kliens komponens, amelyik pedig biztosítja azt, a kiszolgáló komponens. Ezt az együttműködést és megkülönböztetést a 6.1.5.7 pont jellemzi részletesebben. Feltételezés, hogy a kliens komponens fejlesztője támogatja az összetett TOE értékelését valamilyen módon (mint fejlesztő, megbízó vagy közreműködő), és biztosítja a kliens komponens értékeléséből származó szükséges értékelési bizonyítékot.

6.1.5.1. A kompozíció-összeállítás garanciaosztály áttekintése

A komponens-összeállítás (ACO) garanciaosztály az alábbi öt garanciacsaládot tartalmazza:
- A kliens komponens környezetfüggősége (ACO_REL)
- Fejlesztési bizonyíték (ACO_DEV)
- Komponens-összeállítás indoklás (ACO_COR)
- Az összetett TOE tesztelése (ACO_CTT)
- Összetett sebezhetőség elemzés (ACO_VUL)

Az ACO osztályon belüli családok a termék értékelési módszertanban [3] használt „Fejlesztés” (ADV), „Tesztelés” (ATE) és „Sebezhetőség felmérés” (AVA) osztályokhoz hasonló módon működnek, módosítva bizonyos követelményeket a kompozíció-összeállítás szempontja szerint. Van azonban néhány kifejezetten az összetett TOE értékelésre szabott elem is.

Annak meghatározásához, hogy a komponensek hogyan működnek együtt, és az összetevők értékeléséhez képest milyen eltérések vannak, fel kell tárni, hogy a kliens komponensek mennyiben függnek a kiszolgáló komponensektől (ACO_REL).

Ezt a kiszolgáló komponensre való ráépülést azok az interfészek fejezik ki, amelyeken keresztül a kliens komponens szolgáltatás hívásokat kezdeményez, saját SFR-jeinek támogatása céljából. Az interfészeket, illetve magasabb szinteken a kiszolgáló komponens által biztosított támogató működést (melyek a szolgáltatás kérésekre adott válaszok) az ACO_DEV vizsgálja. Az ACO_DEV család a termék értékelési módszertan ADV_TDS családján alapul, mivel legalacsonyabb szinten az egyes komponensek TSF-jét úgy lehet tekinteni, mint az összetett TOE alrendszerét, az egyes komponensek további részeit pedig, mint további alrendszereket. Így komponensek közötti interfészek egy komponens TOE értékelésben alrendszerek közötti kölcsönhatásként jelennek meg.

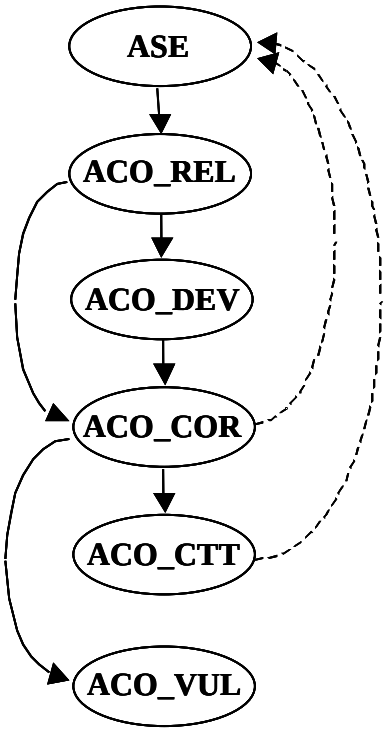
Előfordulhat, hogy az ACO_DEV-hez biztosított, interfészekre és támogató működésre vonatkozó leírások hiányosak. Ez az ACO_COR végrehajtása során derülhet ki, mely garanciacsalád az ACO_REL és ACO_DEV kimenetei alapján dolgozik. ACO_COR annak megállapítását segíti, hogy a komponenseket az értékelt konfigurációban használják-e, egyúttal azonosít minden hiányos specifikációt, melyet majd az ACO_CTT és az ACO_VUL tevékenységek várnak bemenetként (annak meghatározásával, hogy a tesztelés és a sebezhetőség elemzés során mire kell koncentrálni).

Az összetett TOE tesztelésének (ACO_CTT) célja az összetett TOE elvárt működésének megmutatása: megfelel-e annak, ahogyan azokat a TOE SFR-ek megadták, illetve magasabb szinteken annak demonstrálása, hogy az összetett TOE komponensei közötti interfészek kompatibilisek egymással.

Az összetett TOE sebezhetőségi elemzése (ACO_VUL) a komponens értékelések sebezhetőségi elemzések kimeneteit is felhasználja. Figyelembe veszi a komponens értékelésekből származó összes maradvány sebezhetőséget annak megállapításához, hogy a maradvány sebezhetőségek nem vonatkoznak-e az összetett TOE-ra. A komponensekkel kapcsolatos nyilvánosan hozzáférhető információk kutatása a korábbi komponens értékelések befejezése óta jelentett problémák felméréshez is hozzájárul.

Az ACO családok közötti együttműködést szemlélteti a 3. ábra. Ez folytonos vonalú nyilakkal azt mutatja, hogy az egyik család által igazolt bizonyíték és értelmezés hogyan vezet át a következő tevékenységbe, a szaggatott vonalak pedig azt mutatják, ahol egy tevékenység közvetett módon visszavezet az összetett TOE SFR-ekhez, ahogy az fent leírásra került.

Az összetett TOE-kon belüli együttműködést (egymásra hatásokat) a 6.1.5.7 pont tárgyalja részletesebben.



3. ábra - Az ACO családok közötti összefüggések

6.1.5.2. Kliens komponens környezetfüggősége garanciacsalád (ACO_REL)

Ennek a családnak a célja egy kliens és egy kiszolgáló komponens között fennálló függőségi viszony leírása. Ez az információ egy komponens más értékelt IT elemekkel való integrálásáért felelős személyek számára fontos, egyúttal az összeállított rendszer biztonsági tulajdonságaiba is betekintést nyújt.

A család az összetett TOE kliens és kiszolgáló komponensei között azokat az interfészeket írja le, amit az egyedi komponensek értékelése során nem vizsgáltak, mivel azok nem képezték részét az egyes komponens TOE-k TSF interfészeinek.
A család összetevőinek szintjei (ACO_REL.1 és ACO_REL.2) aszerint különböznek, hogy milyen mennyiségű információt biztosítanak a kliens komponens kiszolgálótól való függésének leírására.

„A kliens komponens környezetfüggősége” (ACO_REL) család a komponensek közötti kapcsolatokat, együttműködést vizsgálja, amikor a kliens komponens saját biztonsági funkcionalitásának támogatásához a kiszolgáló komponenstől kapott szolgáltatásra épít. A kiszolgáló komponens ezen szolgáltatásaihoz való interfészeket vélhetően nem vizsgálták a kiszolgáló komponens értékelése során, mivel ez a szolgáltatás a komponens értékelés során nem volt biztonsági szempontból fontos, vagy a szolgáltatás eredeti célja miatt, vagy pedig az érintett SFR-eket nem vették bele a kiszolgáló komponens ST-jébe (például login interfész, amikor nincs FIA: Azonosítás és hitelesítés SFR). A kiszolgáló komponens ezen interfészeit gyakran funkcionális interfészeknek tekintik a kiszolgáló komponens értékelése során, a funkcionális specifikációban pedig csak a biztonsági interfészek (TSFI) kiegészítéseiként szerepelnek.

Összegezve: a funkcionális specifikációban leírt TSFI-k csak a külső egyedek által a TSF felé történő hívásokat, illetve ezen hívásokra való válaszokat írják le. Egy TSF által végrehajtott olyan hívásokat, melyeket a komponensek értékelése során közvetlenül még nem vizsgáltak, „A kliens komponens környezetfüggősége” (ACO_REL) kielégítése céljából létrehozott környezetfüggőségi információ írja le.

6.1.5.2.1. ACO_REL.1: Alap környezetfüggőségi információ

Függések: Nincsenek függések.

Fejlesztői akcióelemek:

ACO_REL.1.1D A fejlesztőnek biztosítania kell a kliens komponensre vonatkozó környezetfüggőségi információt.

A bizonyíték elemek tartalma és bemutatása:

ACO_REL.1.1C A környezetfüggőségi információnak le kell írnia a kiszolgáló komponens azon hardver, szoftver és/vagy förmver elemeinek funkcionalitását, melyre a kliens komponens TSF támaszkodik.

ACO_REL.1.2C A környezetfüggőségi információnak le kell írnia minden kapcsolatot, amelyen át a kliens komponens TSF-je szolgáltatásokat kér a kiszolgáló komponenstől.

ACO_REL.1.3C A környezetfüggőségi információnak le kell írnia, hogy a kliens TSF hogyan védi magát a kiszolgáló komponens beavatkozásával és manipulálásával szemben.

6.1.5.2.2. ACO_REL.2: Környezetfüggőségi információ

Függések: Nincsenek függések.

Fejlesztői akcióelemek:

ACO_REL.2.1D A fejlesztőnek biztosítania kell a kliens komponensre vonatkozó környezetfüggőségi információt.

A bizonyíték elemek tartalma és bemutatása:

ACO_REL.2.1C A környezetfüggőségi információnak le kell írnia a kiszolgáló komponens azon hardver, szoftver és/vagy förmver elemeinek funkcionalitását, melyre a kliens komponens TSF támaszkodik.

ACO_REL.2.2C A környezetfüggőségi információnak le kell írnia minden kapcsolatot, amelyen át a kliens komponens TSF-je szolgáltatásokat kér a kiszolgáló komponenstől.

ACO_REL.2.3C **A környezetfüggőségi információnak le kell írnia minden egyes interakciót, a használt interfész és az általa visszaadott értékek megadásával.**

ACO_REL.2.4C A környezetfüggőségi információnak le kell írnia, hogy a kliens TSF hogyan védi magát a kiszolgáló komponens beavatkozásával és manipulálásával szemben.

6.1.5.3. Fejlesztési bizonyíték garanciacsalád (ACO_DEV)

Ez a család a kiszolgáló komponens specifikációjára ad meg emelkedő részletezettség-szintű követelményeket. Olyan információkra van szükség, amelyekkel szavatolni lehet a megfelelő biztonsági funkcionalitás fennállását a kliens komponens követelményeinek támogatásához (ahogyan azt a környezetfüggőségi információ azonosította).

A család összetevőinek szintjei (ACO_DEV.1, ACO_DEV.2, ACO_DEV.3) aszerint különböznek, hogy milyen részletességgel kell megadni az interfészekről és azok megvalósításáról szóló információkat.

A kiszolgáló komponens TSF-jét gyakran úgy definiálják, hogy nem ismert, milyen függőségei vannak a lehetséges alkalmazásoknak, amelyekkel integrálható. A kiszolgáló komponens TSF-jét úgy kell meghatározni, hogy tartalmazza a kiszolgáló komponens minden olyan elemét, amelyre építeni kell a kiszolgáló komponens SFR-jeinek érvényre juttatása érdekében. Ez magába foglalja a kiszolgáló komponens minden olyan részét, ami az SFR-jeinek megvalósításához szükséges.

A kiszolgáló komponens funkcionális specifikációja leírja a TSFI-t azon interfészek segítségével, melyeket a kiszolgáló komponens biztosít a külső egyedek számára a TSF műveletek indításához. Ez felöleli az emberi felhasználók számára készített interfészeket (melyek lehetővé teszik a TSF-en keresztül a biztonsági funkcionalitás aktivizálását) és azokat is, amelyek a külső IT entitások számára tesznek lehetővé TSF-hívásokat.

A funkcionális specifikáció csak a TSF által az interfészein keresztül biztosított szolgáltatásokról ad leírást, valamint arról, hogyan hívódik meg a TSF funkcionalitás. Ezért a funkcionális specifikáció nem feltétlenül nyújt teljes interfész specifikációt a külső egyedek és a kiszolgáló komponens közötti összes lehetséges interfészről. Nem tartalmazza, hogy a TSF mit vár el (mit követel meg) a működési környezettől. A „kliens komponens környezetfüggősége” (ACO_REL) tárgyalja azt, hogy melyik kliens komponens TSF használ egy kiszolgáló komponenst, illetve a fejlesztési információ írja le a specifikált interfészekre a válaszokat.

A fejlesztési információ tartalmazza a kiszolgáló komponens specifikációját. Ez lehet a kiszolgáló komponens értékelése során használt bizonyíték az ADV követelményeinek kielégítésére, vagy a kiszolgáló komponens fejlesztője vagy az összetett TOE fejlesztője készíthet más bizonyítékot. Ezt a kiszolgáló komponens specifikációt használják a „fejlesztési bizonyíték" (ACO_DEV) tevékenység során annak a garanciának a bizonyításához, hogy a kliens komponens követelményeinek támogatása érdekében a megfelelő biztonsági funkcionalitás fennáll. E bizonyítékhoz szükséges információmennyiség szintje növekszik az összetett TOE elvárt garanciájának szintjével. Az elvárás az, hogy nagy általánosságban tükrözze a garanciacsomagok komponensekre való alkalmazásából eredő növekvő bizalmat. Az értékelő határozza meg, hogy a kiszolgáló komponens leírása nem mond-e ellent a kliens komponenshez készített környezetfüggőségi információnak.

6.1.5.3.1. ACO_DEV.1: Funkcionális leírás

Szükség van a kliens komponens által használt kiszolgáló komponens interfészeinek leírására. Ennek vizsgálata arra mutat rá, hogy ez a leírás összhangban van-e a környezetfüggőségi információban megadott interfész leírásokkal.

Függések: ACO_REL.1

Fejlesztői akcióelemek:

ACO_DEV.1.1D A fejlesztőnek biztosítania kell a kiszolgáló komponens fejlesztési információt.

A bizonyíték elemek tartalma és bemutatása:

ACO_DEV.1.1C A fejlesztési információnak le kell írnia az összetett TOE-ban használt kiszolgáló komponens minden egyes interfészére azok célját.

ACO_DEV.1.2C A fejlesztési információnak ki kell mutatnia az összetett TOE-ban használt, -a kliens komponens TSF-jét támogató- kiszolgáló, valamint a kliens komponens interfészek közötti megfeleltetéseket.

Értékelői akcióelemek:

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

ACO_DEV.1.2E Az értékelőnek meg kell állapítania, hogy a megadott interfész leírás nem mond-e ellent a kliens komponensre megadott környezetfüggőségi információnak.

6.1.5.3.2. ACO_DEV.2: Alap tervezési bizonyíték

Szükség van a kliens komponens által használt kiszolgáló komponens interfészeinek leírására. Ennek vizsgálata arra mutat rá, hogy ez a leírás összhangban van-e a környezetfüggőségi információban megadott interfész leírásokkal.

A kiszolgáló komponens azon biztonsági viselkedése is leírásra kerül, mely a kliens komponens TSF-jét támogatja.

Függések: ACO_REL.1

Fejlesztői akcióelemek:

ACO_DEV.2.1D A fejlesztőnek biztosítania kell a kiszolgáló komponens fejlesztési információit.

A bizonyíték elemek tartalma és bemutatása:

ACO_DEV.2.1C A fejlesztési információnak le kell írnia az összetett TOE-ban használt kiszolgáló komponens minden egyes interfészére azok célját és használati módját.

ACO_DEV.2.2C **A fejlesztési információnak magas szinten le kell írnia a kiszolgáló komponens azon működését, mely a kliens komponens SFR-jeinek érvényre juttatását támogatja.**

ACO_DEV.2.3C A fejlesztési információnak ki kell mutatnia az összetett TOE-ban használt, -a kliens komponens TSF-jét támogató- kiszolgáló, valamint a kliens komponens interfészek közötti megfeleltetéseket.

Értékelői akcióelemek:

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

ACO_DEV.2.2E Az értékelőnek meg kell állapítania, hogy a megadott interfész leírás nem mond-e ellent a kliens komponensre megadott környezetfüggőségi információnak.

6.1.5.3.3. ACO_DEV.3: Részletes tervezési bizonyíték

Szükség van a kliens komponens által használt kiszolgáló komponens interfészeinek leírására. Ennek vizsgálata arra mutat rá, hogy ez a leírás összhangban van-e a környezetfüggőségi információban megadott interfész leírásokkal.

A kiszolgáló komponens architektúrájának interfész leírása az értékelőt abban segíti, hogy megállapítsa, hogy a kiszolgáló komponens TSF-jének részét képezi-e az interfész.

Függések: ACO_REL.2

Fejlesztői akcióelemek:

ACO_DEV.3.1D A fejlesztőnek biztosítania kell a kiszolgáló komponens fejlesztési információit.

A bizonyíték elemek tartalma és bemutatása:

ACO_DEV.3.1C A fejlesztési információnak le kell írnia az összetett TOE-ban használt kiszolgáló komponens minden egyes interfészére azok célját és használati módját.

ACO_DEV.3.2C **A fejlesztési információnak azonosítania kell a kiszolgáló komponens azon alrendszereit, amelyek az összetett TOE-ban használt kiszolgáló komponens interfészeket biztosítják.**

ACO_DEV.3.3C A fejlesztési információnak magas szinten le kell írnia a kiszolgáló komponens azon **alrendszereinek** működését, melyek a kliens komponens SFR-jeinek érvényre juttatását támogatják.

ACO_DEV.3.4C A fejlesztési információnak meg kell adnia az interfészeknek a kiszolgáló komponensbeli alrendszerekre való leképezését.

ACO_DEV.3.5C A fejlesztési információnak ki kell mutatnia az összetett TOE-ban használt, -a kliens komponens TSF-jét támogató- kiszolgáló, valamint a kliens komponens interfészek közötti megfeleltetéseket.

Értékelői akcióelemek:

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

ACO_DEV.3.2E Az értékelőnek meg kell állapítania, hogy a megadott interfész leírás nem mond-e ellent a kliens komponensre megadott környezetfüggőségi információnak.

6.1.5.4. Komponens-összeállítás indoklás garanciacsalád (ACO_COR)

Ez a család azt hivatott megmutatni, hogy a kiszolgáló komponens képes biztosítani a garancia megfelelő szintjét a komponens-összeállításban való használathoz.

Ez a család csak egy összetevőt tartalmaz (ACO_COR.1).

6.1.5.4.4. ACO_COR.1: Komponens-összeállítás indoklás

Függések: ACO_DEV.1, ALC_CMC.1, ACO_REL.1

Fejlesztői akcióelemek:

ACO_COR.1.1D A fejlesztőnek biztosítania kell a komponens-összeállítás indoklást a kiszolgáló komponensre.

A bizonyíték elemek tartalma és bemutatása:

ACO_COR.1.1C A komponens-összeállítás indoklásnak meg kell mutatnia, hogy a garanciaszint legalább olyan magas, mint amit a kliens komponens elért a kiszolgáló komponens támogató funkciójára, amikor a kiszolgáló komponenst a kliens komponens TSF-jének támogatására konfigurálták.

Értékelői akcióelemek:

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

6.1.5.5. Az összetett TOE tesztelése garanciacsalád (ACO_CTT)

Ez a család megköveteli az összetett TOE tesztelését, valamint a kiszolgáló komponensnek az összetett TOE-n belüli használata szerinti tesztelését.

A család összetevőinek szintjei (ACO_CTT.1, ACO_CTT.2) az interfész tesztelés szigorúsága és a tesztek megfelelőség elemzésével kapcsolatos növekvő szigor szerint különböznek, ami annak megmutatásához kell, hogy az összetett TSF a környezetfüggőségi információnak és az összetett TOE SFR-eknek megfelelően működik.

E családhoz kapcsolódóan két különböző tesztelési szempont van:

- A kompatibilitás bizonyítása érdekében a kiszolgáló és a kliens komponens közötti azon interfészek tesztelése, melyekre a kliens komponens épít biztonsági funkcionalitásának érvényre juttatásához;
- Az összetett TOE tesztelése annak megmutatása céljából, hogy a TOE az összetett TOE SFR-jeinek megfelelően működik.

Amennyiben a kliens komponens értékelése során használt teszt konfiguráció tartalmazta a kiszolgáló komponenst „platformként”, és a teszt elemzése kielégítő módon megmutatta, hogy a TSF az SFR-eknek megfelelően működik, akkor a fejlesztőnek nem szükséges tovább tesztelnie az összetett TOE funkcionalitását. Azonban, ha a kiszolgáló komponenst nem használták a kliens komponens tesztelése során, vagy bármelyik komponens konfigurációja változott, akkor a fejlesztőnek el kell végeznie az összetett TOE tesztelését. Ez jelentheti a kliens komponens fejlesztői tesztelésének megismétlését, feltéve, ha ez a tesztelés kielégítően bizonyítja, hogy az összetett TOE TSF az SFR-eket teljesítő módon működik.

A fejlesztőnek rendelkezésre kell bocsátania a TOE összeállításához használt kiszolgáló komponens interfészek tesztelési bizonyítékait. A kiszolgáló komponens TSF interfészeinek működését az ATE: Tesztelési tevékenység részeként kellett elvégezni a kiszolgáló komponens értékelése során. Ezért, feltéve, hogy a kiszolgáló komponens értékelésének teszt mintáiban a megfelelő interfészek szerepeltek, és a „Komponens-összeállítás indoklás”

(ACO_COR) megállapította, hogy a kiszolgáló komponens az értékelt konfigurációjának megfelelően működik a TSF-ben szereplő, a kliens komponens által megkövetelt összes biztonsági funkcionalitással, akkor az ACO_CTT.1.1E értékelői tevékenységnek eleget lehet tenni a kiszolgáló komponens ATE: Tesztelési tevékenység értékelői tevékenység eredményeinek újrafelhasználásával.

Ha a fenti feltétel nem teljesül, akkor tesztelni kell a TOE összeállítás szempontjából fontos kiszolgáló komponens azon interfészeit, melyeket az értékelt konfigurációhoz képest bármilyen módosítás befolyásolt, valamint minden új biztonsági funkcionalitást, az elvártnak megfelelő működés biztosítása érdekében. A tesztelendő elvárt működés az, amit a környezetfüggőségi információ leír („Kliens komponens környezetfüggősége” (ACO_REL)).

6.1.5.5.1. ACO_CTT.1: Interfész tesztelés

Ennek az összetevőnek a célja annak biztosítása, hogy a kiszolgáló komponens minden olyan interfészét letesztelték, amelyre a kliens komponens működése során támaszkodik.

Függések: ACO_REL.1, ACO_DEV.1

Fejlesztői akcióelemek:

ACO_CTT.1.1D A fejlesztőnek biztosítania kell az összetett TOE tesztelési dokumentációját.

ACO_CTT.1.2D A fejlesztőnek biztosítania kell a kiszolgáló komponens interfész tesztelési dokumentációját.

ACO_CTT.1.3D A fejlesztőnek rendelkezésre kell bocsátania az összetett TOE-t tesztelés céljából.

ACO_CTT.1.4D A fejlesztőnek biztosítania kell a kiszolgáló komponens fejlesztői funkcionális tesztelése során használt erőforrásokkal megegyező erőforrásokat.

A bizonyíték elemek tartalma és bemutatása:

ACO_CTT.1.1C Az összetett TOE és a kiszolgáló komponens interfész tesztelési dokumentációjának tartalmaznia kell a tesztelési terveket, az elvárt teszteredményeket és a tényleges (kapott) teszt-eredményeket.

ACO_CTT.1.2C Az összetett TOE tesztek fejlesztő által történt elvégzéséből származó tesztelési dokumentációnak meg kell mutatnia, hogy a TSF a specifikáltnak megfelelően működik.

ACO_CTT.1.3C A kiszolgáló komponens interfész tesztek fejlesztő által történt elvégzéséből származó tesztelési dokumentációnak meg kell mutatnia, hogy a kliens komponens által használt kiszolgáló komponens interfész a specifikáltnak megfelelően működik.

ACO_CTT.1.4C A kiszolgáló komponensnek tesztelésre alkalmasnak kell lennie.

Értékelői akcióelemek:

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

ACO_CTT.1.2E Az értékelőnek végre kell hajtania a tesztelési dokumentációban szereplő tesztek egy mintáját a fejlesztői teszteredmények ellenőrzése céljából.

ACO_CTT.1.3E Az értékelőnek le kell tesztelnie az összetett TOE TSF interfészeinek egy részhalmazát, hogy meggyőződjön arról, hogy az összetett TSF a specifikáltnak megfelelően működik.

6.1.5.5.2. ACO_CTT.2: Szigorú interfész tesztelés

Ennek az összetevőnek a célja annak biztosítása, hogy a kiszolgáló komponens minden olyan interfészét letesztelték, amelyre a kliens komponens működése során támaszkodik.

Függések: ACO_REL.2, ACO_DEV.2

Fejlesztői akcióelemek:

ACO_CTT.2.1D A fejlesztőnek biztosítania kell az összetett TOE tesztelési dokumentációját.

ACO_CTT.2.2D A fejlesztőnek biztosítania kell a kiszolgáló komponens interfész tesztelési dokumentációját.

ACO_CTT.2.3D A fejlesztőnek rendelkezésre kell bocsátania az összetett TOE-t tesztelés céljából.

ACO_CTT.2.4D A fejlesztőnek biztosítania kell a kiszolgáló komponens fejlesztői funkcionális tesztelése során használt erőforrásokkal megegyező erőforrásokat.

A bizonyíték elemek tartalma és bemutatása:

ACO_CTT.2.1C Az összetett TOE és a kiszolgáló komponens interfész tesztelési dokumentációjának tartalmaznia kell a tesztelési terveket, az elvárt teszteredményeket és a tényleges (kapott) teszteredményeket.

ACO_CTT.2.2C Az összetett TOE tesztek fejlesztő által történt elvégzéséből származó tesztelési dokumentációnak meg kell mutatnia, hogy a TSF a specifikáltnak megfelelően működik **és teljes.**

ACO_CTT.2.3C A kiszolgáló komponens interfész tesztek fejlesztő által történt elvégzéséből származó tesztelési dokumentációnak meg kell mutatnia, hogy a kliens komponens által használt kiszolgáló komponens interfész a specifikáltnak megfelelően működik **és teljes.**

ACO_CTT.2.4C A kiszolgáló komponensnek tesztelésre alkalmasnak kell lennie.

Értékelői akcióelemek:

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

ACO_CTT.2.2E Az értékelőnek végre kell hajtania a tesztelési dokumentációban szereplő tesztek egy mintáját a fejlesztői teszteredmények ellenőrzése céljából.

ACO_CTT.2.3E Az értékelőnek le kell tesztelnie az összetett TOE TSF interfészeinek egy részhalmazát, hogy meggyőződjön arról, hogy az összetett TSF a specifikáltnak megfelelően működik.

6.1.5.6. Összetett sebezhetőség elemzés garanciacsalád (ACO_VUL)

Ez a család a nyilvánosan hozzáférhető sebezhetőségekkel kapcsolatos információk elemzését és a TOE összeállítás következményeként esetleg felmerülő sebezhetőségeket célozza meg.

A család összetevőinek szintjei (ACO_VUL.1, ACO_VUL.2, ACO_VUL.3) aszerint különböznek, hogy emelkedő szintű a nyilvános forrásból származó sebezhetőségi információkkal és a független sebezhetőséggel kapcsolatos vizsgálat szigorúsága.

A fejlesztőnek rendelkezésre kell bocsátania minden olyan maradvány sebezhetőséget, ami a komponensek értékelése során felmerült. Ezek beszerezhetők a komponensek fejlesztőitől vagy az értékelési jelentésekből, és az összetett TOE működési környezetére vonatkozó értékelői sebezhetőség elemzéshez bemeneteként szolgának.

Az összetett TOE működési környezetének vizsgálata annak biztosítása miatt szükséges, hogy a komponens működési környezetekre vonatkozó feltételezések és célok (a komponens ST-kben megadva) teljesülnek az összetett TOE-ra. A komponens és az összetett TOE ST-ben szereplő feltételezések és célok közötti ellentmondás-mentesség kezdeti elemzését az összetett TOE-ra vonatkozó ASE tevékenység során végzik el. Ezt a vizsgálatot azonban meg kell ismételni az ACO_REL, ACO_DEV és ACO_COR tevékenységek során szerzett tudás birtokában, biztosítandó, hogy például a kliens komponens ST-jében a környezetre vonatkozó feltételezéseket nem vezetik be újra az összetétel következményeként (azaz a kiszolgáló komponens megfelelően kezeli az összetett TOE kliens komponens ST-jében lévő feltételezéseket).

Egy az értékelő által végrehajtott probléma feltárás azonosítja minden komponensre azokat a lehetséges sebezhetőségeket, melyeket nyilvánosan közzétettek a komponensek értékelésének befejezése óta. Bármilyen lehetséges sebezhetőség ezután tesztelés tárgyát képezi.

6.1.5.6.1. ACO_VUL.1: Komponens-összeállítás sebezhetőségi áttekintés

Függések: ACO_DEV.1

Fejlesztői akcióelemek:

ACO_VUL.1.1D A fejlesztőnek biztosítania kell az összetett TOE-t tesztelés céljából.

A bizonyíték elemek tartalma és bemutatása:

ACO_VUL.1.1C Az összetett TOE-nak tesztelésre alkalmasnak kell lennie.

Értékelői akcióelemek:

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

ACO_VUL.1.2E Az értékelőnek végre kell hajtania egy vizsgálatot annak megállapítása érdekében, hogy a kiszolgáló és a kliens komponensre beazonosított bármilyen maradvány sebezhetőség nem aknázható ki az összetett TOE-ban, annak működési környezetében.

ACO_VUL.1.3E Az értékelőnek kutatnia kell a nyilvánosan hozzáférhető forrásokat a kiszolgáló és a kliens komponensnek az összetett TOE működési környezetében való használatából származó lehetséges sebezhetőségeinek feltárása céljából.

ACO_VUL.1.4E Az értékelőnek behatolás tesztelést kell végeznie, ami az azonosított sebezhetőségeken alapul, annak megmutatása céljából, hogy az összetett TOE ellenáll az alap támadási képességgel rendelkező támadó támadásainak.

6.1.5.6.2. ACO_VUL.2: Komponens-összeállítás sebezhetőségi elemzés

Függések: ACO_DEV.2

Fejlesztői akcióelemek:

ACO_VUL.2.1D A fejlesztőnek biztosítania kell az összetett TOE-t tesztelés céljából.

A bizonyíték elemek tartalma és bemutatása:

ACO_VUL.2.1C Az összetett TOE-nak tesztelésre alkalmasnak kell lennie.

Értékelői akcióelemek:

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

ACO_VUL.2.2E Az értékelőnek végre kell hajtania egy vizsgálatot annak megállapítása érdekében, hogy a kiszolgáló és a kliens komponensre beazonosított bármilyen maradvány sebezhetőség nem aknázható ki az összetett TOE-ban, annak működési környezetében.

ACO_VUL.2.3E Az értékelőnek kutatnia kell a nyilvánosan hozzáférhető forrásokat a kiszolgáló és a kliens komponensnek az összetett TOE működési környezetében való használatából származó lehetséges sebezhetőségeinek feltárása céljából.

ACO_VUL.2.4E **Az értékelőnek végre kell hajtania egy független sebezhetőség elemzést az összetett TOE-ra, az útmutató dokumentáció, környezetfüggőségi információ és komponens-összeállítás indoklás felhasználásával, az összetett TOE-ban fellelhető lehetséges sebezhetőségek azonosítására.**

ACO_VUL.2.5E Az értékelőnek behatolás tesztelést kell végeznie, ami az azonosított sebezhetőségeken alapul, annak megmutatása céljából, hogy az összetett TOE ellenáll az alap támadási képességgel rendelkező támadó támadásainak.

6.1.5.6.3. ACO_VUL.3: Megemelt alap szintű komponens-összeállítás sebezhetőségi elemzés

Függések: ACO_DEV.3

Fejlesztői akcióelemek:

ACO_VUL.3.1D A fejlesztőnek biztosítania kell az összetett TOE-t tesztelés céljából.

A bizonyíték elemek tartalma és bemutatása:

ACO_VUL.3.1C Az összetett TOE-nak tesztelésre alkalmasnak kell lennie.

Értékelői akcióelemek:

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

ACO_VUL.3.2 Az értékelőnek végre kell hajtania egy vizsgálatot annak megállapítása érdekében, hogy a kiszolgáló és a kliens komponensre beazonosított bármilyen maradvány sebezhetőség nem aknázható ki az összetett TOE-ban, annak működési környezetében.

ACO_VUL.3.3E Az értékelőnek kutatnia kell a nyilvánosan hozzáférhető forrásokat a kiszolgáló és a kliens komponensnek az összetett TOE működési környezetében való használatából származó lehetséges sebezhetőségeinek feltárása céljából.

ACO_VUL.3.4E Az értékelőnek végre kell hajtania egy független sebezhetőség elemzést az összetett TOE-ra, az útmutató dokumentáció, környezetfüggőségi információ és komponens-összeállítás indoklás felhasználásával, az összetett TOE-ban fellelhető lehetséges sebezhetőségek azonosítására.

ACO_VUL.3.5E Az értékelőnek behatolás tesztelést kell végeznie, ami az azonosított sebezhetőségeken alapul, annak megmutatása céljából, hogy az összetett TOE ellenáll a **megemelt alap** támadási képességgel rendelkező támadó támadásainak.

6.1.5.7. Az összetett termék komponensei közötti egymásra hatások

Az összetett terméket alkotó komponensek egymásra hatásainak áttekintése hozzásegít annak megértéséhez, hogy egy összetett TOE értékelése milyen új vizsgálatokat igényel a már sikeresen értékelt komponensekhez képest. Ez az összetett termékek értékelésének alább kifejtett két nehézségéből származik.

Az összetett termékek értékelésének egyik nehézsége abból adódik, hogy a kiszolgáló komponens biztonsági funkcionalitását (TSF) gyakran úgy határozzák meg, hogy még nem ismerik azokat az alkalmazásokat (és az ebből adódó függőségeket), amelyekkel ez a komponens különböző összetett termékekben együtt fog működni a jövőben.

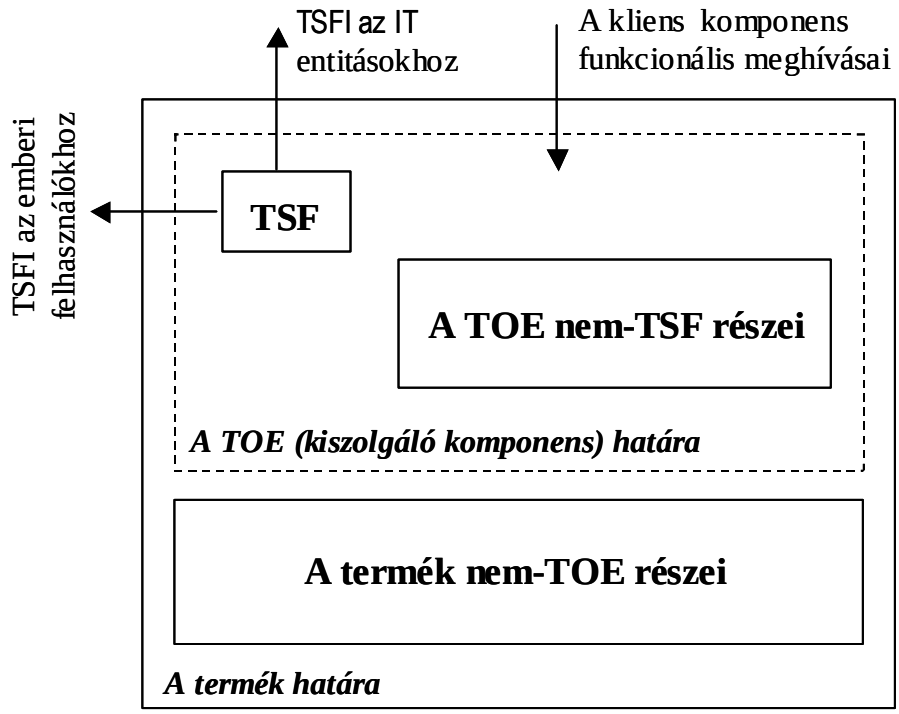
A kiszolgáló komponens TSF-je a komponens összes olyan elemét magában foglalja, amelyekre építeni kell a kiszolgáló komponens biztonsági követelményeinek (SFR) érvényre juttatásához.

A kiszolgáló komponens TSFI-je a TSF által a külső egyedek számára biztosított (a TSF szolgáltatásainak meghívására szolgáló) interfészeket jelenti. Ez egyaránt felöleli az emberi felhasználók és a külső IT entitások számára biztosított interfészeket. A TSFI azonban csak a TSF felé irányuló interfészeket tartalmazza, ezért nem feltétlenül ad teljes interfész specifikációt a kiszolgáló komponens és a külső egyedek közötti összes lehetséges interfészre. A kiszolgáló komponens ajánlhat interfészeket biztonsági szempontból nem jelentősnek ítélt szolgáltatásokhoz is.

A kiszolgáló komponens által biztosított funkcionális interfészek a biztonsági interfészeket (TSFI) kiegészítik, és azokat nem vizsgálják a kiszolgáló komponens értékelése során. Ugyanakkor ezeket az interfészeket is gyakran meghívják a kiszolgáló komponens szolgáltatásaira épülő kliens komponensek.

A kiszolgáló komponens tartalmazhat olyan közvetett interfészeket is, amelyeken keresztül a TSFI-k meghívhatók (például a TSF egy szolgáltatásának meghívására használható API-kat), de amelyeket nem vettek figyelembe a kiszolgáló komponens értékelése során.

A kiszolgáló komponens és interfészeinek absztrakcióját mutatja a 4. ábra.



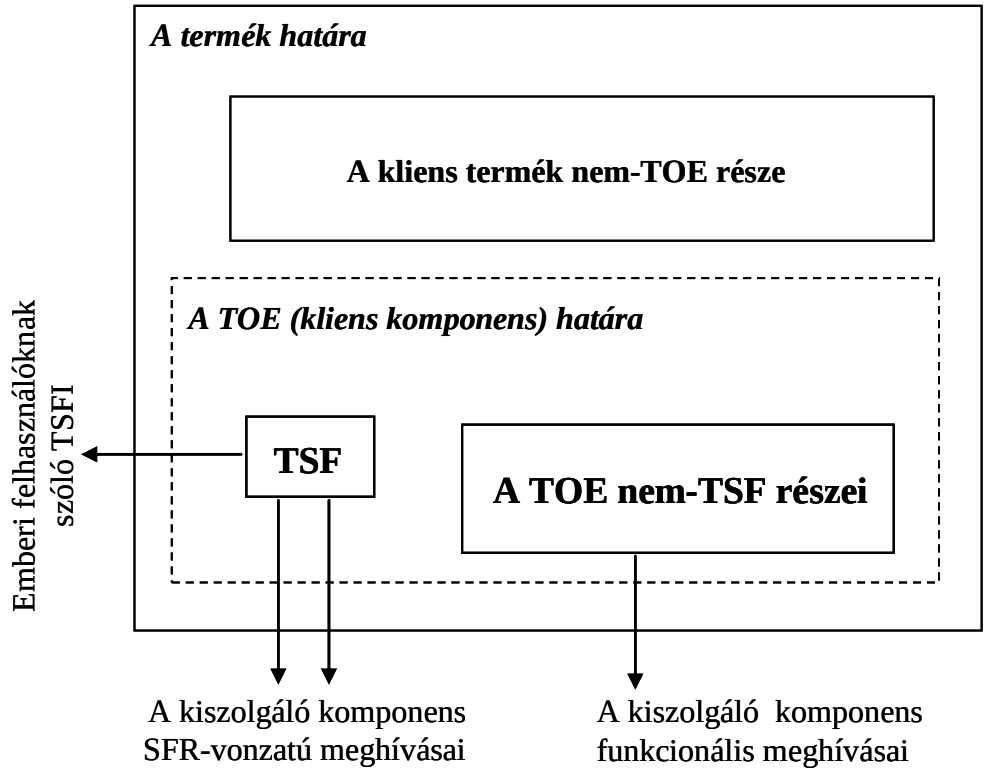
4. ábra - A kiszolgáló komponens absztrakciója

A kliens komponens működése során támaszkodik a kiszolgáló komponens szolgáltatásaira, köztük biztonsági szolgáltatásokra is. A kliens komponens TSFI-jéhez tartoznak azok az interfészei, melyeken keresztül a kiszolgáló komponens biztonsági szolgáltatásaira támaszkodik. Ezeket a kliens komponens értékelése során (az ADV_FSP értékelői tevékenységnél) megvizsgálták.

Egy SFR támogatása céljából a kliens TSF-ből a környezetbe való minden hívás azt mutatja, hogy a kliens TSF a környezettől vár el bizonyos szolgáltatást a kliens SFR-ek érvényre juttatása érdekében. De egy ilyen szolgáltatás kívül esik a kliens komponens határain, és nem valószínű, hogy a kiszolgáló komponenst a kliens ST-ben külső egyedként definiálják.

Az összetett termékek értékelésének másik nehézsége ezért abból adódik, hogy a kliens TSF által az alapot képező platformra (kiszolgáló komponensre) való szolgáltatás-hívásokat nem elemezték a funkcionális specifikáció (ADV_FSP) értékelői tevékenység részeként. (A kiszolgáló komponensre vonatkozó ilyen függéseket a kliens komponens ST-ben környezetre vonatkozó biztonsági célokként fejezték ki, s csak feltételezték annak kielégítését).

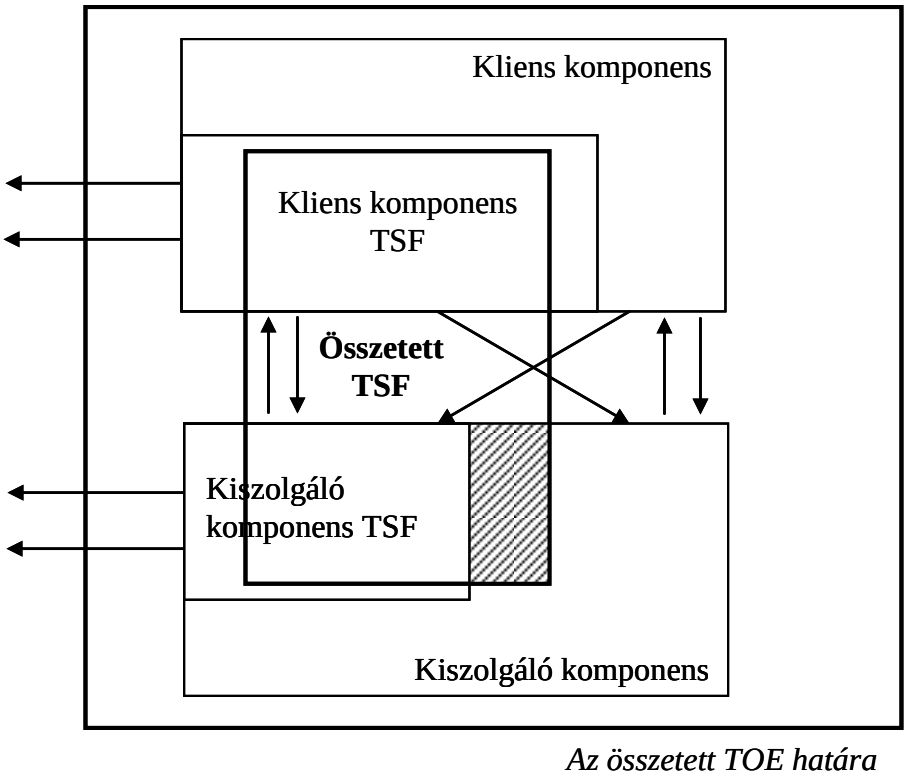
A kliens komponens és interfészeinek absztrakcióját mutatja az 5. ábra.



5. ábra - A kliens komponens absztrakciója

A kiszolgáló és a kliens komponens összeállításának kialakításakor –ha a kliens komponens TSF-je szolgáltatásokat kér a kiszolgáló komponenstől az SFR megvalósításához–, definiálni kell a szolgáltatáshoz tartozó interfészt. Ha ezt a szolgáltatást a kiszolgáló komponens TSF-je biztosítja, akkor az interfésznek a kiszolgáló komponens TSFI-jének kell lennie, és ezért szerepelnie kell a kiszolgáló komponens funkcionális specifikációjában.

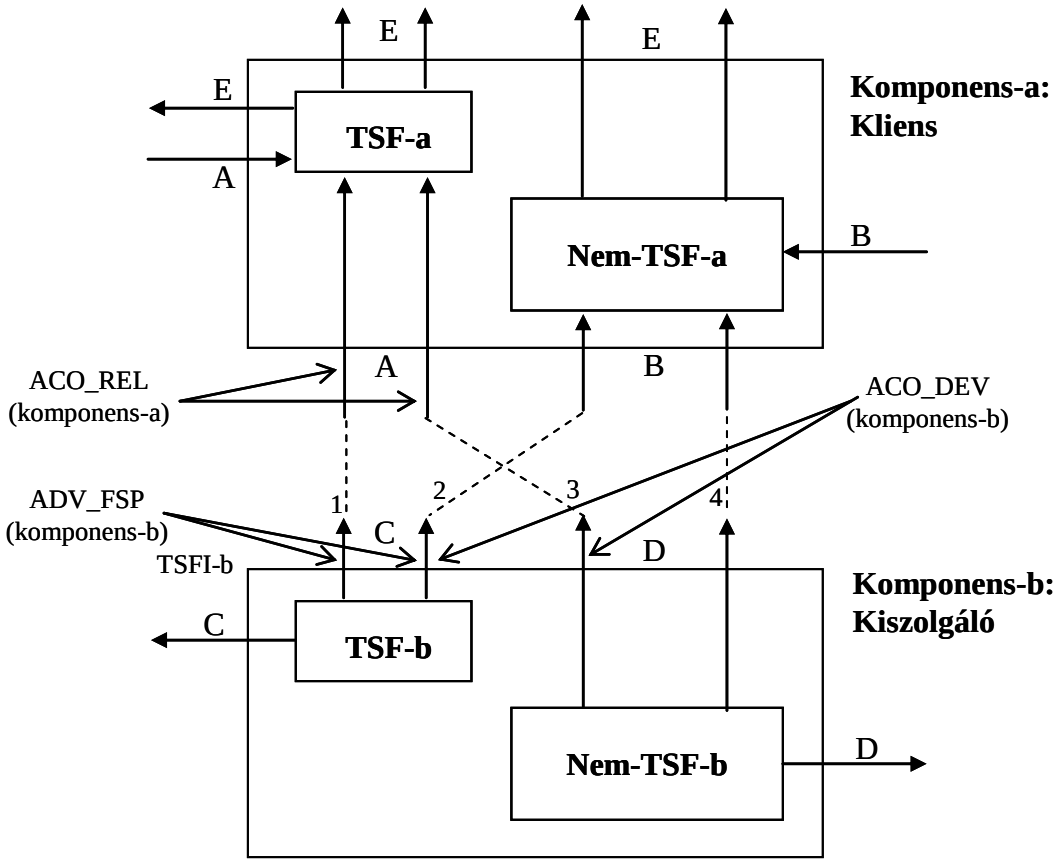
Amennyiben azonban a kliens komponens TSF által hívott szolgáltatást nem biztosítja a kiszolgáló komponens TSF-je (azaz azt a kiszolgáló komponens nem TSF része valósítja meg, vagy a kiszolgáló komponens nem TOE hatókörbe eső része (az 5. ábrán nem szereplő rész)), akkor nem valószínű, hogy a szolgáltatáshoz kapcsolódó kiszolgáló komponens TSFI-je legyen, hacsak a szolgáltatást nem közvetíti a kiszolgáló komponens TSF-je. A kliens komponenstől a működési környezet felé irányuló ilyen szolgáltatások interfészeivel tehát külön kell foglalkozni az összetett termékek értékelése során. Az ezzel kapcsolatos vizsgálatokat végzi el a „Kliens komponens környezetfüggősége” (ACO_REL) garanciacsalád.



6. ábra - Az összetett TOE absztrakciója

A kiszolgáló komponens nem TSF része is az összetett TOE TSF-jébe kerülhet, ha a kliens komponens támaszkodik erre saját SFR-jeinek kielégítéséhez. Az ilyen esetekben tehát az összetett TOE TSF-je bővebb lesz, mint az alkotó TSF-ek egyszerű uniója.

Előfordulhat, hogy a kiszolgáló komponens TSFI-jét oly módon hívják meg, amit nem lehetett előre látni a kiszolgáló komponens értékelése során. Ezért követelmény a kiszolgáló komponens TSFI további tesztelése is.



7. ábra - Az összetett TOE interfészei

A 7. ábra és a hozzá tartozó szöveg tovább jellemzi a lehetséges interfészeket:

- A "kliens komponens-a" (A és B) felé mutató nyilak = a komponens-a környezetétől várja el, hogy válaszoljon egy szolgáltatás kérésre (válasz a kliens komponensből a környezet felé irányuló hívásokra);
- A "kiszolgáló komponens-b" (C és D)-ből jövő nyilak = a kiszolgáló komponens által a környezetnek nyújtott szolgáltatások interfészei;
- A komponensek közötti szaggatott vonalak = interfész-párok közötti kommunikáció típusai;
- Egyéb (szürke) nyilak = a jelzett garanciacsalád követelményei szerint vizsgált interfészek.
- „a" jelöli a kliens komponens-a-t, „b" pedig a kiszolgáló komponens–b-t.
- A TSF-a-ból kijövő nyilak („A") a TSF-a által biztosított szolgáltatások, ezért TSFI(a).
- A TSF-b-ből kijövő nyilak („C") a TSFI(b).
- TSFI(a)-t és TSFI(b)-t a komponensre vonatkozó funkcionális specifikációk részletezik.
- A komponens-a szolgáltatásokat kér a környezetétől: azok, amiket a TSF(a) igényel az „A" címkéjűek; az egyéb (nem TSF-a-hoz kapcsolódó) szolgáltatások a „B" címkéjűek.

Az a és b komponens integrálása esetén a {komponens-a által igényelt szolgáltatások} és a {komponens-b által biztosított szolgáltatások}-nak négy lehetséges kombinációja lehet, amit a

szaggatott vonal mutat (interfész-párok közötti kommunikáció típusai). Ezek bármilyen halmaza létrejöhet egy adott összeállításra:

1. TSF-a kéri azokat a szolgáltatásokat, melyeket a TSF-b nyújt (“A” csatlakozik “C”-hez): Ez az eset egyértelmű: a “C”-re vonatkozó részletek a komponens-b FSP-jében vannak. Ekkor komponens-a és komponens-b funkcionális specifikációi megadnak minden interfészt.

2. A “nem-TSF-a” kéri a TSF-b által nyújtott szolgáltatásokat (“B” csatlakozik “C”-hez): Ez az eset is egyértelmű: (a “C”-vel kapcsolatos részletek ismét a komponens-b FSP-jében vannak), de biztonsági szempontból nem fontosak.

3. A “TSF-a” kéri a “nem TSF-b” szoláltatásait (“A” csatlakozik “D”-hez): Ez akkor merül fel, amikor a komponens-a és a komponens-b különbözőképpen értelmezi a “biztonsági szolgáltatás” fogalmát. Például a komponens-b nem fogalmaz meg azonosításra és hitelesítésre vonatkozó követelményt (nincs FIA SFR az ST-jében), de a komponens-a-nak szüksége van a környezet által biztosított hitelesítésre. Ebben az esetben nem áll rendelkezésre információ a “D” interfészekről, mert azok nem a TSFI(b) részei, így nem képezik részét a komponens-b FSP-jének.

4. A “nem-TSF-a” kéri a “nem TSF-b” által nyújtott szolgáltatásokat (“B” csatlakozik “D”-hez): Ebben az esetben nincs információ D-ről, de az interfészek használatának nincsenek biztonsági kihatásai, így azokat ki lehet hagyni az értékelés során, a fejlesztő számára ugyanakkor valószínűleg integrálási szempontot jelentenek.

Megjegyzés: Ha a fenti 3. esetben leírt kölcsönhatás létezik, akkor az összetett TOE TSF-je: TSF-a + TSF-b + „Nem-TSF-b” lesz. Egyébként az összetett TOE TSF-je: TSF-a + TSF-b.

A 7. ábra 2. és 4. interfész típusai az összetett TOE értékelése szempontjából nem közvetlenül fontosak. Az 1. és 3. interfészeket kell figyelembe venni a különböző családok alkalmazása során:

- A (komponens-b) „Funkcionális specifikáció”-ja (ADV_FSP) leírja a C interfészeit.
- A „Kliens komponens környezetfüggősége” (ACO_REL) leírja A interfészeit.
- A „Fejlesztési bizonyíték” (ACO_DEV) leírja a C interfészeit az 1. kapcsolat típusra, és a D interfészeit a 3. kapcsolat típusra.

Tipikus példa komponens-összeállítás alkalmazására egy adatbázis-kezelő rendszer (DBMS), ami használja az alapul szolgáló operációs rendszert. A DBMS komponens értékelése során felmérik a DBMS biztonsági tulajdonságait (az értékelés garancia-összetevői által előírt szigorral): azonosításra kerülnek a TSF határai, megvizsgálják a funkcionális specifikációt, hogy az leírja-e a TSF által nyújtott biztonsági szolgáltatásokhoz szükséges interfészeket, esetleg további információkat biztosítanak a TSF-ről (terv, biztonsági szerkezet), tesztelik a TSF-et, ellenőrzik az életciklus és az útmutató dokumentációkat stb.

A DBMS értékelés azonban nem vár el bizonyítékot arról, hogy a DBMS milyen mértékben függ az operációs rendszertől. A DBMS biztonsági előirányzata nagy valószínűséggel feltételezéseket tesz az OS-ről a feltételezések részben, és a környezetre vonatkozó szakaszban megfogalmazza az OS-re vonatkozó biztonsági célokat. A DBMS ST még konkrétabbá is teheti e környezeti célokat operációs rendszerre vonatkozó SFR-ek

formájában. Azonban nem fog tartalmazni olyan OS specifikációt, ami tükrözi a funkcionális specifikáció, a biztonsági szerkezet leírás vagy más ADV bizonyíték részletességét. Ezt az igényt a „Kliens komponens környezetfüggősége” (ACO_REL) hivatott teljesíteni.

A „Kliens komponens környezetfüggősége” (ACO_REL) leírja a kliens TOE azon interfészeit, amelyek szolgáltatások kielégítése érdekében hívásokat kezdeményeznek a kiszolgáló komponens felé. Ezek azok az interfészek, amelyekre a kiszolgáló komponens válaszol. Az interfész leírásokat a kliens komponens oldaláról kell megadni.

A „Fejlesztési bizonyíték” (ACO_DEV) leírja a kiszolgáló komponens által biztosított azon interfészeket, amelyek a kliens komponens szolgáltatáskéréseire válaszolnak. Ezek az interfészek leképezhetők a megfelelő kliens komponens interfészekre, melyeket a környezetfüggőségi információ azonosít. (E leképezés teljessége –hogy a kiszolgáló komponens interfészek minden kliens komponens interfészt képviselnek– nem itt kerül ellenőrzésre, hanem a „Komponens-összeállítás indoklás”-ban (ACO_COR)). Az ACO_DEV magasabb szintjein az interfészeket biztosító alrendszereket is le kell írni.

A kiszolgáló komponensre nem leírt, de a kliens komponens által igényelt bármely interfészt a „Komponens-összeállítás indoklás” (ACO_COR) indoklás része tartalmazza. Az indoklás azt is tárgyalja, hogy azokat a kiszolgáló komponens interfészeket, amelyekre a kliens komponens számít működése során, figyelembe vették-e a kiszolgáló komponens értékelésekor. Minden olyan interfész esetén, amelyet nem vizsgáltak a kiszolgáló komponens értékelése során, indoklást kell adni az interfész használatának a kiszolgáló komponens TSF-jére gyakorolt hatásáról.

6.1.6. Kiegészítő garancia-összetevők

A 2. táblázat összegzi a három összetett garanciacsomagot. Ebből jól látszik, hogy az egyes összetett garanciacsomagok a komponens-összeállítás (ACO) garanciaosztály különböző garancia-összetevőin kívül tartalmaznak még egyéb, a termékértékelésnél már meghatározott garancia-összetevőket is. Ezek a kiegészítő garancia-összetevők megegyeznek mindhárom összetett garanciacsomagban.

6.1.6.1. A kiegészítő garancia-összetevők áttekintése

Mindhárom összetett garanciacsomag tartalmazza az alábbi kiegészítő garancia-összetevőket:

- Előkészítő eljárások (AGD_PRE.1) – az összetett termék komponenseinek telepítése, biztonságos konfigurálása (integrálás).
- Üzemeltetési felhasználói útmutató (AGD_OPE.1) – az összetett termék biztonságos üzemeltetése.
- A TOE megcímkézése (ALC_CMC.1) – az összetett termék egységes megcímkézése.
- A TOE részeinek CM lefedettsége (ALC_CMS.2) - konfiguráció lista az alábbiakról: összetett termék, komponensei, az értékelési bizonyítékok.

6.1.6.2. Előkészítő eljárások (AGD_PRE.1)

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.1)

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.

6.1.6.4. A TOE megcímkézése (ALC_CMC.1)

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 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.

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

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.

6.2. Útmutató az összetett termékek biztonsági értékelői számára

6.2.1. Összetett TOE biztonsági előirányzatának értékelése

Az összetett TOE (kiszolgáló komponens + kliens komponens) értékeléséhez a fejlesztőnek ST-t kell benyújtania, ami azonosítja az összetett TOE-ra alkalmazandó garanciacsomagot is.

Az összetett TOE-re vonatkozó ST értékelésének legfontosabb célja annak ellenőrzése, hogy a komponensek mind a környezet, mind a követelmények szempontjából kompatibilisek egymással, egyúttal az összetett TOE ST nem mond ellent a komponensek ST-inek és a bennük kifejtett biztonsági szabályzatoknak.

Az összetett termék ST értékelési tevékenysége nagyon hasonlít a termékre (ami lehet egy összetett TOE komponense is) vonatkozó ST értékelési tevékenységére. Ugyanakkor, mivel az összetett TOE biztonsági előirányzatára néhány kiegészítő követelmény is vonatkozik, igaz ez ennek értékelésére is. A kiegészítő feladatok jól megkülönböztethetők az értékelői tevékenységek részletes leírásában (6.2.2–6.2.4 alfejezetekben), mindig az alábbi kifejezéssel kezdődnek: „Összetett TOE esetén”.

Alkalmazási megjegyzések tanúsított PP-k értékelési eredményeinek újra felhasználásáról:
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.

6.2.1.1. Biztonsági előirányzat értékelése CAP-A esetén

6.2.1.1.1. 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.

6.2.1.1.1.1. 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.

Olyan értékelésekben, melyek CM rendszert is használnak, az értékelő érvényesítheti a hivatkozások egyediségét a konfiguráció lista ellenőrzésével. Más esetekben, az ST-nek kell valamilyen hivatkozási módszert alkalmaznia, ami képes az egyedi hivatkozások támogatására (pl. számozás, betűk vagy dátumok használata).

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.

Összetett TOE esetén az ST-ben szereplő TOE áttekintésnek az összetett TOE használatát és fő biztonsági tulajdonságait kell leírnia, nem pedig az összetett TOE egyes elemeire vonatkozó információkat.

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 működtetési 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 nem-TOE 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 nem-TOE 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.

Összetett TOE esetén az ST hivatkozhat az összetevő TOE-k logikai határainak leírására, melyek az alkotó TOE-k ST-iben szerepelnek, és az összetett TOE leírásának nagy részét képezik. Azonban az értékelőnek meg kell állapítania, hogy az összetett TOE ST-je egyértelműen leírja-e, hogy az egyedi komponensek melyik szolgáltatása nem tartozik az összetett TOE-ba, következésképp nem jelenik meg az összetett TOE-ban sem tulajdonságként.

6.2.1.1.1.2. 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.

6.2.1.1.2. 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.

6.2.1.1.2.1. 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.

Összetett TOE esetén az értékelő vegye figyelembe az egyes összetevőknél használt CC verzió és az összetett TOE-re alkalmazott CC verzió közötti összes különbséget. Ha a verziók különböznek, az értékelő mérje fel, hogy a verziók közötti különbségek ellentmondó nyilatkozatot eredményeznek-e.

Összetett TOE esetén minden olyan példány esetén, ahol a kiszolgáló TOE-ra és a kliens TOE-ra vonatkozó CC megfelelőségi nyilatkozat a CC nagyon eltérő verzióira vonatkozik (például egyik komponens TOE megfelelőségi nyilatkozata CC v2.x, míg egy másik TOE összetevőé CC v3.x), akkor az összetett TOE megfelelőségi nyilatkozata a CC korábbi verziójához való megfelelést fog állítani, mivel a CC-t azzal a céllal fejlesztették, hogy visszafelé kompatibilis legyen (bár ez a legszigorúbb értelemben nem teljesülhet, de elvileg igen).

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.

Összetett TOE esetén az értékelő nézze meg, hogy a nyilatkozat összhangban van-e nem csak a CC 2. részével, hanem a CC 2. részére vonatkozó megfelelőségi nyilatkozatokkal is, minden komponens TOE-ra. Azaz, ha egy vagy több komponens TOE CC 2. rész kiterjesztést állít, akkor az összetett TOE-nak szintén CC 2. rész kiterjesztettnek kell lennie.

Összetett TOE esetén az összetett TOE-ra vonatkozó CC megfelelőségi nyilatkozat lehet CC 2. rész kiterjesztett, akkor is, ha a komponens TOE-k megfelelnek a CC 2. részének. (Ez abban az esetben lehetséges, ha a kiszolgáló TOE-ra további, kiterjesztett SFR-eket állítanak.)

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.

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.

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).

Összetett TOE esetén az értékelőnek nem szabad figyelmen kívül hagynia, hogy PP-nek való részleges megfelelés nem megengedett. Ezért összetett TOE-ra csak egy összetett megoldást megkövetelő PP-nek való megfelelést lehet állítani egy ST-ben. Ilyen PP-nek való megfelelést nem állíthattak tehát a komponens TOE-k értékelése során, mivel ezek a komponensek nem elégítették volna ki az összetett megoldást. Ez tehát csak olyan esetekben lehetséges, amikor az "összetett" PP megengedi az összetételek értékelése megközelítést (ACO összetevők használata).

Összetett TOE esetén az ST azonosítsa a komponens TOE-k ST-it, melyekből az összetett ST áll. Az összetett TOE lényegileg a komponens TOE-k ST-inek való megfelelést állít.

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).

Összetett TOE esetén az értékelő állapítsa meg, hogy az összetett TOE-t alkotó komponens TOE-k ST-it egyértelműen azonosították.

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.

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.

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).

Összetett TOE esetén az értékelő állapítsa meg, hogy a megfelelőségi nyilatkozat indoklása megmutatja-e azt, hogy a komponens TOE-k TOE típusai összhangban vannak az összetett TOE típusával. Ez nem jelenti azt, hogy az összetett és a komponens TOE típusoknak meg kell egyezniük, de a komponens TOE-knak alkalmasnak kell lenniük az összetett TOE-hez való integrálásra. Az összetett TOE ST-jében egyértelművé kell tenni, hogy melyik SFR-k az összeállítás eredményei, és hogy nem vizsgálták azokat SFR-ként a kiszolgáló és kliens komponens TOE-k (pl. EALx) értékelése során.

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 megegyezik a megfelelőség alapjául szolgáló PP-ben szereplő biztonsági probléma meghatározással, vagy szigorúbb annál.

Összetett TOE esetén az értékelőnek meg kell néznie, hogy az összetett TOE biztonsági probléma meghatározása összhangban van-e a komponens TOE-k ST-iben specifikáltakkal. Az összhangot a kimutatható megfelelés szerint kell értelmezni. Az értékelő a megfelelőségi nyilatkozatot különösen az alábbiak megállapítása érdekében vizsgálja meg:

a) Az összetett TOE ST-ben szereplő fenyegetések és szervezeti biztonsági szabályzatok nem mondanak ellent a komponens ST-kben szereplőknek.;
b) A komponens ST-kben leírt feltételezések fennállnak az összetett TOE ST-ben. Azaz, vagy a feltételezésnek kell szerepelnie az összetett TOE-ban, vagy a feltételezést pozitív módon kezelni kell az összetett ST-ben. A feltételezés pozitívan kezelhető az összetett TOE-ban követelmények meghatározásával a feltételezésben megcélzott szempont teljesítését biztosító funkcionalitás biztosításával.

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 működési környezetre vonatkozó biztonsági célt (a következő pontban részletezett kivételtől eltekintve). Megjegyzés: megengedett, hogy az értékelés alatt álló ST további biztonsági célokat tartalmazzon a működési környezetre;
c) Az ST megszabhatja, hogy a megfelelés alapjául szolgáló PP működési 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 megegyezik-e a megfelelés alapját adó PP-ben szereplő biztonsági célok nyilatkozatával, vagy szigorúbb annál.

Összetett TOE esetén az értékelőnek figyelembe kell vennie, hogy az összetett TOE biztonsági céljai összhangban vannak-e a komponens TOE-k ST-iben specifikáltakkal. Az összhangot a kimutatható megfelelés szerint kell értelmezni. Az értékelő a megfelelőségi nyilatkozatot különösen az alábbiak megállapítása érdekében vizsgálja meg:

a) A kliens TOE ST-jében szereplő egyetlen működési környezetben releváns IT vonatkozású biztonsági cél sem mond ellent a kiszolgáló TOE ST-jében szereplő

biztonsági céloknak. Az nem elvárás, hogy a kliens TOE ST-jén belül a környezeti biztonsági célok nyilatkozata lefedje a kiszolgáló TOE ST-jében található TOE biztonsági célok minden szempontját.

b) Az összetett ST-ben lévő biztonsági célok nyilatkozata nem mond ellent a komponens TOE-k ST-iben szereplő biztonsági célok nyilatkozatának.

Amennyiben a PP kimutatható megfelelést követel meg, az értékelő vizsgálja meg a megfelelőségi nyilatkozat indoklását annak megállapítása érdekében, hogy az megmutatja-e, hogy az ST-ben szereplő biztonsági célok nyilatkozata tartalmazza a PP-ben lévő összes biztonsági célt.

Összetett TOE esetén, amennyiben a PP kimutatható megfelelést követel meg, az értékelő vizsgálja meg a megfelelőségi nyilatkozat indoklását annak megállapítása érdekében, hogy az megmutatja-e, hogy az összetett TOE ST-ben szereplő biztonsági célok nyilatkozata legalább megegyezik a komponens TOE ST-kben szereplőkkel.

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 megegyezik-e a megfelelés alapjául szolgáló PP-ben lévő biztonsági követelményekkel, vagy még korlátozóbb annál.

Összetett TOE esetén az értékelőnek figyelembe kell vennie, hogy az összetett TOE biztonsági követelményei összhangban vannak-e a komponens TOE-k ST-iben specifikáltakkal. Az összhangot a kimutatható megfelelés szerint kell értelmezni. Az értékelő a megfelelőségi nyilatkozatot különösen az alábbiak megállapítása érdekében vizsgálja meg:

a) A kliens TOE ST-jében szereplő egyetlen működési környezetben releváns IT vonatkozású biztonsági követelmény sem mond ellent a kiszolgáló TOE ST-jében szereplő biztonsági követelményeknek. Az nem elvárás, hogy a kliens TOE ST-jén belül a környezeti biztonsági követelményekről szóló nyilatkozata lefedje a kiszolgáló TOE ST-jében található TOE biztonsági célok minden aspektusát, mivel

néhány SFR-t valószínűleg hozzá kell adni az összetett TOE ST biztonsági követelményeihez. A kiszolgáló TOE-ben lévő biztonsági követelményekről szóló nyilatkozatának azonban támogatnia kell a kliens komponens működését.

b) A kliens TOE ST-jében szereplő egyetlen működési környezetben releváns IT vonatkozású biztonsági cél sem mond ellent a kiszolgáló TOE ST-jében szereplő biztonsági követelményeknek. Az nem elvárás, hogy a kliens TOE ST-jén belül a környezeti biztonsági célok nyilatkozata lefedje a kiszolgáló TOE ST-jében található TOE biztonsági követelmények minden szempontját.

c) Az összetett TOE-ban a biztonsági követelményekről szóló nyilatkozatának összhangban kell lennie a komponens TOE-kre vonatkozó ST-k biztonsági követelményeivel.

Amennyiben a PP kimutatható megfelelést követel meg, az értékelő vizsgálja meg a megfelelőségi nyilatkozat indoklását annak megállapítása érdekében, hogy az megmutatja-e, hogy az ST-ben szereplő biztonsági követelményekről szóló nyilatkozata legalább megegyezik a PP-ben lévő biztonsági célokkal.

Összetett TOE esetén, amennyiben a PP kimutatható megfelelést követel meg, az értékelő vizsgálja meg a megfelelőségi nyilatkozat indoklását annak megállapítása érdekében, hogy az megmutatja-e, hogy az összetett ST-ben szereplő biztonsági követelményekről szóló nyilatkozat legalább megegyezik a komponens TOE-k ST-iben lévőkkel.

6.2.1.1.3. A biztonsági probléma meghatározás (ASE_SPD.1) értékelése

Alap összetett garanciacsomag esetén a (csökkentett garanciájú) ST nem tartalmaz biztonsági probléma meghatározást.

Következésképpen nem tartozik ehhez értékelői altevékenység sem.

6.2.1.1.4. A biztonsági célok (ASE_OBJ.1) értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a működési környezetre vonatkozó biztonsági célokat világosan meghatározták.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST.

6.2.1.1.4.1. Az ASE_OBJ.1.1E értékelői akció

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

ASE_OBJ.1.1C A biztonsági célokról szóló nyilatkozatnak le kell írnia a működési környezetre vonatkozó biztonsági célokat.

ASE_OBJ.1-1 Az értékelőnek ellenőriznie kell, hogy a biztonsági célokról szóló nyilatkozat megadja-e a működési környezetre vonatkozó biztonsági célokat.

Az értékelő ellenőrizze, hogy azonosították-e a működési környezetre vonatkozó biztonsági célokat.

6.2.1.1.5. 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.

6.2.1.1.5.1. 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 vagy 3. rész meglévő családjának tagja, vagy
b) az ST-ben meghatározott új család tagja.

Amennyiben a kiterjesztett összetevő egy CC 2. vagy 3. 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. vagy 3. részbeli meglévő osztály tagja, vagy
b) az ST-ben meghatározott új osztály tagja.

Amennyiben a család egy CC 2. vagy 3. 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 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 7.1.3 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 CC 1. rész 8. (Műveletek) szakaszával.

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 7.2.1 (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 7.1.2 (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 7.1.1 (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.

Ha az ST nem tartalmaz kiterjesztett SAR-t, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy a kiterjesztett garanciális összetevő meghatározás összhangban van-e a CC 3. rész 7.1.3 (A garanciális összetevők szerkezete) szakaszban írtakkal.

Amennyiben a kiterjesztett garanciális összetevőben műveleteket alkalmaztak, az értékelő állapítsa meg, hogy a kiterjesztett garanciális összetevő összhangban van-e a CC 1. rész 8. (Műveletek) szakaszával.

Amennyiben a kiterjesztett garanciális összetevő hierarchia szerint alárendelt egy meglévő garanciális összetevőnek, akkor az értékelő állapítsa meg, hogy a kiterjesztett garanciális összetevő összhangban van-e a CC 3. rész 7.1.3 (Garanciális összetevők szerkezete) szakaszával.

ASE_ECD.1-9 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden kiterjesztett garanciális összetevőhöz biztosítottak alkalmazható módszertant.

Ha az ST nem tartalmaz kiterjesztett SAR-t, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő minden kiterjesztett SAR esetén minden értékelői feladatelemre, állapítsa meg, hogy létezik-e hozzá egy vagy több munkaegység, és hogy az összes munkaegység sikeres végrehajtása egy adott értékelői feladatelemre megmutatja-e, hogy az abban foglaltak teljesültek.

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.

Amennyiben az ST nem határoz meg új garanciális családot, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy az összes meghatározott új garanciális család megfelel-e a CC 3. rész 7.1.2 (A garanciális családok szerkezete) szakaszban foglaltaknak.

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.

Amennyiben az ST nem határoz meg új garanciális családot, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy az összes meghatározott új garanciális osztály megfelel a CC 3. rész 7.1.1 (A garanciális osztályok szerkezete) szakaszban foglaltaknak.

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.

Amennyiben az ST nem tartalmaz kiterjesztett biztonsági követelményt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy a kiterjesztett funkcionális összetevők elemeit oly módon fogalmazták meg, hogy azok tesztelhetők, és visszakövethetők a megfelelő TSF reprezentációkon keresztül.

Az értékelő azt is határozza meg, hogy a kiterjesztet garanciális összetevők elemei kivédik a szubjektív értékelői döntés szükségességét.

Az értékelőnek szem előtt kell tartania, hogy miközben minden értékelői kritérium ismérve a mérhetőség és objektivitás, ennek ellenére nem létezik formális módszer az ilyen tulajdonságok bizonyítására. Ezért a meglévő CC funkcionális és garanciális összetevőket kell használni annak meghatározási modelljeként, hogy mi képezi a megfelelőség alapját e követelményben.

6.2.1.1.5.2. 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. és 3. 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.

6.2.1.1.6. A biztonsági követelmények (ASE_REQ.1) értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy az SFR-k és SAR-k világosak, egyértelműek, jól meghatározottak és belső ellentmondásoktól mentesek.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST.

6.2.1.1.6.1. Az ASE_REQ.1.1E 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.1.1C A biztonsági követelményekről szóló nyilatkozatnak le kell írnia az SFR-ket és az SAR-kat.

ASE_REQ.1-1 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 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 SFR azonosítása ugyanolyan módszerrel történjen.

ASE_REQ.1-2 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.1.2C Az SFR-ekben és SAR-ekben használt minden szubjektumot, objektumot, műveletet, biztonsági tulajdonságot, külső egyedet és egyéb terminológiai egységet meg kell határozni.

ASE_REQ.1-3 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 Közös Szempontok (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.1.3C A biztonsági követelményekről szóló nyilatkozatnak azonosítania kell a biztonsági követelményekben szereplő összes műveletet.

ASE_REQ.1-4 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 vagy SAR-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.1.4C Minden műveletet pontosan és helyesen kell végrehajtani.

ASE_REQ.1-5 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: CC 1. rész, 8. (Műveletek) alatt.

ASE_REQ.1-6 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: CC 1. rész, 8. (Műveletek) alatt.

ASE_REQ.1-7 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: CC 1. rész, 8. (Műveletek) alatt.

ASE_REQ.1-8 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: CC 1. rész, 8. (Műveletek) alatt.

ASE_REQ.1.5C A biztonsági követelmények minden függési viszonyát vagy teljesíteni kell, vagy a biztonsági követelmények indoklásának igazolnia kell a függés nem teljesítését.

ASE_REQ.1-9 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 nyilatkozatába. 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 működési környezete teljesíti; ekkor az igazolásnak le kell írnia, hogy a működési környezetre vonatkozó biztonsági célok hogyan elégítik ki ezt a függést.

ASE_REQ.1.6C A biztonsági követelményekről szóló nyilatkozatnak belső ellentmondásoktól mentesnek kell lennie.

ASE_REQ.1-10 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) olyan kiterjesztett SAR, amely azt specifikálja, hogy egy adott kriptográfiai algoritmus tervét titokban kell tartani, és egy másik kiterjesztett garanciális követelmény nyílt forrás átnézését követeli meg;
b) 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;
c) 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;
d) 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.

6.2.1.1.7. A TOE összefoglaló előírás (ASE_TSS.1) értékelése

Ezen altevékenység célja annak megállapítása, hogy a TOE összefoglaló előírás foglalkozik-e az összes SFR-rel, valamint összhangban van-e a TOE egyéb leíró részeivel.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST.

6.2.1.1.7.1. Az ASE_TSS.1.1E értékelői akció

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

ASE_TSS.1.1C A TOE összefoglaló előírásnak le kell írnia, hogy a TOE hogyan teljesíti az egyes SFR-eket.

ASE_TSS.1-1 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.

Egy összetett TOE-ra az értékelő azt is állapítsa meg, hogy egyértelmű-e, hogy melyik komponens gondoskodik az egyes SFR-ekről, vagy az egyes SFR-ek teljesítéséhez a komponensek milyen együttesére van szükség.

6.2.1.1.7.2. Az ASE_TSS.1.2E értékelői akció

ASE_TSS.1.2E 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.1-2 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.

6.2.1.2. Biztonsági előirányzat értékelése CAP-F esetén

6.2.1.2.1. 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.

6.2.1.2.1.1. 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.

Olyan értékelésekben, melyek CM rendszert is használnak, az értékelő érvényesítheti a hivatkozások egyediségét a konfiguráció lista ellenőrzésével. Más esetekben, az ST-nek kell valamilyen hivatkozási módszert alkalmaznia, ami képes az egyedi hivatkozások támogatására (pl. számozás, betűk vagy dátumok használata).

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.

Összetett TOE esetén az ST-ben szereplő TOE áttekintésnek az összetett TOE használatát és fő biztonsági tulajdonságait kell leírnia, nem pedig az összetett TOE egyes elemeire vonatkozó információkat.

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 működtetési 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 nem-TOE 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 nem-TOE 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.

Összetett TOE esetén az ST hivatkozhat az összetevő TOE-k logikai határainak leírására, melyek az alkotó TOE-k ST-iben szerepelnek, és az összetett TOE leírásának nagy részét képezik. Azonban az értékelőnek meg kell állapítania, hogy az összetett TOE ST-je egyértelműen leírja-e, hogy az egyedi komponensek melyik szolgáltatása nem tartozik az összetett TOE-ba, következésképp nem jelenik meg az összetett TOE-ban sem tulajdonságként.

6.2.1.2.1.2. 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.

6.2.1.2.2. 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.

6.2.1.2.2.1. 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.

Összetett TOE esetén az értékelő vegye figyelembe az egyes összetevőknél használt CC verzió és az összetett TOE-re alkalmazott CC verzió közötti összes különbséget. Ha a verziók különböznek, az értékelő mérje fel, hogy a verziók közötti különbségek ellentmondó nyilatkozatot eredményeznek-e.

Összetett TOE esetén minden olyan példány esetén, ahol a kiszolgáló TOE-ra és a kliens TOE-ra vonatkozó CC megfelelőségi nyilatkozat a CC nagyon eltérő verzióira vonatkozik (például egyik komponens TOE megfelelőségi nyilatkozata CC v2.x, míg egy másik TOE összetevőé CC v3.x), akkor az összetett TOE megfelelőségi nyilatkozata a CC korábbi verziójához való megfelelést fog állítani, mivel a CC-t azzal a céllal fejlesztették, hogy visszafelé kompatibilis legyen (bár ez a legszigorúbb értelemben nem teljesülhet, de elvileg igen).

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.

Összetett TOE esetén az értékelő nézze meg, hogy a nyilatkozat összhangban van-e nem csak a CC 2. részével, hanem a CC 2. részére vonatkozó megfelelőségi nyilatkozatokkal is, minden komponens TOE-ra. Azaz, ha egy vagy több komponens TOE CC 2. rész kiterjesztést állít, akkor az összetett TOE-nak szintén CC 2. rész kiterjesztettnek kell lennie.

Összetett TOE esetén az összetett TOE-ra vonatkozó CC megfelelőségi nyilatkozat lehet CC 2. rész kiterjesztett, akkor is, ha a komponens TOE-k megfelelnek a CC 2. részének. (Ez abban az esetben lehetséges, ha a kiszolgáló TOE-ra további, kiterjesztett SFR-eket állítanak.)

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.

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.

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).

Összetett TOE esetén az értékelőnek nem szabad figyelmen kívül hagynia, hogy PP-nek való részleges megfelelés nem megengedett. Ezért összetett TOE-ra csak egy összetett megoldást megkövetelő PP-nek való megfelelést lehet állítani egy ST-ben. Ilyen PP-nek való megfelelést nem állíthattak tehát a komponens TOE-k értékelése során, mivel ezek a komponensek nem elégítették volna ki az összetett megoldást. Ez tehát csak olyan esetekben lehetséges, amikor

az "összetett" PP megengedi az összetételek értékelése megközelítést (ACO összetevők használata).

Összetett TOE esetén az ST azonosítsa a komponens TOE-k ST-it, melyekből az összetett ST áll. Az összetett TOE lényegileg a komponens TOE-k ST-inek való megfelelést állít.

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).
Összetett TOE esetén az értékelő állapítsa meg, hogy az összetett TOE-t alkotó komponens TOE-k ST-it egyértelműen azonosították.

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.

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.

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).

Összetett TOE esetén az értékelő állapítsa meg, hogy a megfelelőségi nyilatkozat indoklása megmutatja-e azt, hogy a komponens TOE-k TOE típusai összhangban vannak az összetett TOE típusával. Ez nem jelenti azt, hogy az összetett és a komponens TOE típusoknak meg kell egyezniük, de a komponens TOE-knak alkalmasnak kell lenniük az összetett TOE-hez való integrálásra. Az összetett TOE ST-jében egyértelművé kell tenni, hogy melyik SFR-k az összeállítás eredményei, és hogy nem vizsgálták azokat SFR-ként a kiszolgáló és kliens komponens TOE-k (pl. EALx) értékelése során.

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 megegyezik a megfelelőség alapjául szolgáló PP-ben szereplő biztonsági probléma meghatározással, vagy szigorúbb annál.

Összetett TOE esetén az értékelőnek meg kell néznie, hogy az összetett TOE biztonsági probléma meghatározása összhangban van-e a komponens TOE-k ST-iben specifikáltakkal. Az összhangot a kimutatható megfelelés szerint kell értelmezni. Az értékelő a megfelelőségi nyilatkozatot különösen az alábbiak megállapítása érdekében vizsgálja meg:

a) Az összetett TOE ST-ben szereplő fenyegetések és szervezeti biztonsági szabályzatok nem mondanak ellent a komponens ST-kben szereplőknek.;
b) A komponens ST-kben leírt feltételezések fennállnak az összetett TOE ST-ben. Azaz, vagy a feltételezésnek kell szerepelnie az összetett TOE-ban, vagy a feltételezést pozitív módon kezelni kell az összetett ST-ben. A feltételezés pozitívan kezelhető az összetett TOE-ban követelmények meghatározásával a feltételezésben megcélzott szempont teljesítését biztosító funkcionalitás biztosításával.

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 működési környezetre vonatkozó biztonsági célt (a következő pontban részletezett kivételtől eltekintve). Megjegyzés: megengedett, hogy az értékelés alatt álló ST további biztonsági célokat tartalmazzon a működési környezetre;
c) Az ST megszabhatja, hogy a megfelelés alapjául szolgáló PP működési 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 megegyezik-e a megfelelés alapját adó PP-ben szereplő biztonsági célok nyilatkozatával, vagy szigorúbb annál.

Összetett TOE esetén az értékelőnek figyelembe kell vennie, hogy az összetett TOE biztonsági céljai összhangban vannak-e a komponens TOE-k ST-iben specifikáltakkal. Az

összhangot a kimutatható megfelelés szerint kell értelmezni. Az értékelő a megfelelőségi nyilatkozatot különösen az alábbiak megállapítása érdekében vizsgálja meg:

a) A kliens TOE ST-jében szereplő egyetlen működési környezetben releváns IT vonatkozású biztonsági cél sem mond ellent a kiszolgáló TOE ST-jében szereplő biztonsági céloknak. Az nem elvárás, hogy a kliens TOE ST-jén belül a környezeti biztonsági célok nyilatkozata lefedje a kiszolgáló TOE ST-jében található TOE biztonsági célok minden szempontját.

b) Az összetett ST-ben lévő biztonsági célok nyilatkozata nem mond ellent a komponens TOE-k ST-iben szereplő biztonsági célok nyilatkozatának.

Amennyiben a PP kimutatható megfelelést követel meg, az értékelő vizsgálja meg a megfelelőségi nyilatkozat indoklását annak megállapítása érdekében, hogy az megmutatja-e, hogy az ST-ben szereplő biztonsági célok nyilatkozata tartalmazza a PP-ben lévő összes biztonsági célt.

Összetett TOE esetén, amennyiben a PP kimutatható megfelelést követel meg, az értékelő vizsgálja meg a megfelelőségi nyilatkozat indoklását annak megállapítása érdekében, hogy az megmutatja-e, hogy az összetett TOE ST-ben szereplő biztonsági célok nyilatkozata legalább megegyezik a komponens TOE ST-kben szereplőkkel.

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 megegyezik-e a megfelelés alapjául szolgáló PP-ben lévő biztonsági követelményekkel, vagy még korlátozóbb annál.

Összetett TOE esetén az értékelőnek figyelembe kell vennie, hogy az összetett TOE biztonsági követelményei összhangban vannak-e a komponens TOE-k ST-iben specifikáltakkal. Az összhangot a kimutatható megfelelés szerint kell értelmezni. Az értékelő a megfelelőségi nyilatkozatot különösen az alábbiak megállapítása érdekében vizsgálja meg:

a) A kliens TOE ST-jében szereplő egyetlen működési környezetben releváns IT vonatkozású biztonsági követelmény sem mond ellent a kiszolgáló TOE ST-jében szereplő biztonsági követelményeknek. Az nem elvárás, hogy a kliens TOE ST-jén belül a környezeti biztonsági követelményekről szóló nyilatkozata lefedje a kiszolgáló TOE ST-jében található TOE biztonsági célok minden aspektusát, mivel néhány SFR-t valószínűleg hozzá kell adni az összetett TOE ST biztonsági követelményeihez. A kiszolgáló TOE-ben lévő biztonsági követelményekről szóló nyilatkozatának azonban támogatnia kell a kliens komponens működését.

b) A kliens TOE ST-jében szereplő egyetlen működési környezetben releváns IT vonatkozású biztonsági cél sem mond ellent a kiszolgáló TOE ST-jében szereplő biztonsági követelményeknek. Az nem elvárás, hogy a kliens TOE ST-jén belül a környezeti biztonsági célok nyilatkozata lefedje a kiszolgáló TOE ST-jében található TOE biztonsági követelmények minden szempontját.

c) Az összetett TOE-ban a biztonsági követelményekről szóló nyilatkozatának összhangban kell lennie a komponens TOE-kre vonatkozó ST-k biztonsági követelményeivel.

Amennyiben a PP kimutatható megfelelést követel meg, az értékelő vizsgálja meg a megfelelőségi nyilatkozat indoklását annak megállapítása érdekében, hogy az megmutatja-e, hogy az ST-ben szereplő biztonsági követelményekről szóló nyilatkozata legalább megegyezik a PP-ben lévő biztonsági célokkal.

Összetett TOE esetén, amennyiben a PP kimutatható megfelelést követel meg, az értékelő vizsgálja meg a megfelelőségi nyilatkozat indoklását annak megállapítása érdekében, hogy az megmutatja-e, hogy az összetett ST-ben szereplő biztonsági követelményekről szóló nyilatkozat legalább megegyezik a komponens TOE-k ST-iben lévőkkel.

6.2.1.2.3. A biztonsági probléma meghatározás (ASE_SPD.1) értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a TOE-ra és működési környezetére vonatkozó biztonsági problémát világosan meghatározták.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST.

6.2.1.2.3.1. 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 működési 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 működési 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 működési 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 működési környezetére vonatkozó feltételezéseket.

Amennyiben nincsenek feltételezések, ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekintendő.

Az értékelő állapítsa meg, hogy a TOE működési környezetére vonatkozó minden feltételezést kellő részletességgel megmagyaráztak ahhoz, hogy a vásárlók ebből meg tudják állapítani, vajon az ő működési környezetük megfelel-e a feltételezésnek. Amennyiben a feltételezések nem eléggé világosak, akkor a vásárlók olyan működési környezetben is alkalmazhatják a TOE-t, amelyben az nem biztonságos módon működik.

6.2.1.2.4. 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 működtetési környezet közötti megosztását.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST.

6.2.1.2.4.1. 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 a működési környezetre vonatkozó biztonsági célokat.

ASE_OBJ.2-1 Az értékelőnek ellenőriznie kell, hogy a biztonsági célokról szóló nyilatkozat megadja-e a TOE-ra, valamint a működési 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 működési 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 működési 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 működési 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 működési 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 a működési 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 működési környezetre vonatkozó feltételezésre tartalmaz-e megfelelő igazolást arra, hogy a működési környezetre vonatkozó biztonsági célok alkalmasak az adott feltételezés alátámasztására.

Amennyiben nincsenek a feltételezésre visszavezethető, működési környezetre vonatkozó biztonsági célok, e munkaegység „Nem felelt meg” eredményt ad.

Az értékelő állapítsa meg, hogy egy a TOE működési környezetével kapcsolatos feltételezésre vonatkozó indoklás szemlélteti-e a biztonsági célok elégségességét: ha egy adott feltételezésre visszavezetett összes működési környezetre vonatkozó biztonsági cél teljesül, akkor a működési környezet alátámasztja az adott feltételezést.

Az értékelő azt is állapítsa meg, hogy egy feltételezésre visszavezetett, a TOE működési környezetére vonatkozó összes biztonsági cél szükséges: ha a biztonsági cél teljesül, akkor az ténylegesen hozzájárul ahhoz, hogy a működési környezet az adott feltételezést alátámassza.

Megjegyzendő, hogy a működési 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 működési 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”.

6.2.1.2.5. 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.

6.2.1.2.5.1. 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 vagy 3. rész meglévő családjának tagja, vagy
b) az ST-ben meghatározott új család tagja.

Amennyiben a kiterjesztett összetevő egy CC 2. vagy 3. 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. vagy 3. részbeli meglévő osztály tagja, vagy
b) az ST-ben meghatározott új osztály tagja.

Amennyiben a család egy CC 2. vagy 3. 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 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 7.1.3 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 CC 1. rész 8. (Műveletek) szakaszával.

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 7.2.1 (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 7.1.2 (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 7.1.1 (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.

Ha az ST nem tartalmaz kiterjesztett SAR-t, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy a kiterjesztett garanciális összetevő meghatározás összhangban van-e a CC 3. rész 7.1.3 (A garanciális összetevők szerkezete) szakaszban írtakkal.

Amennyiben a kiterjesztett garanciális összetevőben műveleteket alkalmaztak, az értékelő állapítsa meg, hogy a kiterjesztett garanciális összetevő összhangban van-e a CC 1. rész 8. (Műveletek) szakaszával.

Amennyiben a kiterjesztett garanciális összetevő hierarchia szerint alárendelt egy meglévő garanciális összetevőnek, akkor az értékelő állapítsa meg, hogy a kiterjesztett garanciális összetevő összhangban van-e a CC 3. rész 7.1.3 (Garanciális összetevők szerkezete) szakaszával.

ASE_ECD.1-9 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden kiterjesztett garanciális összetevőhöz biztosítottak alkalmazható módszertant.

Ha az ST nem tartalmaz kiterjesztett SAR-t, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő minden kiterjesztett SAR esetén minden értékelői feladatelemre, állapítsa meg, hogy létezik-e hozzá egy vagy több munkaegység, és hogy az összes munkaegység sikeres végrehajtása egy adott értékelői feladatelemre megmutatja-e, hogy az abban foglaltak teljesültek.

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.

Amennyiben az ST nem határoz meg új garanciális családot, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy az összes meghatározott új garanciális család megfelel-e a CC 3. rész 7.1.2 (A garanciális családok szerkezete) szakaszban foglaltaknak.

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.

Amennyiben az ST nem határoz meg új garanciális családot, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy az összes meghatározott új garanciális osztály megfelel a CC 3. rész 7.1.1 (A garanciális osztályok szerkezete) szakaszban foglaltaknak.

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.

Amennyiben az ST nem tartalmaz kiterjesztett biztonsági követelményt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy a kiterjesztett funkcionális összetevők elemeit oly módon fogalmazták meg, hogy azok tesztelhetők, és visszakövethetők a megfelelő TSF reprezentációkon keresztül.

Az értékelő azt is határozza meg, hogy a kiterjesztet garanciális összetevők elemei kivédik a szubjektív értékelői döntés szükségességét.

Az értékelőnek szem előtt kell tartania, hogy miközben minden értékelői kritérium ismérve a mérhetőség és objektivitás, ennek ellenére nem létezik formális módszer az ilyen tulajdonságok bizonyítására. Ezért a meglévő CC funkcionális és garanciális összetevőket kell használni annak meghatározási modelljeként, hogy mi képezi a megfelelőség alapját e követelményben.

6.2.1.2.5.2. 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. és 3. 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.

6.2.1.2.6. 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.

6.2.1.2.6.1. Az ASE_REQ.2.1E értékelői akció

ASE_REQ.2.1E 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 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 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 Közös Szempontok (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 vagy SAR-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: CC 1. rész, 8. (Műveletek) alatt.

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: CC 1. rész, 8. (Műveletek) alatt.

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: CC 1. rész, 8. (Műveletek) alatt.

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: CC 1. rész, 8. (Műveletek) alatt.

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 működési környezete teljesíti; ekkor az igazolásnak le kell írnia, hogy a működési 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 egy [3]-beli AVA_VAN 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) olyan kiterjesztett SAR, amely azt specifikálja, hogy egy adott kriptográfiai algoritmus tervét titokban kell tartani, és egy másik kiterjesztett garanciális követelmény nyílt forrás átnézését követeli meg;
b) 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;
c) 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;
d) 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.

6.2.1.2.7. 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 beavatkozással, a logikai meghamisítással és a biztonsági funkciók megkerülésével, valamint összhangban van-e a TOE egyéb leíró részeivel.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) ST.

6.2.1.2.7.1. 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.

Egy összetett TOE esetén az értékelő azt is állapítsa meg, hogy egyértelmű-e, hogy melyik komponens gondoskodik az egyes SFR-ekről, vagy az egyes SFR-ek teljesítéséhez a komponensek milyen együttesére van szükség.

ASE_TSS.2.2C A TOE összefoglaló előírásnak le kell írnia, hogy a TOE hogyan védi meg magát a beavatkozás és a logikai meghamisítás 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 beavatkozás és a logikai meghamisítás 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 beavatkozás és a logikai meghamisítás ellen, ezért a leírásnak nem kell túlzottan részletesnek lennie.

Egy összetett TOE esetén az értékelő azt is állapítsa meg, hogy egyértelmű-e, hogy melyik komponens biztosítja a védelmet, vagy a komponensek milyen együttese biztosítja azt.

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.

Egy összetett TOE esetén az értékelő azt is állapítsa meg, hogy egyértelmű-e, hogy melyik komponens biztosítja a védelmet, vagy a komponensek milyen együttese biztosítja azt.

6.2.1.2.7.2. 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.

6.2.1.3. Biztonsági előirányzat értékelése CAP-K esetén

Az kiemelt összetett garanciacsomag (CAP-K) biztonsági előirányzatra vonatkozó elvárásai megegyeznek az fokozott összetett garanciacsomag (CAP-F) megfelelő elvárásaival.

Következésképpen e két garanciacsomag esetén a biztonsági előirányzat értékelői feladatai is megegyeznek. Lásd 6.2.1.2 alfejezetet.

6.2.2. Összetett TOE értékelése CAP-A esetén

6.2.2.1. Alap környezetfüggőségi információ (ACO_REL.1) értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztői környezetfüggőségi bizonyíték kielégítő információt tartalmaz-e annak meghatározásához, hogy a kiszolgáló komponens biztosítja a szükséges funkcionalitást, illetve e funkciók meghívásának módszeréről. Ez egy magas szintű leírás segítségével fejezhető ki.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az összetett ST,
b) a kliens komponens funkcionális specifikációja,
c) a kliens komponens terve,
d) a kliens komponens architektúra terve,
e) a környezetfüggőségi információ.

Egy olyan kliens komponens, amelynek TSF-je együttműködik a kiszolgáló komponenssel, funkcionalitást vár el a kiszolgáló komponenstől (például távoli hitelesítés, távoli naplóadat tárolás). Ezekben az esetekben a hívott szolgáltatásokat le kell írni azok részére, akik a végfelhasználók számára konfigurálják az összetett TOE-t. E leírási követelmény oka, hogy segíteni kell az összetett TOE integrátorokat annak meghatározásában, hogy a kiszolgáló komponens mely szolgáltatásainak lehet kedvezőtlen (ártalmas) hatása a kliens komponensre, és információk álljanak rendelkezésre, amelyek alapján meg lehet állapítani a komponensek kompatibilitását a fejlesztési bizonyíték (ACO_DEV) család alkalmazása során.

6.2.2.1.1. Az ACO_REL.1.1E értékelői akció

ACO_REL.1.1C A környezetfüggőségi információnak le kell írnia a kiszolgáló komponens azon hardver, szoftver és/vagy förmver elemeinek funkcionalitását, melyre a kliens komponens TSF támaszkodik.

ACO_REL.1-1 Az értékelőnek ellenőriznie kell a környezetfüggőségi információt, annak megállapítása érdekében, hogy szerepel-e benne a kiszolgáló komponens hardverei, förmverei és/vagy szoftverei által nyújtott funkcionalitás leírása, amire a kliens komponens TSF-je épít a működése végrehajtása során.

Az értékelő vizsgálja meg annak a biztonsági funkcionalitásnak a leírását, amit a kliens komponens TSF-je igényel a kiszolgáló komponens hardver, szoftver, förmver elemeitől. A munkaegység fókuszában elsősorban e leírás részletessége álljon, és nem annyira az információ pontosságának ellenőrzése. (Ez utóbbira a következő munkaegység összpontosít).

A kiszolgáló komponens leírásának nem kell részletesebbnek lennie, mint egy komponens TSF leírás részletessége, ahogyan azt a TOE terv (ADV_TDS) megadja.

ACO_REL.1-2 Az értékelőnek meg kell vizsgálnia a környezetfüggőségi információt annak megállapítása érdekében, hogy az pontosan tükrözi-e a kliens komponens működtetési környezetére vonatkozó célokat.

A környezetfüggőségi információ tartalmazza a kliens komponens által használt kiszolgáló komponens biztonsági funkcionalitás leírását. Annak biztosítása érdekében, hogy a környezetfüggőségi információ összhangban legyen a kliens komponens működési környezetére vonatkozó elvárásaival, az értékelő hasonlítsa össze a környezetfüggőségi információt a kliens komponens ST-jében megadott környezeti biztonsági célok nyilatkozatával.

Például ha a környezetfüggőségi információban az szerepel, hogy a kliens komponens TSF-je a kiszolgáló komponens funkcióira épít a naplóadatok tárolása és védelme tekintetében, de egy másik értékelési bizonyíték (pl. a kliens komponens tervdokumentációja) egyértelművé teszi, hogy a kliens komponens TSF-je maga tárolja és védi a naplóadatokat, akkor ez pontatlanságot jelez.

Megjegyzendő, hogy a működtetési környezetre vonatkozó célok tartalmazhatnak nem IT eszközökkel kielégíthető célokat. A kiszolgáló komponenstől elvárt szolgáltatások leírhatók a kliens komponens ST-ben a működési környezetre vonatkozó IT biztonsági célokként, de az nem követelmény, hogy minden ilyen környezetre vonatkozó elvárás szerepeljen a környezetfüggőségi információ között.

ACO_REL.1.2C A környezetfüggőségi információnak le kell írnia minden kapcsolatot, amelyen át a kliens komponens TSF-je szolgáltatásokat kér a kiszolgáló komponenstől.

ACO_REL.1-3 Az értékelőnek meg kell vizsgálnia a környezetfüggőségi információt, annak megállapítása érdekében, hogy leírták-e benne a kliens és a kiszolgáló komponens közötti

összes kölcsönhatást, mely kölcsönhatások révén a kliens komponens TSF-je szolgáltatásokat kér a kiszolgáló komponenstől.

A kliens komponens TSF-je kérhet olyan szolgáltatásokat a kiszolgáló komponenstől, amelyek nem voltak a kiszolgáló komponens TSF-jén belül. (Lásd B.3 függeléket, CC 3. részben: Összetett IT egyedek közötti kölcsönhatások).

A kiszolgáló komponens funkcionalitásával kapcsolatos interfészeket ugyanolyan szinten kell leírni, mint a kliens TSF funkcionalitását, amint azt a „TOE terv" (ADV_TDS.1) biztosítja az alrendszerek között.

A kliens és a kiszolgáló komponens közötti együttműködés leírásának célja annak megmutatása, hogy a kliens komponens TSF-je hogyan alapoz a kiszolgáló komponens szolgáltatásaira a saját biztonsági funkcionalitásának végrehajtása céljából. Ezeket a kölcsönhatásokat nem kell a megvalósítás szintjén jellemezni (pl. rutinok közötti paraméterátadás szintjén), de egy összetevő által használandó adott összetevőhöz meghatározott adatelemeket tartalmaznia kell e leírásnak. A leírásnak segítenie kell az olvasót annak általános megértésében, hogy miért van szükség az interakcióra.

Az interfészek pontossága és teljessége a kiszolgáló komponens által biztosítandó, TSF által kért biztonsági funkcionalitáson alapul, amint azt az ACO_REL.2-1 és ACO_REL.2-2 munkaegységek elemzik. Lehetséges, hogy a korábbi munkaegységekben leírt összes funkcionalitás leképezhető az ebben a munkaegységben azonosított interfészekre, és fordítva. Egy olyan interfész, ami nem tartozik leírt funkcióhoz, szintén pontatlanságot jelez.

ACO_REL.1.3C A környezetfüggőségi információnak le kell írnia, hogy a kliens TSF hogyan védi magát a kiszolgáló komponens beavatkozásával és manipulálásával szemben.

ACO_REL.1-4 Az értékelőnek meg kell vizsgálnia a környezetfüggőségi információt, annak megállapítása érdekében, hogy szerepel-e benne az, hogy a kliens TSF hogyan védi meg magát a kiszolgáló komponenshez köthető beavatkozás és manipulálás ellen.

A beavatkozás és manipulálás elleni védelem módját az ADV_ARC.1-4-hez szükséges részletességgel kell biztosítani.

6.2.2.2. Funkcionális leírás (ACO_DEV.1) értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a kiszolgáló komponens a megfelelő biztonsági funkcionalitást nyújtja-e a kliens komponens számára. Ez a kiszolgáló komponens interfészeinek arra irányuló vizsgálatával állapítható meg, hogy azok összhangban vannak-e a környezetfüggőségi információban specifikált, kliens komponens által igényelt interfészekkel.

A kiszolgáló komponens interfészeinek leírását az ADV_FSP.2 értékelői altevékenységgel összhangban álló részletességgel kell megadni, ugyanakkor az ADV_FSP.2 nem minden szükséges szempontját követeli meg az ACO_DEV.1. Az interfész azonosítása és céljának leírása után az interfész további részleteinek specifikálása nem szükséges, az adódik a kiszolgáló komponens értékeléséből.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az összetett ST,
b) a fejlesztési információ,
c) a környezetfüggőségi információ.

6.2.2.2.1. Az ACO_DEV.1.1E értékelői akció

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

ACO_DEV.1.1C A fejlesztési információnak le kell írnia az összetett TOE-ban használt kiszolgáló komponens minden egyes interfészére azok célját.

ACO_DEV.1-1 Az értékelőnek meg kell vizsgálnia a fejlesztési információt, annak megállapítása érdekében, hogy az leírja-e az egyes interfészek célját.

A kiszolgáló komponens interfészeket biztosít a kliens komponenssel való együttműködéshez a kliens TSF működésének támogatásához. Az egyes interfészek célját ugyanolyan szinten kell leírni, mint a kliens komponens TSF funkcionalitásához szükséges interfészeket, ahogyan azokat a TOE tervben az alrendszerek között meg kell adni (ADV_TDS.1). Ez a leírás teszi lehetővé az olvasó számára annak megismerését, hogy a kiszolgáló komponens hogyan biztosítja a kliens komponens TSF-je által igényelt szolgáltatásokat.

Ez a munkaegység teljesíthető a kiszolgáló komponens TSFI interfészeire vonatkozó funkcionális specifikáció biztosításával.

ACO_DEV.1.2C A fejlesztési információnak ki kell mutatnia az összetett TOE-ban használt, - a kliens komponens TSF-jét támogató- kiszolgáló és kliens komponens interfészek közötti megfeleltetéseket.

ACO_DEV.1-2 Az értékelőnek meg kell vizsgálnia a fejlesztési információt, annak megállapítása érdekében, hogy pontos-e a kiszolgáló komponens interfészei és a kliens komponens által használt interfészek közötti megfeleltetés.

A kiszolgáló komponens interfészei és a kliens komponens által használt interfészek közötti megfeleltetés elvégezhető táblázatos vagy mátrix formában. A kliens komponens által használt interfészeket a környezetfüggőségi információ azonosítja (és a „kliens komponens környezetfüggősége” (ACO_REL) során vizsgálják).

E tevékenység során nem követelmény a kliens komponens által használt interfészek teljes lefedettségének a megállapítása, csak az, hogy a megfeleltetés helyes-e, és a kiszolgáló komponens interfészeit leképezték-e a kliens komponens által hívott interfészekre, ahol ez lehetséges. A lefedettség teljességét a „komponens-összeállítás indoklás” (ACO_COR) tevékenység vizsgálja.

6.2.2.2.2. Az ACO_DEV.1.2E értékelői akció

ACO_DEV.1.2E Az értékelőnek meg kell állapítania, hogy a megadott interfész leírás nem mond-e ellent a kliens komponensre megadott környezetfüggőségi információnak.

ACO_DEV.1-3 Az értékelőnek meg kell vizsgálnia a fejlesztési információt és a környezetfüggőségi információt, annak megállapítása érdekében, hogy az interfészek leírása ellentmondásmentes-e.

E munkaegység értékelői célja annak meghatározása, hogy a kiszolgáló komponens fejlesztési információjában és a kliens komponens környezetfüggőségi információjában leírt interfészek összhangban vannak-e egymással.

6.2.2.3. Komponens-összeállítás indoklás (ACO_COR.1) értékelése

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az összetett ST,
b) a komponens-összeállítás indoklás,
c) a környezetfüggőségi információ,
d) a fejlesztési információ,
e) egyedi azonosító,

6.2.2.3.1. Az ACO_COR.1.1E értékelői akció

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

ACO_COR.1.1C A komponens-összeállítás indoklásnak meg kell mutatnia, hogy a garanciaszint legalább olyan magas, mint amit a kliens komponens elért a kiszolgáló komponens támogató funkciójára, amikor a kiszolgáló komponenst a kliens komponens TSF-jének támogatására konfigurálták.

ACO_COR.1-1 Az értékelőnek meg kell vizsgálnia a komponens-összeállítás indoklást a fejlesztési információkkal és környezetfüggőségi információkkal együtt a kliens komponens által használt olyan interfészek azonosítása céljából, amelyeket a fejlesztési információk nem részleteznek.

E munkaegység elvégzésének célja kettős:

a) annak meghatározása, hogy a kliens komponens által használt mely interfészek esetén alkalmazták a megfelelő garanciális intézkedéseket;
b) annak megállapítása, hogy a kiszolgáló komponens értékelése során használt garanciacsomag ugyanazon, vagy hierarchikusan magasabb garanciális követelményeket tartalmazta, mint amelyeket a kliens komponens értékelése során figyelembe vettek.

Az értékelő felhasználhatja a „fejlesztési bizonyíték” (ACO_DEV) tevékenységek végzése során létrehozott fejlesztési információkban szereplő megfelelőség visszavezetést (pl. ACO_DEV.l-2, ACO_DEV.2-4, ACO_DEV.3-6) a környezetfüggőségi információban azonosított azon interfészek meghatározására, melyeket a fejlesztési információk figyelmen kívül hagytak.

Az értékelőnek rögzítenie kell az SFR-t érvényre juttató interfészeket, melyek a környezetfüggőségi információban szerepelnek, de a fejlesztési információban nem. Ezek jelentik az ACO_COR.1-3 munkaegység bemenetét, a kiszolgáló komponens további garanciát igénylő részeinek azonosítását segítve.

Amennyiben a kiszolgáló és a kliens komponenst is ugyanazon garanciacsomag szerint értékelték, akkor magától értetődő annak meghatározása, hogy a kiszolgáló komponens értékelésen belüli részeinek garanciaszintje legalább olyan magas-e, mint a kliens komponensé. Amennyiben azonban a komponensek értékelésekor alkalmazott garanciacsomagok különböznek, akkor az értékelőnek meg kell állapítania, hogy a kiszolgáló komponensre alkalmazott garanciális követelmények mindegyike hierarchikusan magasabb-e, mint a kliens komponensre alkalmazott garanciális követelmény.

ACO_COR.1-2 Az értékelőnek meg kell vizsgálnia a komponens-összeállítás indoklását annak meghatározásához, hogy azon kiszolgáló komponens interfészekre, melyekre a kliens TSF a működésében hagyatkozik, az interfészt vizsgálták-e a kiszolgáló komponens értékelése során.

Az összetett ST, valamint a kiszolgáló komponensre vonatkozó nyilvános értékelési jelentés (pl. tanúsítási jelentés) és útmutató dokumentumok információkat adnak a kiszolgáló komponens logikai hatóköréről és határairól. Az összetett ST részletekkel szolgál az összetett TOE logikai hatóköréről és határairól, lehetővé téve az értékelő számára annak megállapítását, hogy egy interfész kapcsolódik-e az értékelés hatókörébe tartozó termékrészhez. Az útmutató dokumentáció részletesen leírja az összetett TOE összes interfészének a használatát. Bár az útmutató dokumentáció olyan interfészeket is tárgyalhat, amelyek nem esnek értékelés alá, minden ilyen interfésznek azonosíthatónak kell lennie, vagy az ST-ben szereplő hatókör meghatározásból vagy az értékelt konfigurációt részletező útmutató részekből. A nyilvános értékelési jelentés további szükséges megszorításokat tartalmazhat az összetett TOE használatára.

Ezért a fenti bemenetek kombinációja lehetővé teszi az értékelő számára, hogy megállapítsa, a komponens-összeállítás indoklásban leírt interfész rendelkezik-e a hozzá kapcsolódó garanciákkal, vagy szükség van további garanciára. Az értékelő rögzítse a kiszolgáló komponens azon interfészeit, melyekre szükséges ilyen további garancia, amit az ACO_COR.1-3 során mérlegelnek.

ACO_COR.1-3 Az értékelőnek meg kell vizsgálnia a komponens-összeállítás indoklást annak megállapítása érdekében, hogy a kiszolgáló komponensre alkalmazták-e a szükséges garanciális intézkedéseket.

A kiszolgáló komponensre vonatkozó értékelői döntés és az abból következő garancia újrahasználható, feltéve, ha az összetett TOE-ban a kiszolgáló komponens ugyanazon részeit használják, és következetesen alkalmazzák azokat.

Annak meghatározásához, hogy a komponensre alkalmazták-e már a szükséges garanciális intézkedéseket, és a komponens mely részeire kell még garanciális intézkedéseket alkalmazni, az értékelőnek használnia kell az ACO_DEV.*.2E tevékenység és az ACO_COR.1-1 és ACO_COR.1-2 munkaegység kimenetét:

a) A környezetfüggőségi információban (ACO_REL) azonosított, de a fejlesztési információ (ACO_DEV) között nem elemzett interfészek esetén további információ szükséges (azonosítva ACO_COR.1-1-ben).
b) A kiszolgáló komponens azon interfészei esetén, melyeket nem konzisztens módon használtak az összetett TOE-ban (különbség van a „fejlesztési bizonyíték” (ACO_DEV) és a „kliens komponens környezetfüggősége” (ACO_REL) között), a különbség kihatását meg kell nézni (ACO_DEV.*.2E).
c) További információra van szükség azon interfészek esetén, melyeket a komponens-összeállítás indoklás azonosít és nincs hozzájuk korábban igazolt garancia (azonosítva ACO_COR.1-2-ben).
d) Azon interfészek esetén pedig, melyeket a környezetfüggőségi információ, a komponens-összeállítás indoklás és a fejlesztési információ ellentmondásmentesen írnak le, nincs további teendő, mivel a kiszolgáló komponens értékelési eredményei újrahasználhatók.

A környezetfüggőségi információ által megkövetelt, de a fejlesztési információban nem szereplő kiszolgáló komponens interfészek a kiszolgáló komponens azon elemeit mutatják, ahol további garanciára van szükség. Az interfészek azonosítják a kiszolgáló komponens belépési pontjait.

Azoknál az interfészeknél, melyeket mind a fejlesztési információ, mind a környezetfüggőségi információ tárgyal, az értékelőnek kell megállapítania, hogy az interfészeket az összetett TOE-ban oly módon alkalmazzák-e, ami megfelel a kiszolgáló komponens értékelésének. Az interfész használat módját a „fejlesztési bizonyíték” (ACO_DEV) tevékenység során vizsgálják abból a célból, hogy kiderüljön, az interfész használat megfelel mind a kiszolgáló komponensnek, mind az összetett TOE-nak. A fennmaradó vizsgálat tárgya annak megállapítása, hogy nem mondanak-e ellent egymásnak a kiszolgáló komponens és az összetett TOE konfigurációi. Ennek meghatározásához az értékelő vizsgálja meg a vonatkozó útmutató dokumentációkat, hogy azok ellentmondásmentesek-e (további útmutató a konzisztens dokumentációkról jelen anyag további részeiben olvasható). A dokumentációban talált bármilyen eltérés esetén újabb vizsgálat következik a lehetséges következmények felmérése céljából.

Azon interfészek esetén, melyekre fennáll a környezetfüggőségi és fejlesztési információ ellentmondás-mentessége, és amelyeknél a kiszolgáló komponens és az összetett TOE útmutatója összhangban van egymással, biztosított a megkívánt garancia szintje.

Az alábbi bekezdések támpontot adnak ahhoz, hogyan lehet meghatározni a konzisztenciát a kiszolgáló komponensre érvényes garancia és az összetett TOE-hez adott bizonyíték között,

valamint az értékelő által végrehajtott elemzéshez olyan esetekben, amikor ellentmondásokra derül fény.

6.2.2.3.1.1. Fejlesztés

A környezetfüggőségi információ azonosítja a kliens komponens interfészeit, amiket a kiszolgáló komponenshez kell illeszteni. Ha a környezetfüggőségi információ között azonosított interfész nem szerepel a fejlesztési információ között, akkor a komponens-összeállítás indoklásnak kell gondoskodnia annak bizonyításáról, hogy a kiszolgáló komponens hogyan biztosítja az igényelt interfészt.

Ha a környezetfüggőségi információkban azonosított interfész szerepel a fejlesztési információk között, de ellentmondások lelhetők fel a leírások között, akkor további elemzésre van szükség. Az értékelő beazonosítja a kiszolgáló komponens használatában felmerülő különbségeket a kiszolgáló komponens értékelése és az összetett TOE értékelés alapján. Az értékelő tesztelés végrehajtását állapítja meg (az „összetett TOE tesztelése” (ACO_CTT) végrehajtása során) az interfész tesztelése céljából.

A kiszolgáló és a kliens komponensek összetett TOE-beli javítási állapotát (patch-ek alkalmazását) össze kell vetni a komponens értékelések során fennálló komponens frissítési státuszokkal. Ha bármilyen patch-et alkalmaztak a komponensekre, akkor a komponens-összeállítás indoklásban szerepeltetni kell a javítások információit, ideértve az értékelt komponens SFR-jeire gyakorolt minden lehetséges hatást. Az értékelőnek mérlegelnie kell a megadott módosításokat, és ellenőriznie kell a komponens SFR-ekre gyakorolt lehetséges következmények pontosságát. Az értékelőnek ezután meg kell vizsgálnia, hogy a javítások által bevezetett módosításokat ellenőriznie kell-e teszteléssel, valamint azonosítania kell a szükséges tesztelési módszert. A tesztelés elvégezhető a komponens értékelés során elvégzett megfelelő értékelői/fejlesztői tesztelések megismétlésével, vagy az értékelő elrendelhet új teszteket a módosított komponens helyes működésének ellenőrzésére.

Amennyiben az egyedi komponensek garancia folytonossági tevékenység tárgyát képezték a komponens értékelés befejezése óta eltelt időszakban, az értékelő mérlegelje a garancia folytonosság tevékenység során felmért módosításokat az összetett TOE-ra vonatkozó független sebezhetőségi elemzés során (ACO_VUL).

6.2.2.3.1.2. Útmutatók

Az összetett TOE-ra vonatkozó útmutatók nagy eséllyel hivatkoznak az egyedi komponensek útmutatóira. Az elvárt minimális útmutató, hogy azonosítva legyen a kliens és kiszolgáló komponensek útmutatóinak alkalmazásához a sorrendi függőség, különös tekintettel az összetett TOE előkészületi (telepítési) szakaszára.

Az előkészítő eljárások (AGD_PRE) és „üzemeltetési felhasználói útmutató” (AGD_OPE) családok összetett TOE-ra vonatkozó alkalmazásán kívül vizsgálni kell a komponensek és az összetett TOE útmutatóit ellentmondás-mentesség szempontjából, és jelezni kell minden eltérést.

Ha az összetett TOE útmutató hivatkozik a kiszolgáló és kliens komponensek útmutató dokumentációira, akkor az ellentmondás-mentesség mérlegelése az egyes komponensekhez adott útmutatók közötti konzisztenciára korlátozódik (a kiszolgáló és a kliens komponens útmutatói közötti ellentmondás-mentességre). Ha azonban az összetett TOE-ra további útmutatókat is készítettek, akkor alaposabb elemzésre van szükség, hiszen a komponensekhez készített és az összetett TOE-ra vonatkozó útmutató dokumentációk közötti ellentmondás-mentességet is garantálni kell.

Ekkor az ellentmondás-mentesség azt jelenti, hogy az útmutató vagy ugyanaz, vagy további megszorításokat szab az egyedi komponensekre azok integrálása esetére, hasonló módon a funkcionális/garanciális összetevők pontosítási módjához.

A rendelkezésre álló információk segítségével (melyeket a „fejlesztési bizonyíték” (ACO_DEV) használ bemenetként) az értékelő képes lehet annak megállapítására, hogy a komponens értékelés során specifikált kiszolgáló komponens konfigurációtól való eltérések milyen lehetséges következményekkel járnak. Magas EAL-ok esetén azonban (amikor a kiszolgáló komponens értékelés tartalmazta a „TOE terv” (ADV_TDS) követelményeket) előfordulhat, hogy az útmutató módosításainak lehetséges kihatásai nem határozhatók meg teljes mértékben, - hacsak az összetett TOE-hoz nem bocsátják rendelkezésre a fejlesztési információ részeként a részletes tervezési leírásokat-, mivel a belső részletek nem ismertek. Ekkor az értékelőnek jelentést kell írnia a maradvány kockázatokról.

Ezeket a maradvány kockázatokat szerepeltetni kell az összetett TOE-ről szóló minden nyilvános értékelési jelentésben.

Az értékelőnek rögzítenie kell az útmutatók eltéréseit, ami az értékelő független tesztelési tevékenység („összetett TOE tesztelése”, ACO_CTT) bemenete lesz.

Az összetett TOE útmutatója kiegészítheti a komponensek útmutatóit, elsősorban a telepítésre, illetve a kiszolgáló és kliens komponens telepítési lépéseinek egymáshoz viszonyított végrehajtási sorrendjére vonatkozóan. Az egyedi komponensekre nézve a telepítési lépések sorrendje nem módosulhat, azonban előfordulhat a lépések összefésülésének szükségessége. Az értékelő vizsgálja meg az útmutatót, hogy az továbbra is teljesíti-e a komponensek értékelése során végrehajtott AGP_PRE tevékenység követelményét.

Előfordulhat olyan eset, hogy a környezetfüggőségi információ a kiszolgáló komponens olyan TSFI-n kívüli interfészeit is azonosítja, amelyekre a környezetfüggőségi információ szerint a kliens komponens hagyatkozik. A kiszolgáló komponens ilyen további interfészeihez útmutatóra lehet szükség. Feltéve, hogy az összetett TOE felhasználója megkapja a kiszolgáló komponensre vonatkozó útmutató dokumentációt, a kiszolgáló komponens AGP_PRE és AGP_OPE döntéseinek eredményei újrahasználhatók azokra az interfészekre, melyeket a kiszolgáló komponens értékelése során vizsgáltak. Azonban, ha a kliens komponens egyéb interfészeket is használ, az értékelőnek meg kell állapítania, hogy a kiszolgáló komponens útmutató dokumentációja megfelel-e az AGP_PRE és AGP_OPE követelményeinek, ahogyan azokat a kiszolgáló komponens értékelése során alkalmazták.

A kiszolgáló komponens értékelés során vizsgált interfészekre, vagyis amelyekre már igazolt a garancia, az értékelő győződjön meg arról, hogy az összetett TOE minden egyes interfész

használati leírása összhangban van-e a kiszolgáló komponensnél írtakkal. Ennek megállapításához az értékelőnek minden interfész esetén végre kell hajtania egy leképezést az összetett TOE és a kiszolgáló komponens útmutatóira. Az értékelő ezután hasonlítsa össze az útmutatókat az ellentmondás-mentesség megállapításához.

Példák összetett TOE útmutatóban megadott olyan egyéb megszorításokra, melyeket vizsgálni kell abból a szempontból, hogy összhangban vannak-e a komponens útmutatóval (egy adott komponens útmutatót követi egy összetett TOE útmutató példa, ami további megszorításnak tekintendő):

- Komponens: A jelszó hosszt minimum 8 karakter hosszúra kell beállítani, és tartalmaznia kell alfabetikus és numerikus karaktereket.
- Összetett TOE: A jelszó hosszt minimum 10 karakter hosszúra kell beállítani, és tartalmaznia kell alfabetikus és numerikus karaktereket, és legalább egyet a következő speciális karakterekből: ( ) { } ^ < > -_
- Megjegyzés: A jelszóhosszt csak növelni lehet [egész szám>8] karakterre, míg az alfabetikus és numerikus karakterek használatának elhagyása csak akkor elfogadható, ha ugyanolyan vagy magasabb mértéket ér el az erősségi besorolás (figyelembe véve a jelszó találgatás valószínűségét).
- Komponens: A következő szolgáltatásokat le kell tiltani a registry beállításokban: WWW Publishing Service és ICDBReporter Service.
- Összetett TOE: A következő szolgáltatásokat le kell tiltani a registry beállításokban: WWW Publishing Service és ICDBReporter Service, Remote Procedure Call (RPC) Locator and Procedure Call (RPC) Service
- Komponens: Válassza ki a következő tulajdonságokat a biztonsági naplóállományban való szerepeltetéshez: dátum, idő, esemény típusa, szubjektum azonosítója, siker/sikertelenség.
- Összetett TOE: Válassza ki a következő tulajdonságokat a biztonsági naplóállományban való szerepeltetéshez: dátum, idő, esemény típusa, szubjektum azonosítója, siker/sikertelenség, esemény szövege és folyamat szál.

Amennyiben az összetett TOE útmutató eltér a kiszolgáló komponensétől (nem pontosítása annak), az értékelő mérje fel az útmutató változásainak lehetséges kockázatait. Ehhez használja a rendelkezésre álló információt (ideértve a nyilvánosan elérhető információkat, a kiszolgáló komponens nyilvánosan elérhető értékelési jelentésében (tanúsítási jelentésben) szereplő architektúra leírást, valamint az útmutató egyéb részeit), azért, hogy azonosítani tudja az útmutató módosításainak az összetett TOE SFR-jeire gyakorolt valószínű hatását.

Amennyiben a kliens komponens értékelése során a próbatelepítés a kiszolgáló komponenst használta a környezeti követelmények teljesítésére, akkor az összetett TOE-ra vonatkozó ezen munkaegység teljesítettnek tekinthető. Ha nem a kiszolgáló komponenst használták az AGD_PRE.1-3 munkaegység kielégítésére a kliens komponens értékelése folyamán, akkor az értékelő alkalmazza az összetett TOE-hoz biztosított felhasználói eljárásokat az összetett TOE előkészítéséhez, ahogyan azt az AGD_PRE.1-3-ban megadott útmutató leírja. Ez lehetővé teszi az értékelő számára annak megállapítását, hogy az összetett TOE-hoz készített előkészítő útmutató kielégítő-e az összetett TOE és annak működési környezete biztonságos előkészítéséhez.

6.2.2.3.1.3. Életciklus - Szállítás

Ha az összetett TOE esetén különböző szállítási mechanizmusokat alkalmaznak (azaz nem a komponensek értékelése során definiált és értékelt biztonságos szállítási eljárásoknak megfelelően juttatják el a komponenseket a felhasználóhoz), akkor az összetett TOE szállítási eljárásait a komponens értékelések során alkalmazott „szállítás” (ALC_DEL) követelményei szerinti értékelésnek kell alávetni.

Az összetett TOE szállítható integrált termékként vagy a komponenseket külön is lehet szállítani.

Ha a komponenseket külön-külön szállítják, akkor a kiszolgáló és kliens komponensek szállítás értékelési eredményei újrahasználhatók. A kiszolgáló komponensek szállítását a kliens komponens értékelői próbatelepítése során ellenőrzik a kiszolgáló komponens útmutatója alapján, alkalmazva a vonatkozó útmutatókat és a szállítást ellenőrző szempontokat, ami a felhasználó felelőssége.

Ha az összetett TOE-t egy egységként szállítják, akkor ennek szállítási eljárásait az összetett TOE értékelési tevékenység részeként kell vizsgálni.

Az összetett TOE elemeinek szállítási eljárásaira vonatkozó értékelést a TOE komponensekre alkalmazott „szállítás” (ALC_DEL) módszertan szerint kell elvégezni, biztosítva, hogy minden további elemet (például kiegészítő útmutatók az összetett TOE-ra) figyelembe vesznek a szállítási eljárásokban.

6.2.2.3.1.4. Életciklus - CM képességek

Az ALC_CMC.1 értékelési altevékenység vizsgálja az összetett TOE egyedi azonosítását, az ALC_CMS.2 értékelési altevékenység pedig azokat az elemeket, melyek az összetett TOE-t alkotják.

Bár az összetett TOE-ra kiegészítő útmutatók készíthetők, ezen útmutató egyedi azonosítása (az ALC_CMC.1 során az összetett TOE egyedi azonosításának részeként) elegendő az útmutató kezeléséhez.

A fennmaradó (fentebb nem vizsgált) ALC osztály (Életciklus támogatás) tevékenységek során hozott döntések újrahasználhatók a kiszolgáló komponens értékeléséből, mivel az összetett TOE integrálása során nem történik további fejlesztés.

A fejlesztés biztonságára nézve nincsenek további szempontok, mivel az integráció vélhetően a felhasználó telephelyén történik, vagy (ha az összetett TOE-t egy egységként szállítják) a kliens komponens fejlesztői telephelyén. A felhasználó telephelye a CC hatókörén kívül esik. Akkor sincsenek további követelmények vagy útmutatók, ha az integrálás ugyanott történik, mint a kliens komponens kialakítása, mivel minden komponens az összetett TOE konfiguráció elemeinek számít, és ezért mindenképp a kliens komponens fejlesztés biztonsági eljárásai értelmében kell vizsgálni.

Az integrálás során alkalmazott eszközök és technikák vizsgálata a kliens komponens fejlesztője által szolgáltatott bizonyítékok segítségével történik. A kiszolgáló komponens szempontjából lényeges összes eszköz/technika ellenőrzését a kiszolgáló komponens értékelése során kell végrehajtani. Például, ha a kiszolgáló komponenst forráskód formájában szállítják, és a felhasználónak kell fordítania, összeszerkesztenie (például az integrációt végző kliens komponens fejlesztőjének), a fordítóprogramot a kiszolgáló komponens értékelése során specifikálni és értékelni kellett, csakúgy, mint a vonatkozó paramétereket.

Az összetett TOE-ra vonatkozóan nincs életciklus definíció, mivel az elemeket nem fejlesztik tovább.

Egy komponens hibajavításának eredményei nem vonatkoznak az összetett TOE-ra. Ha az összetett TOE esetén belevették a garanciacsomagba a hibajavítást, akkor a „hibajavítás” (ALC_FLR) követelményeket kell alkalmazni az összetett TOE értékelése során (mint minden szigorításnál).

6.2.2.3.1.5. Tesztek

Az összetett TOE tesztelése a kliens komponens értékelésekor végzett „tesztelés” (ATE) tevékenység végrehajtása során fog megtörténni, mivel a kliens komponens teszteléséhez használt konfigurációnak magába kellett foglalnia a kiszolgáló komponenst abból a célból, hogy teljesüljenek a működési környezetre vonatkozó követelmények. Ha a kiszolgáló komponenst nem használták a kliens komponens teszteléséhez a kliens értékelése során, vagy az értékelt konfigurációhoz képest bármelyik komponens konfigurációja megváltozott, akkor az összetett TOE-ra meg kell ismételni a kliens komponens értékelésekor végrehajtott fejlesztői tesztet az ATE osztály követelményeinek kielégítése céljából.

6.2.2.4. Interfész tesztelés (ACO_CTT.1) értékelése

Ennek az altevékenységnek a célja annak meghatározása, hogy a fejlesztő jól hajtotta-e végre és dokumentálta-e a teszteket a kiszolgáló komponens azon interfészeire, amelyeket a kliens komponens a működése során meghív. Ennek az elemzésnek a részeként az értékelő megismétli a fejlesztői tesztek egy részét, és további teszteket végez, hogy garantálni lehessen az összetett TOE és a kliens komponens által használt kiszolgáló komponens interfészeinek elvárt működését.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) a tesztelésre alkalmas összetett TOE,
b) az összetett TOE tesztelési bizonyítéka,
c) a környezetfüggőségi információ,
d) a fejlesztési információ.

6.2.2.4.1. Az ACO_CTT.1.1E értékelői akció

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

ACO_CTT.1.1C Az összetett TOE és a kiszolgáló komponens interfész tesztelési dokumentációjának tartalmaznia kell a tesztelési terveket, az elvárt teszteredményeket és a tényleges (kapott) teszteredményeket.

ACO_CTT.1-1 Az értékelőnek meg kell vizsgálnia az összetett TOE tesztelési dokumentációját annak megállapítása érdekében, hogy az tartalmazza-e a tesztelési tervet, a várt teszteredményeket és a tényleges, kapott eredményeket.

Ez a munkaegység teljesíthető a kliens komponens értékeléséből származó tesztelési bizonyítékok által, ha a kiszolgáló komponenst használták a kliens komponens működési környezetére vonatkozó IT követelmények kielégítésére.

Az ATE_FUN.1.1E kielégítéséhez szükséges minden munkaegység alkalmazandó annak meghatározásához, hogy:

a) a tesztelési dokumentáció tartalmazza a tesztelési tervet, a várt teszteredményeket és a tényleges, kapott eredményeket;
b) a tesztelési dokumentáció tartalmazza a tesztek megismételhetőségéhez szükséges információkat;
c) a kiszolgáló komponens tesztelésére fordított fejlesztői munka mennyiségét/szintjét.

ACO_CTT.1-2 Az értékelőnek meg kell vizsgálnia a kiszolgáló komponens interfész tesztelési dokumentációját, annak megállapítása érdekében, hogy az tartalmazza-e a tesztelési tervet, a várt teszteredményeket és a ténylegesen kapott eredményeket.

Ez a munkaegység teljesíthető a kiszolgáló komponens értékeléséből származó tesztelési bizonyítékok által, azon interfészek esetén, amelyeket az összetett TOE-ban a kliens komponens használ, és a kiszolgáló komponens sikeres értékelése során a TSFI részét képezték. Annak megállapítására, hogy a kiszolgáló komponens interfészei, melyeket a kliens használ, valóban a TSFI részei voltak-e, az ACO_COR tevékenység végrehajtása során kerül sor.

Az ATE_FUN.1.1E kielégítéséhez szükséges minden munkaegység alkalmazandó annak meghatározásához, hogy:

a) a tesztelési dokumentáció tartalmazza a tesztelési tervet, a várt teszteredményeket és a tényleges, kapott eredményeket;
b) a tesztelési dokumentáció tartalmazza a tesztek megismételhetőségéhez szükséges információkat;
c) a kiszolgáló komponens tesztelésére fordított fejlesztői munka mennyiségét/szintjét.

ACO_CTT.1.2C Az összetett TOE tesztek fejlesztő által történt elvégzéséből származó tesztelési dokumentációnak meg kell mutatnia, hogy a TSF a specifikáltnak megfelelően működik.

ACO_CTT.1-3 Az értékelőnek meg kell vizsgálnia a tesztelési dokumentációt, annak megállapítása érdekében, hogy a fejlesztő által végrehajtott összetett TOE tesztek megmutatják-e, hogy a TSF a specifikációnak megfelelően működik.

Az értékelőnek egy leképezést ajánlott végeznie a tesztelési tervben leírt tesztek és az összetett TOE számára specifikált SFR-ek között, annak megállapítása érdekében, hogy mely SFR-eket tesztelte a fejlesztő.

E munkaegységhez útmutató található:
a) 7.1 fejezetben és
b) 7.2 fejezetben.

A tesztek sikeres végrehajtásából származó kimenetek (ATE_FUN.1.3C számára) összehasonlíthatók a leképezéssel annak megállapítása érdekében, hogy az összetett TOE SFR-ek –ahogyan azokat a fejlesztő tesztelte- az elvárt módon működnek-e.

ACO_CTT.1.3C A kiszolgáló komponens interfész tesztek fejlesztő által történt elvégzéséből származó tesztelési dokumentációnak meg kell mutatnia, hogy a kliens komponens által használt kiszolgáló komponens interfész a specifikáltnak megfelelően működik.

ACO_CTT.1-4 Az értékelőnek meg kell vizsgálnia a tesztelési dokumentációt, annak megállapítása érdekében, hogy a fejlesztő által végrehajtott kiszolgáló komponens interfész tesztek megmutatják-e, hogy a kliens komponens által használt kiszolgáló komponens interfészek a specifikációnak megfelelően működnek.

Az értékelőnek egy leképezést ajánlott végeznie a tesztelési tervben leírt tesztek és a kliens komponens által használt kiszolgáló komponens interfészek (ahogyan azt az ACO_REL által vizsgált környezetfüggőségi információ specifikálja) között, annak megállapítása érdekében, hogy mely kiszolgáló komponens interfészeket tesztelte a fejlesztő.

E munkaegységhez útmutató található:
a) 7.1 fejezetben és
b) 7.2 fejezetben.

A tesztek sikeres végrehajtásából származó kimenetek (ATE_FUN.1.3C számára) összehasonlíthatók a leképezéssel annak megállapítása érdekében, hogy kiszolgáló komponens interfészei –ahogyan azokat a fejlesztő tesztelte- az elvárt módon működnek-e.

ACO_CTT.1.4C A kiszolgáló komponensnek tesztelésre alkalmasnak kell lennie.

ACO_CTT.1-5 Az értékelőnek meg kell vizsgálnia az összetett TOE-t, annak megállapítása érdekében, hogy azt megfelelő módon telepítették-e, és az ismert állapotok egyikében van-e.

Annak megállapítása, hogy az összetett TOE-t megfelelően telepítették, és az ismert állapotok valamelyikében van-e, az ATE_IND.2-1 és ATE_IND.2-2 munkaegységek feladata, aminek keretében a fejlesztő által tesztelésre átadott TOE-t vizsgálják.

ACO_CTT.1-6 Az értékelőnek meg kell vizsgálnia a fejlesztő által biztosított erőforrás együttest, annak megállapítása érdekében, hogy azok megegyeznek-e a kiszolgáló komponens funkcionális teszteléséhez a kiszolgáló komponens fejlesztője által használt erőforrásokkal.

Annak megállapítása, hogy a biztosított erőforrások megegyeznek a kiszolgáló komponens összetett TOE-beli használata szerinti funkcionális teszteléséhez használt erőforrásokkal, az ATE_IND.2-3 munkaegység hatásköre.

6.2.2.4.2. Az ACO_CTT.1.2E értékelői akció

ACO_CTT.1.2E Az értékelőnek végre kell hajtania a tesztelési dokumentációban szereplő tesztek egy mintáját a fejlesztői teszteredmények ellenőrzése céljából.

ACO_CTT.1-7 A tesztek kiválasztását és végrehajtását az ATE_IND.2.2E-vel összhangban kell elvégezni, bizonyítandó, hogy az összetett TOE biztonsági előirányzatban specifikált SFR-ek megfelelően működnek.

Az értékelőnek az ATE_IND.2.2E kielégítéséhez szükséges összes munkaegységet alkalmaznia kell, és az összetett TOE ETR-ben rögzítenie kell a kapcsolódó munkaegységek által előírt minden vizsgálatot, kapott eredményt és döntést.

6.2.2.4.3. Az ACO_CTT.1.3E értékelői akció

ACO_CTT.1.3E Az értékelőnek le kell tesztelnie az összetett TOE TSF interfészeinek egy részhalmazát, hogy meggyőződjön arról, hogy az összetett TSF a specifikáltnak megfelelően működik.

ACO_CTT.1-8 Az értékelőnek az ATE_IND.2.3E szerinti tesztelést kell végeznie az összetett TOE biztonsági előirányzatában megadott SFR-ek részhalmazára, azt bizonyítandó, hogy a TSF a specifikációnak megfelelően működik.

Az értékelőnek alkalmaznia kell az ATE_IND.2.3E kielégítéséhez szükséges minden munkaegységet, és rögzítenie kell az összetett TOE ETR-ben minden előírt vizsgálatot, eredményt és döntést.

Amikor az összetett TOE TSF interfészeinek tesztelésre való kiválasztása történik, az értékelőnek figyelembe kell vennie minden olyan módosítást, amely a komponensekben az értékelt verzió vagy konfiguráció óta történt. Ez jelenthet javításokat, a módosított útmutató dokumentációk miatti eltérő konfigurálást, a komponens TSF-jébe nem eső egyéb komponens elemektől való környezeti függőséget. Ezeket a módosításokat a „komponens-összeállítás indoklás” (ACO_COR) tevékenység során kell azonosítani.

6.2.2.5. Kompozíció sebezhetőség áttekintés (ACO_VUL.1) értékelése

Ezen altevékenység célja annak megállapítása, hogy az összetett TOE-nek, működési környezetében vannak-e alap támadási képességgel kihasználható sebezhetőségei.

A fejlesztő részleteket szolgáltat a komponensek értékelése során jelentett maradvány sebezhetőségekről. Az értékelő egy elemzést végez a jelentett maradvány kockázatokkal kapcsolatosan, majd kutatásokat végez a nyilvánosan hozzáférhető forrásokban, hogy azonosítson minden lehetséges új, a komponenseket fenyegető sebezhetőséget (a komponensek értékelésének befejezése óta felmerült sebezhetőségeket). Az értékelő ezen kívül egy behatolás tesztelést hajt végre annak kimutatására, hogy a lehetséges sebezhetőségek nem kihasználhatók az összetett TOE működési környezetében, egy alap támadási képességgel rendelkező támadó számára.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) a tesztelésre alkalmas összetett TOE,
b) az összetett ST,
c) a komponens-összeállítás indoklás,
d) az útmutató dokumentáció,
e) nyilvánosan elérhető információ a lehetséges biztonsági sebezhetőségek meghatározásának támogatására,
f) az összes komponens értékelése során jelentett maradvány sebezhetőségek.

6.2.2.5.1. Az ACO_VUL.1.1E értékelői akció

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

ACO_VUL.1.1C Az összetett TOE-nak tesztelésre alkalmasnak kell lennie.

ACO_VUL.1-1 Az értékelőnek meg kell vizsgálnia az összetett TOE-t, annak megállapítása érdekében, hogy azt megfelelő módon telepítették-e, és az ismert állapotok egyikében van-e.

Annak megállapítása, hogy az összetett TOE-t megfelelően telepítették-e, és az ismert állapotok valamelyikében van-e, az összetett TOE-ra vonatkozó ATE_IND.2-1 és ATE_IND.2-2 munkaegységek feladata.

Ha a garanciacsomag tartalmazza az ACO_CTT családot, akkor az értékelő hivatkozhat az „összetett TOE tesztelése” (ACO_CTT)*-1 eredményére, hogy az teljesül.

ACO_VUL.1-2 Az értékelőnek meg kell vizsgálnia az összetett TOE konfigurációt annak megállapítása érdekében, hogy az ST-ben szereplő, a komponensekre vonatkozó bármilyen feltételezést és célt, amely IT entitásokkal kapcsolatos, más komponensek kielégítenek.

A komponens ST-je tartalmazhat feltételezéseket más komponensekkel kapcsolatban, amelyek használhatják az ST-vel kapcsolatos komponenst; például egy kiszolgáló komponensként alkalmazott operációs rendszerre vonatkozó ST tartalmazhat olyan feltételezést, hogy a rajta működő bármilyen alkalmazás ne fusson privilegizált módban. Ezek a feltételezések és célok az összetett TOE más komponensei által teljesítendők.

6.2.2.5.2. Az ACO_VUL.1.2E értékelői akció

ACO_VUL.1.2E Az értékelőnek végre kell hajtania egy vizsgálatot annak megállapítása érdekében, hogy a kiszolgáló és a kliens komponensre beazonosított bármilyen maradvány sebezhetőség nem aknázható ki az összetett TOE-ban, annak működési környezetében.

ACO_VUL.1-3 Az értékelőnek meg kell vizsgálnia a kiszolgáló komponens értékeléséből származó maradvány sebezhetőségeket annak megállapítása érdekében, hogy azok nem kiaknázhatók-e az összetett TOE működési környezetében.

A kiszolgáló komponens értékelés során a termékre felismert sebezhetőségek listáját – melyeket a kiszolgáló komponensben nem kihasználhatónak ítéltek – kell használni ennek a tevékenységnek a bemeneteként. Az értékelő állapítsa meg, hogy azok a feltételek, amelyek alapján a sebezhetőséget nem kihasználhatónak ítélték, fennállnak-e az összetett TOE-ra, vagy a komponens-összeállítás miatt felmerülhet az adott sebezhetőség kiaknázhatósága. Például, ha a kiszolgáló komponens értékelése során felételezték, hogy egy bizonyos operációs rendszer szolgáltatás le van tiltva, ami viszont engedélyezett az összetett TOE értékelésben, akkor az ehhez a szolgáltatáshoz kapcsolódó bármilyen lehetséges sebezhetőséget, amelyet korábban kizártak, most figyelembe kell venni.

Továbbá, a kiszolgáló komponens értékeléséből származó ismert, nem kihasználható sebezhetőségeket is figyelembe kell venni a többi komponenssel (pl. kliens komponenssel) kapcsolatos minden ismert, nem kihasználható sebezhetőség ismeretében az összetett TOE-n belül. Ez azt az esetet fedi le, amikor egy lehetséges sebezhetőség, ami elszigetelve nem kihasználható volt, egy másik -potenciális sebezhetőséget tartalmazó- IT egyeddel való integrálás után kiaknázhatóvá válik.

ACO_VUL.1-4 Az értékelőnek meg kell vizsgálnia a kliens komponens értékeléséből származó maradvány sebezhetőségeket annak megállapítása érdekében, hogy azok nem kihasználhatók-e az összetett TOE működési környezetében.

A kliens komponens értékelés során a termékre felismert sebezhetőségek listáját –melyeket a kliens komponensben nem kihasználhatóknak ítéltek – kell használni ennek a tevékenységnek a bemeneteként. Az értékelő állapítsa meg, hogy azok a feltételek, amelyek alapján a sebezhetőséget nem kihasználhatónak ítélték, fennállnak-e az összetett TOE-ra, vagy a komponens-összeállítás miatt felmerülhet az adott sebezhetőség kiaknázhatósága. Például, ha a kliens komponens értékelése során azt felételezték, hogy a működési környezet követelményeit kielégítő IT-egyed nem ad vissza egy bizonyos értéket egy szolgáltatás kérésre, amelyet az összetett TOE-ban a kiszolgáló komponens most visszaad, akkor az ehhez a visszatérési értékhez kapcsolódó, korábban kizárt bármilyen lehetséges sebezhetőséget újra figyelembe kell venni.

Továbbá, a kliens komponens értékeléséből származó ismert, nem kihasználható sebezhetőségeket is figyelembe kell venni a többi komponenssel (pl. kiszolgáló komponenssel) kapcsolatos minden ismert, nem kihasználható sebezhetőség ismeretében az összetett TOE-n belül. Ez azt az esetet fedi le, amikor egy lehetséges sebezhetőség, ami elszigetelve nem kihasználható volt, egy másik - lehetséges sebezhetőséget tartalmazó - IT egyeddel való integrálás után kiaknázhatóvá válik.

6.2.2.5.3. Az ACO_VUL.1.3E értékelői akció

ACO_VUL.2.3E Az értékelőnek kutatnia kell a nyilvánosan hozzáférhető forrásokat a kiszolgáló és a kliens komponensnek az összetett TOE működési környezetében való használatából származó lehetséges sebezhetőségeinek feltárása céljából.

ACO_VUL.1-5 Az értékelőnek meg kell vizsgálnia a nyilvánosan hozzáférhető információforrásokat annak érdekében, hogy azonosítani lehessen a kiszolgáló komponensben azokat a lehetséges biztonsági sebezhetőségeket, amelyek a kiszolgáló komponens értékelésének befejezése óta váltak ismertté.

Az értékelőnek fel kell használnia a nyilvánosan hozzáférhető információkat –ahogyan azt a [3]-beli AVA_VAN.1-2 leírja- a kiszolgáló komponens sebezhetőségeinek feltárása céljából.

Nem kell tovább vizsgálni azokat a lehetséges sebezhetőségeket, amelyek a kiszolgáló komponens értékelése előtt már nyilvánosan ismertek voltak, kivéve, ha nyilvánvaló az értékelő számára, hogy a szóban forgó sebezhetőség kiaknázásához szükséges támadás képesség jelentős mértékben csökkent. Ez bekövetkezhet a kiszolgáló komponens értékelése óta megjelent új technológia miatt, melynek alkalmazása egyszerűsíti a sebezhetőség kihasználását.

ACO_VUL.1-6 Az értékelőnek meg kell vizsgálnia a nyilvánosan hozzáférhető információforrásokat annak érdekében, hogy azonosítani lehessen a kliens komponensben azokat a lehetséges biztonsági sebezhetőségeket, amelyek a kliens komponens értékelésének befejezése óta váltak ismertté.

Az értékelőnek fel kell használnia a nyilvánosan hozzáférhető információkat –ahogyan azt a [3]-beli AVA_VAN.1-2 leírja- a kiszolgáló komponens sebezhetőségeinek feltárása céljából.

Nem kell tovább vizsgálni azokat a lehetséges sebezhetőségeket, amelyek a kliens komponens értékelése előtt már nyilvánosan ismertek voltak, kivéve, ha nyilvánvaló az értékelő számára, hogy a szóban forgó sebezhetőség kiaknázásához szükséges támadás képesség jelentős mértékben csökkent. Ez bekövetkezhet a kliens komponens értékelése óta megjelent új technológia miatt, melynek alkalmazása egyszerűsíti a sebezhetőség kihasználását.

ACO_VUL.1-7 Az értékelőnek rögzítenie kell az ETR-ben az azonosított lehetséges sebezhetőségeket, melyek szóba jönnek a tesztelésnél, és amelyek az összetett TOE működési környezetében kihasználhatóak lehetnek.

Az ST, az útmutató dokumentumok és a funkcionális specifikáció segítségével meg kell állapítani, hogy a sebezhetőségek valóban relevánsak-e az összetett TOE működési környezetében.

Az értékelő rögzítsen minden olyan indokot, ami miatt sebezhetőségek kizárhatók a további vizsgálatokból, ha úgy ítéli meg, hogy a sebezhetőség nem vonatkoztatható a működési környezetre. Egyébként pedig rögzítse a lehetséges sebezhetőségeket további mérlegelés, vizsgálat céljából.

Az összetett TOE-ra annak működési környezetében vonatkoztatható lehetséges sebezhetőségek listáját, ami a behatolás tesztelési tevékenység (ACO_VUL.1.4E) bemenete, az értékelőknek az ETR-ben meg kell adniuk.

6.2.2.5.4. Az ACO_VUL.1.4E értékelői akció

ACO_VUL.1.4E Az értékelőnek behatolás tesztelést kell végeznie, ami az azonosított sebezhetőségeken alapul, annak megmutatása céljából, hogy az összetett TOE ellenáll az alap támadási képességgel rendelkező támadó támadásainak.

ACO_VUL.1-8 Az értékelőnek végre kell hajtania a behatolás tesztelést, ahogyan azt a [3]-beli AVA_VAN.1.3E leírja.

Az értékelő a [3]-beli AVA_VAN.1.3E értékelői feladat teljesítése érdekében alkalmazza az összes szükséges munkaegységet, és az ETR-ben rögzítse az összetett TOE-ra elvégzett összes vizsgálatot és meghozott döntést, melyeket a munkaegységek előírnak.

Az értékelő a [3]-beli AVA_VAN.1.1E értékelői feladathoz is alkalmazza a munkaegységeket annak megállapítása érdekében, hogy a fejlesztő által biztosított összetett TOE alkalmas-e a tesztelésre.

6.2.3. Összetett TOE értékelése CAP-F esetén

6.2.3.1. Alap környezetfüggőségi információ (ACO_REL.1) értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztői környezetfüggőségi bizonyíték kielégítő információt tartalmaz-e annak meghatározásához, hogy a kiszolgáló komponens biztosítja a szükséges funkcionalitást, illetve e funkciók meghívásának módszeréről. Ez egy magas szintű leírás segítségével fejezhető ki.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az összetett ST,
b) a kliens komponens funkcionális specifikációja,
c) a kliens komponens terve,
d) a kliens komponens architektúra terve,
e) a környezetfüggőségi információ.

Egy olyan kliens komponens, amelynek TSF-je együttműködik a kiszolgáló komponenssel, funkcionalitást vár el a kiszolgáló komponenstől (például távoli hitelesítés, távoli naplóadat tárolás). Ezekben az esetekben a hívott szolgáltatásokat le kell írni azok részére, akik a végfelhasználók számára konfigurálják az összetett TOE-t. E leírási követelmény oka, hogy segíteni kell az összetett TOE integrátorokat annak meghatározásában, hogy a kiszolgáló komponens mely szolgáltatásainak lehet kedvezőtlen (ártalmas) hatása a kliens komponensre, és információk álljanak rendelkezésre, amelyek alapján meg lehet állapítani a komponensek kompatibilitását a fejlesztési bizonyíték (ACO_DEV) család alkalmazása során.

6.2.3.1.1. Az ACO_REL.1.1E értékelői akció

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

ACO_REL.1.1C A környezetfüggőségi információnak le kell írnia a kiszolgáló komponens azon hardver, szoftver és/vagy förmver elemeinek funkcionalitását, melyre a kliens komponens TSF támaszkodik.

ACO_REL.1-1 Az értékelőnek ellenőriznie kell a környezetfüggőségi információt, annak megállapítása érdekében, hogy szerepel-e benne a kiszolgáló komponens hardverei, förmverei és/vagy szoftverei által nyújtott funkcionalitás leírása, amire a kliens komponens TSF-je épít a működése végrehajtása során.

Az értékelő vizsgálja meg annak a biztonsági funkcionalitásnak a leírását, amit a kliens komponens TSF-je igényel a kiszolgáló komponens hardver, szoftver, förmver elemeitől. A munkaegység fókuszában elsősorban e leírás részletessége álljon, és nem annyira az információ pontosságának ellenőrzése. (Ez utóbbira a következő munkaegység összpontosít).

A kiszolgáló komponens leírásának nem kell részletesebbnek lennie, mint egy komponens TSF leírás részletessége, ahogyan azt a TOE terv (ADV_TDS) megadja.

ACO_REL.1-2 Az értékelőnek meg kell vizsgálnia a környezetfüggőségi információt annak megállapítása érdekében, hogy az pontosan tükrözi-e a kliens komponens működtetési környezetére vonatkozó célokat.

A környezetfüggőségi információ tartalmazza a kliens komponens által használt kiszolgáló komponens biztonsági funkcionalitás leírását. Annak biztosítása érdekében, hogy a környezetfüggőségi információ összhangban legyen a kliens komponens működési környezetére vonatkozó elvárásaival, az értékelő hasonlítsa össze a környezetfüggőségi információt a kliens komponens ST-jében megadott környezeti biztonsági célok nyilatkozatával.

Például ha a környezetfüggőségi információban az szerepel, hogy a kliens komponens TSF-je a kiszolgáló komponens funkcióira épít a naplóadatok tárolása és védelme tekintetében, de egy másik értékelési bizonyíték (pl. a kliens komponens tervdokumentációja) egyértelművé teszi, hogy a kliens komponens TSF-je maga tárolja és védi a naplóadatokat, akkor ez pontatlanságot jelez.

Megjegyzendő, hogy a működtetési környezetre vonatkozó célok tartalmazhatnak nem IT eszközökkel kielégíthető célokat. A kiszolgáló komponenstől elvárt szolgáltatások leírhatók a kliens komponens ST-ben a működési környezetre vonatkozó IT biztonsági célokként, de az nem követelmény, hogy minden ilyen környezetre vonatkozó elvárás szerepeljen a környezetfüggőségi információ között.

ACO_REL.1.2C A környezetfüggőségi információnak le kell írnia minden kapcsolatot, amelyen át a kliens komponens TSF-je szolgáltatásokat kér a kiszolgáló komponenstől.

ACO_REL.1-3 Az értékelőnek meg kell vizsgálnia a környezetfüggőségi információt, annak megállapítása érdekében, hogy leírták-e benne a kliens és a kiszolgáló komponens közötti összes kölcsönhatást, mely kölcsönhatások révén a kliens komponens TSF-je szolgáltatásokat kér a kiszolgáló komponenstől.

A kliens komponens TSF-je kérhet olyan szolgáltatásokat a kiszolgáló komponenstől, amelyek nem voltak a kiszolgáló komponens TSF-jén belül. (Lásd B.3 függeléket, CC 3. részben: Összetett IT egyedek közötti kölcsönhatások).

A kiszolgáló komponens funkcionalitásával kapcsolatos interfészeket ugyanolyan szinten kell leírni, mint a kliens TSF funkcionalitását, amint azt a „TOE terv" (ADV_TDS.1) biztosítja az alrendszerek között.

A kliens és a kiszolgáló komponens közötti együttműködés leírásának célja annak megmutatása, hogy a kliens komponens TSF-je hogyan alapoz a kiszolgáló komponens szolgáltatásaira a saját biztonsági funkcionalitásának végrehajtása céljából. Ezeket a kölcsönhatásokat nem kell a megvalósítás szintjén jellemezni (pl. rutinok közötti paraméterátadás szintjén), de egy összetevő által használandó adott összetevőhöz meghatározott adatelemeket tartalmaznia kell e leírásnak. A leírásnak segítenie kell az olvasót annak általános megértésében, hogy miért van szükség az interakcióra.

Az interfészek pontossága és teljessége a kiszolgáló komponens által biztosítandó, TSF által kért biztonsági funkcionalitáson alapul, amint azt az ACO_REL.2-1 és ACO_REL.2-2 munkaegységek elemzik. Lehetséges, hogy a korábbi munkaegységekben leírt összes funkcionalitás leképezhető az ebben a munkaegységben azonosított interfészekre, és fordítva. Egy olyan interfész, ami nem tartozik leírt funkcióhoz, szintén pontatlanságot jelez.

ACO_REL.1.3C A környezetfüggőségi információnak le kell írnia, hogy a kliens TSF hogyan védi magát a kiszolgáló komponens beavatkozásával és manipulálásával szemben.

ACO_REL.1-4 Az értékelőnek meg kell vizsgálnia a környezetfüggőségi információt, annak megállapítása érdekében, hogy szerepel-e benne az, hogy a kliens TSF hogyan védi meg magát a kiszolgáló komponenshez köthető beavatkozás és manipulálás ellen.

A beavatkozás és manipulálás elleni védelem módját az ADV_ARC.1-4-hez szükséges részletességgel kell biztosítani.

6.2.3.2. Alap tervezési bizonyíték (ACO_DEV.2) értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a kiszolgáló komponens a megfelelő biztonsági funkcionalitást nyújtja-e a kliens komponens számára. Ez a kiszolgáló komponens interfészeinek és a kapcsolódó biztonsági funkciók működésének arra irányuló vizsgálatával állapítható meg, hogy azok összhangban vannak-e a környezetfüggőségi információban specifikált, kliens komponens által igényelt interfészekkel.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az összetett ST,

b) a fejlesztési információ,
c) a környezetfüggőségi információ.

6.2.3.2.1. Az ACO_DEV.2.1E értékelői akció

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

ACO_DEV.2.1C A fejlesztési információnak le kell írnia az összetett TOE-ban használt kiszolgáló komponens minden egyes interfészére azok célját és használati módját.

ACO_DEV.2-1 Az értékelőnek meg kell vizsgálnia a fejlesztési információt, annak megállapítása érdekében, hogy az leírja-e az egyes interfészek célját.

A kiszolgáló komponens interfészeket biztosít a kliens komponenssel való együttműködéshez a kliens TSF működésének támogatásához. Az egyes interfészek célját ugyanolyan szinten kell leírni, mint a kliens komponens TSF funkcionalitásához szükséges interfészeket, ahogyan azokat a TOE tervben az alrendszerek között meg kell adni (ADV_TDS.1). Ez a leírás teszi lehetővé az olvasó számára annak megismerését, hogy a kiszolgáló komponens hogyan biztosítja a kliens komponens TSF-je által igényelt szolgáltatásokat.

Ez a munkaegység teljesíthető a kiszolgáló komponens TSFI interfészeire vonatkozó funkcionális specifikáció biztosításával.

ACO_DEV.2-2 Az értékelőnek meg kell vizsgálnia a fejlesztési információt, annak megállapítása érdekében, hogy az leírja-e az egyes interfészek használati módját.

Az interfészek használati módja azt összegzi, hogy az interfészt hogyan kell alkalmazni a műveletek kezdeményezéséhez és az eredmények fogadásához. Az értékelőnek meg kell tudni határozni a fejlesztési információ ezen része alapján, hogy az egyes interfészeket hogyan kell használni. Ez nem feltétlenül jelenti, hogy minden egyes interfészre külön módszer van, például általánosan is leírható, hogy API hívásokat hogyan kell kezdeményezni, és ezen általános formával azonosíthatók az egyes interfészek.

Ez a munkaegység teljesíthető a kiszolgáló komponens TSFI interfészeire vonatkozó funkcionális specifikáció biztosításával.

ACO_DEV.2.2C A fejlesztési információnak magas szinten le kell írnia a kiszolgáló komponens azon alrendszereinek működését, melyek a kliens komponens SFR-jeinek érvényre juttatását támogatják.

ACO_DEV.2-3 Az értékelőnek meg kell vizsgálnia a fejlesztési információt, annak megállapítása érdekében, hogy az leírja-e a kliens komponens SFR-jeinek érvényre juttatását támogató kiszolgáló komponens alrendszerek működését.

A kliens komponens a kiszolgáló komponens interfészeit hívja meg a kiszolgáló komponens funkcióinak használata céljából. A kiszolgáló komponens meghívott interfészeire a fejlesztési

információban meg kell adni a kiszolgáló komponens vonatkozó biztonsági működésének magas szintű leírását. Ez a leírás megmutatja, hogy a kiszolgáló komponens hogyan biztosítja a szükséges szolgáltatásokat az interfészhívás pillanatában. A leírásnak az ADV_TDS.1.4C-hez hasonló szinten kell az információkat megadnia. Ezért a kiszolgáló komponens értékeléséből származó TOE terv bizonyíték biztosítása kielégíti ezt a munkaegységet, amikor a kliens komponens által hívott interfészek a kiszolgáló komponens TSFI-elemei. Ha viszont nem azok, akkor a kapcsolódó biztonsági működést nem feltétlenül kell leírni a kiszolgáló komponens TOE terv bizonyítékban.

ACO_DEV.2.3C A fejlesztési információnak ki kell mutatnia az összetett TOE-ban használt,
- a kliens komponens TSF-jét támogató- kiszolgáló és kliens komponens interfészek közötti megfeleltetéseket.

ACO_DEV.2-4 Az értékelőnek meg kell vizsgálnia a fejlesztési információt, annak megállapítása érdekében, hogy pontos-e a kiszolgáló komponens interfészei és a kliens komponens által használt interfészek közötti megfeleltetés.

A kiszolgáló komponens interfészei és a kliens komponens által használt interfészek közötti megfeleltetés elvégezhető táblázatos vagy mátrix formában. A kliens komponens által használt interfészeket a környezetfüggőségi információ azonosítja (és a „kliens komponens környezetfüggősége” (ACO_REL) során vizsgálják).

E tevékenység során nem követelmény a kliens komponens által használt interfészek teljes lefedettségének a megállapítása, csak az, hogy a megfeleltetés helyes-e, és a kiszolgáló komponens interfészeit leképezték-e a kliens komponens által hívott interfészekre, ahol ez lehetséges. A lefedettség teljességét a „komponens-összeállítás indoklás” (ACO_COR) tevékenység vizsgálja.

6.2.3.2.2. Az ACO_DEV.2.2E értékelői akció

ACO_DEV.2.2E Az értékelőnek meg kell állapítania, hogy a megadott interfész leírás nem mond-e ellent a kliens komponensre megadott környezetfüggőségi információnak.

ACO_DEV.2-5 Az értékelőnek meg kell vizsgálnia a fejlesztési információt és a környezetfüggőségi információt, annak megállapítása érdekében, hogy az interfészek leírása ellentmondásmentes-e.

E munkaegység értékelői célja annak meghatározása, hogy a kiszolgáló komponens fejlesztési információjában és a kliens komponens környezetfüggőségi információjában leírt interfészek összhangban vannak-e egymással.

6.2.3.3. Komponens-összeállítás indoklás (ACO_COR.1) értékelése

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:
a) az összetett ST,
b) a komponens-összeállítás indoklás,
c) a környezetfüggőségi információ,

d) a fejlesztési információ,
e) egyedi azonosító.

6.2.3.3.1. Az ACO_COR.1.1E értékelői akció

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

ACO_COR.1.1C A komponens-összeállítás indoklásnak meg kell mutatnia, hogy a garanciaszint legalább olyan magas, mint amit a kliens komponens elért a kiszolgáló komponens támogató funkciójára, amikor a kiszolgáló komponenst a kliens komponens TSF-jének támogatására konfigurálták.

ACO_COR.1-1 Az értékelőnek meg kell vizsgálnia a komponens-összeállítás indoklást a fejlesztési információkkal és környezetfüggőségi információkkal együtt a kliens komponens által használt olyan interfészek azonosítása céljából, amelyeket a fejlesztési információk nem részleteznek.

E munkaegység elvégzésének célja kettős:
a) annak meghatározása, hogy a kliens komponens által használt mely interfészek esetén alkalmazták a megfelelő garanciális intézkedéseket;
b) annak megállapítása, hogy a kiszolgáló komponens értékelése során használt garanciacsomag ugyanazon, vagy hierarchikusan magasabb garanciális követelményeket tartalmazta, mint amelyeket a kliens komponens értékelése során figyelembe vettek.

Az értékelő felhasználhatja a „fejlesztési bizonyíték” (ACO_DEV) tevékenységek végzése során létrehozott fejlesztési információkban szereplő megfelelőség visszavezetést (pl. ACO_DEV.l-2, ACO_DEV.2-4, ACO_DEV.3-6) a környezetfüggőségi információban azonosított azon interfészek meghatározására, melyeket a fejlesztési információk figyelmen kívül hagytak.

Az értékelőnek rögzítenie kell az SFR-t érvényre juttató interfészeket, melyek a környezetfüggőségi információban szerepelnek, de a fejlesztési információban nem. Ezek jelentik az ACO_COR.1-3 munkaegység bemenetét, a kiszolgáló komponens további garanciát igénylő részeinek azonosítását segítve.

Amennyiben a kiszolgáló és a kliens komponenst is ugyanazon garanciacsomag szerint értékelték, akkor magától értetődő annak meghatározása, hogy a kiszolgáló komponens értékelésen belüli részeinek garanciaszintje legalább olyan magas-e, mint a kliens komponensé. Amennyiben azonban a komponensek értékelésekor alkalmazott garanciacsomagok különböznek, akkor az értékelőnek meg kell állapítania, hogy a kiszolgáló komponensre alkalmazott garanciális követelmények mindegyike hierarchikusan magasabb-e, mint a kliens komponensre alkalmazott garanciális követelmény.

ACO_COR.1-2 Az értékelőnek meg kell vizsgálnia a komponens-összeállítás indoklását annak meghatározásához, hogy azon kiszolgáló komponens interfészekre, melyekre a kliens

TSF a működésében hagyatkozik, az interfészt vizsgálták-e a kiszolgáló komponens értékelése során.

Az összetett ST, valamint a kiszolgáló komponensre vonatkozó nyilvános értékelési jelentés (pl. tanúsítási jelentés) és útmutató dokumentumok információkat adnak a kiszolgáló komponens logikai hatóköréről és határairól. Az összetett ST részletekkel szolgál az összetett TOE logikai hatóköréről és határairól, lehetővé téve az értékelő számára annak megállapítását, hogy egy interfész kapcsolódik-e az értékelés hatókörébe tartozó termékrészhez. Az útmutató dokumentáció részletesen leírja az összetett TOE összes interfészének a használatát. Bár az útmutató dokumentáció olyan interfészeket is tárgyalhat, amelyek nem esnek értékelés alá, minden ilyen interfésznek azonosíthatónak kell lennie, vagy az ST-ben szereplő hatókör meghatározásból vagy az értékelt konfigurációt részletező útmutató részekből. A nyilvános értékelési jelentés további szükséges megszorításokat tartalmazhat az összetett TOE használatára.

Ezért a fenti bemenetek kombinációja lehetővé teszi az értékelő számára, hogy megállapítsa, a komponens-összeállítás indoklásban leírt interfész rendelkezik-e a hozzá kapcsolódó garanciákkal, vagy szükség van további garanciára. Az értékelő rögzítse a kiszolgáló komponens azon interfészeit, melyekre szükséges ilyen további garancia, amit az ACO_COR.1-3 során mérlegelnek.

ACO_COR.1-3 Az értékelőnek meg kell vizsgálnia a komponens-összeállítás indoklást annak megállapítása érdekében, hogy a kiszolgáló komponensre alkalmazták-e a szükséges garanciális intézkedéseket.

A kiszolgáló komponensre vonatkozó értékelői döntés és az abból következő garancia újrahasználható, feltéve, ha az összetett TOE-ban a kiszolgáló komponens ugyanazon részeit használják, és következetesen alkalmazzák azokat.

Annak meghatározásához, hogy a komponensre alkalmazták-e már a szükséges garanciális intézkedéseket, és a komponens mely részeire kell még garanciális intézkedéseket alkalmazni, az értékelőnek használnia kell az ACO_DEV.*.2E tevékenység és az ACO_COR.1-1 és ACO_COR.1-2 munkaegység kimenetét:

a) A környezetfüggőségi információban (ACO_REL) azonosított, de a fejlesztési információ (ACO_DEV) között nem elemzett interfészek esetén további információ szükséges (azonosítva ACO_COR.1-1-ben).
b) A kiszolgáló komponens azon interfészei esetén, melyeket nem konzisztens módon használtak az összetett TOE-ban (különbség van a „fejlesztési bizonyíték” (ACO_DEV) és a „kliens komponens környezetfüggősége” (ACO_REL) között), a különbség kihatását meg kell nézni (ACO_DEV.*.2E).
c) További információra van szükség azon interfészek esetén, melyeket a komponens-összeállítás indoklás azonosít és nincs hozzájuk korábban igazolt garancia (azonosítva ACO_COR.1-2-ben).
d) Azon interfészek esetén pedig, melyeket a környezetfüggőségi információ, a komponens-összeállítás indoklás és a fejlesztési információ ellentmondásmentesen írnak le, nincs további teendő, mivel a kiszolgáló komponens értékelési eredményei újrahasználhatók.

A környezetfüggőségi információ által megkövetelt, de a fejlesztési információban nem szereplő kiszolgáló komponens interfészek a kiszolgáló komponens azon elemeit mutatják, ahol további garanciára van szükség. Az interfészek azonosítják a kiszolgáló komponens belépési pontjait.

Azoknál az interfészeknél, melyeket mind a fejlesztési információ, mind a környezetfüggőségi információ tárgyal, az értékelőnek kell megállapítania, hogy az interfészeket az összetett TOE-ban oly módon alkalmazzák-e, ami megfelel a kiszolgáló komponens értékelésének. Az interfész használat módját a „fejlesztési bizonyíték" (ACO_DEV) tevékenység során vizsgálják abból a célból, hogy kiderüljön, az interfész használat megfelel mind a kiszolgáló komponensnek, mind az összetett TOE-nak. A fennmaradó vizsgálat tárgya annak megállapítása, hogy nem mondanak-e ellent egymásnak a kiszolgáló komponens és az összetett TOE konfigurációi. Ennek meghatározásához az értékelő vizsgálja meg a vonatkozó útmutató dokumentációkat, hogy azok ellentmondásmentesek-e (további útmutató a konzisztens dokumentációkról jelen anyag további részeiben olvasható). A dokumentációban talált bármilyen eltérés esetén újabb vizsgálat következik a lehetséges következmények felmérése céljából.

Azon interfészek esetén, melyekre fennáll a környezetfüggőségi és fejlesztési információ ellentmondás-mentessége, és amelyeknél a kiszolgáló komponens és az összetett TOE útmutatója összhangban van egymással, biztosított a megkívánt garancia szintje.

Az alábbi bekezdések támpontot adnak ahhoz, hogyan lehet meghatározni a konzisztenciát a kiszolgáló komponensre érvényes garancia és az összetett TOE-hez adott bizonyíték között, valamint az értékelő által végrehajtott elemzéshez olyan esetekben, amikor ellentmondásokra derül fény.

6.2.3.3.1.1. Fejlesztés

A környezetfüggőségi információ azonosítja a kliens komponens interfészeit, amiket a kiszolgáló komponenshez kell illeszteni. Ha a környezetfüggőségi információ között azonosított interfész nem szerepel a fejlesztési információ között, akkor a komponens-összeállítás indoklásnak kell gondoskodnia annak bizonyításáról, hogy a kiszolgáló komponens hogyan biztosítja az igényelt interfészt.

Ha a környezetfüggőségi információkban azonosított interfész szerepel a fejlesztési információk között, de ellentmondások lelhetők fel a leírások között, akkor további elemzésre van szükség. Az értékelő beazonosítja a kiszolgáló komponens használatában felmerülő különbségeket a kiszolgáló komponens értékelése és az összetett TOE értékelés alapján. Az értékelő tesztelés végrehajtását állapítja meg (az „összetett TOE tesztelése" (ACO_CTT) végrehajtása során) az interfész tesztelése céljából.

A kiszolgáló és a kliens komponensek összetett TOE-beli javítási állapotát (patch-ek alkalmazását) össze kell vetni a komponens értékelések során fennálló komponens frissítési státuszokkal. Ha bármilyen patch-et alkalmaztak a komponensekre, akkor a komponens-összeállítás indoklásban szerepeltetni kell a javítások információit, ideértve az értékelt komponens SFR-jeire gyakorolt minden lehetséges hatást. Az értékelőnek mérlegelnie kell a megadott módosításokat, és ellenőriznie kell a komponens SFR-ekre gyakorolt lehetséges

következmények pontosságát. Az értékelőnek ezután meg kell vizsgálnia, hogy a javítások által bevezetett módosításokat ellenőriznie kell-e teszteléssel, valamint azonosítania kell a szükséges tesztelési módszert. A tesztelés elvégezhető a komponens értékelés során elvégzett megfelelő értékelői/fejlesztői tesztelések megismétlésével, vagy az értékelő elrendelhet új teszteket a módosított komponens helyes működésének ellenőrzésére.

Amennyiben az egyedi komponensek garancia folytonossági tevékenység tárgyát képezték a komponens értékelés befejezése óta eltelt időszakban, az értékelő mérlegelje a garancia folytonosság tevékenység során felmért módosításokat az összetett TOE-ra vonatkozó független sebezhetőségi elemzés során (ACO_VUL).

6.2.3.3.1.2. Útmutatók

Az összetett TOE-ra vonatkozó útmutatók nagy eséllyel hivatkoznak az egyedi komponensek útmutatóira. Az elvárt minimális útmutató, hogy azonosítva legyen a kliens és kiszolgáló komponensek útmutatóinak alkalmazásához a sorrendi függőség, különös tekintettel az összetett TOE előkészületi (telepítési) szakaszára.

Az előkészítő eljárások (AGD_PRE) és „üzemeltetési felhasználói útmutató” (AGD_OPE) családok összetett TOE-ra vonatkozó alkalmazásán kívül vizsgálni kell a komponensek és az összetett TOE útmutatóit ellentmondás-mentesség szempontjából, és jelezni kell minden eltérést.

Ha az összetett TOE útmutató hivatkozik a kiszolgáló és kliens komponensek útmutató dokumentációira, akkor az ellentmondás-mentesség mérlegelése az egyes komponensekhez adott útmutatók közötti konzisztenciára korlátozódik (a kiszolgáló és a kliens komponens útmutatói közötti ellentmondás-mentességre). Ha azonban az összetett TOE-ra további útmutatókat is készítettek, akkor alaposabb elemzésre van szükség, hiszen a komponensekhez készített és az összetett TOE-ra vonatkozó útmutató dokumentációk közötti ellentmondás-mentességet is garantálni kell.

Ekkor az ellentmondás-mentesség azt jelenti, hogy az útmutató vagy ugyanaz, vagy további megszorításokat szab az egyedi komponensekre azok integrálása esetére, hasonló módon a funkcionális/garanciális összetevők pontosítási módjához.

A rendelkezésre álló információk segítségével (melyeket a „fejlesztési bizonyíték” (ACO_DEV) használ bemenetként) az értékelő képes lehet annak megállapítására, hogy a komponens értékelés során specifikált kiszolgáló komponens konfigurációtól való eltérések milyen lehetséges következményekkel járnak. Magas EAL-ok esetén azonban (amikor a kiszolgáló komponens értékelés tartalmazta a „TOE terv” (ADV_TDS) követelményeket) előfordulhat, hogy az útmutató módosításainak lehetséges kihatásai nem határozhatók meg teljes mértékben, - hacsak az összetett TOE-hoz nem bocsátják rendelkezésre a fejlesztési információ részeként a részletes tervezési leírásokat-, mivel a belső részletek nem ismertek. Ekkor az értékelőnek jelentést kell írnia a maradvány kockázatokról.

Ezeket a maradvány kockázatokat szerepeltetni kell az összetett TOE-ről szóló minden nyilvános értékelési jelentésben.

Az értékelőnek rögzítenie kell az útmutatók eltéréseit, ami az értékelő független tesztelési tevékenység („összetett TOE tesztelése”, ACO_CTT) bemenete lesz.

Az összetett TOE útmutatója kiegészítheti a komponensek útmutatóit, elsősorban a telepítésre, illetve a kiszolgáló és kliens komponens telepítési lépéseinek egymáshoz viszonyított végrehajtási sorrendjére vonatkozóan. Az egyedi komponensekre nézve a telepítési lépések sorrendje nem módosulhat, azonban előfordulhat a lépések összefésülésének szükségessége. Az értékelő vizsgálja meg az útmutatót, hogy az továbbra is teljesíti-e a komponensek értékelése során végrehajtott AGP_PRE tevékenység követelményét.

Előfordulhat olyan eset, hogy a környezetfüggőségi információ a kiszolgáló komponens olyan TSFI-n kívüli interfészeit is azonosítja, amelyekre a környezetfüggőségi információ szerint a kliens komponens hagyatkozik. A kiszolgáló komponens ilyen további interfészeihez útmutatóra lehet szükség. Feltéve, hogy az összetett TOE felhasználója megkapja a kiszolgáló komponensre vonatkozó útmutató dokumentációt, a kiszolgáló komponens AGP_PRE és AGP_OPE döntéseinek eredményei újrahasználhatók azokra az interfészekre, melyeket a kiszolgáló komponens értékelése során vizsgáltak. Azonban, ha a kliens komponens egyéb interfészeket is használ, az értékelőnek meg kell állapítania, hogy a kiszolgáló komponens útmutató dokumentációja megfelel-e az AGP_PRE és AGP_OPE követelményeinek, ahogyan azokat a kiszolgáló komponens értékelése során alkalmazták.

A kiszolgáló komponens értékelés során vizsgált interfészekre, vagyis amelyekre már igazolt a garancia, az értékelő győződjön meg arról, hogy az összetett TOE minden egyes interfész használati leírása összhangban van-e a kiszolgáló komponensnél írtakkal. Ennek megállapításához az értékelőnek minden interfész esetén végre kell hajtania egy leképezést az összetett TOE és a kiszolgáló komponens útmutatóira. Az értékelő ezután hasonlítsa össze az útmutatókat az ellentmondás-mentesség megállapításához.

Példák összetett TOE útmutatóban megadott olyan egyéb megszorításokra, melyeket vizsgálni kell abból a szempontból, hogy összhangban vannak-e a komponens útmutatóval (egy adott komponens útmutatót követi egy összetett TOE útmutató példa, ami további megszorításnak tekintendő):

- Komponens: A jelszó hosszt minimum 8 karakter hosszúra kell beállítani, és tartalmaznia kell alfabetikus és numerikus karaktereket.
- Összetett TOE: A jelszó hosszt minimum 10 karakter hosszúra kell beállítani, és tartalmaznia kell alfabetikus és numerikus karaktereket, és legalább egyet a következő speciális karakterekből: ( ) { } ^ < > -_
- Megjegyzés: A jelszóhosszt csak növelni lehet [egész szám>8] karakterre, míg az alfabetikus és numerikus karakterek használatának elhagyása csak akkor elfogadható, ha ugyanolyan vagy magasabb mértéket ér el az erősségi besorolás (figyelembe véve a jelszó találgatás valószínűségét).
- Komponens: A következő szolgáltatásokat le kell tiltani a registry beállításokban: WWW Publishing Service és ICDBReporter Service.
- Összetett TOE: A következő szolgáltatásokat le kell tiltani a registry beállításokban: WWW Publishing Service és ICDBReporter Service, Remote Procedure Call (RPC) Locator and Procedure Call (RPC) Service

— Komponens: Válassza ki a következő tulajdonságokat a biztonsági naplóállományban való szerepeltetéshez: dátum, idő, esemény típusa, szubjektum azonosítója, siker/sikertelenség.
— Összetett TOE: Válassza ki a következő tulajdonságokat a biztonsági naplóállományban való szerepeltetéshez: dátum, idő, esemény típusa, szubjektum azonosítója, siker/sikertelenség, esemény szövege és folyamat szál.

Amennyiben az összetett TOE útmutató eltér a kiszolgáló komponensétől (nem pontosítása annak), az értékelő mérje fel az útmutató változásainak lehetséges kockázatait. Ehhez használja a rendelkezésre álló információt (ideértve a nyilvánosan elérhető információkat, a kiszolgáló komponens nyilvánosan elérhető értékelési jelentésében (tanúsítási jelentésben) szereplő architektúra leírást, valamint az útmutató egyéb részeit), azért, hogy azonosítani tudja az útmutató módosításainak az összetett TOE SFR-jeire gyakorolt valószínű hatását.

Amennyiben a kliens komponens értékelése során a próbatelepítés a kiszolgáló komponenst használta a környezeti követelmények teljesítésére, akkor az összetett TOE-ra vonatkozó ezen munkaegység teljesítettnek tekinthető. Ha nem a kiszolgáló komponenst használták az AGD_PRE.1-3 munkaegység kielégítésére a kliens komponens értékelése folyamán, akkor az értékelő alkalmazza az összetett TOE-hoz biztosított felhasználói eljárásokat az összetett TOE előkészítéséhez, ahogyan azt az AGD_PRE.1-3-ban megadott útmutató leírja. Ez lehetővé teszi az értékelő számára annak megállapítását, hogy az összetett TOE-hoz készített előkészítő útmutató kielégítő-e az összetett TOE és annak működési környezete biztonságos előkészítéséhez.

6.2.3.3.1.3. Életciklus - Szállítás

Ha az összetett TOE esetén különböző szállítási mechanizmusokat alkalmaznak (azaz nem a komponensek értékelése során definiált és értékelt biztonságos szállítási eljárásoknak megfelelően juttatják el a komponenseket a felhasználóhoz), akkor az összetett TOE szállítási eljárásait a komponens értékelések során alkalmazott „szállítás” (ALC_DEL) követelményei szerinti értékelésnek kell alávetni.

Az összetett TOE szállítható integrált termékként vagy a komponenseket külön is lehet szállítani.

Ha a komponenseket külön-külön szállítják, akkor a kiszolgáló és kliens komponensek szállítás értékelési eredményei újrahasználhatók. A kiszolgáló komponensek szállítását a kliens komponens értékelői próbatelepítése során ellenőrzik a kiszolgáló komponens útmutatója alapján, alkalmazva a vonatkozó útmutatókat és a szállítást ellenőrző szempontokat, ami a felhasználó felelőssége.

Ha az összetett TOE-t egy egységként szállítják, akkor ennek szállítási eljárásait az összetett TOE értékelési tevékenység részeként kell vizsgálni.

Az összetett TOE elemeinek szállítási eljárásaira vonatkozó értékelést a TOE komponensekre alkalmazott „szállítás” (ALC_DEL) módszertan szerint kell elvégezni, biztosítva, hogy minden további elemet (például kiegészítő útmutatók az összetett TOE-ra) figyelembe vesznek a szállítási eljárásokban.

6.2.3.3.1.4. Életciklus - CM képességek

Az ALC_CMC.1 értékelési altevékenység vizsgálja az összetett TOE egyedi azonosítását, az ALC_CMS.2 értékelési altevékenység pedig azokat az elemeket, melyek az összetett TOE-t alkotják.

Bár az összetett TOE-ra kiegészítő útmutatók készíthetők, ezen útmutató egyedi azonosítása (az ALC_CMC.1 során az összetett TOE egyedi azonosításának részeként) elegendő az útmutató kezeléséhez.

A fennmaradó (fentebb nem vizsgált) ALC osztály (Életciklus támogatás) tevékenységek során hozott döntések újrahasználhatók a kiszolgáló komponens értékeléséből, mivel az összetett TOE integrálása során nem történik további fejlesztés.

A fejlesztés biztonságára nézve nincsenek további szempontok, mivel az integráció vélhetően a felhasználó telephelyén történik, vagy (ha az összetett TOE-t egy egységként szállítják) a kliens komponens fejlesztői telephelyén. A felhasználó telephelye a CC hatókörén kívül esik. Akkor sincsenek további követelmények vagy útmutatók, ha az integrálás ugyanott történik, mint a kliens komponens kialakítása, mivel minden komponens az összetett TOE konfiguráció elemeinek számít, és ezért mindenképp a kliens komponens fejlesztés biztonsági eljárásai értelmében kell vizsgálni.

Az integrálás során alkalmazott eszközök és technikák vizsgálata a kliens komponens fejlesztője által szolgáltatott bizonyítékok segítségével történik. A kiszolgáló komponens szempontjából lényeges összes eszköz/technika ellenőrzését a kiszolgáló komponens értékelése során kell végrehajtani. Például, ha a kiszolgáló komponenst forráskód formájában szállítják, és a felhasználónak kell fordítania, összeszerkesztenie (például az integrációt végző kliens komponens fejlesztőjének), a fordítóprogramot a kiszolgáló komponens értékelése során specifikálni és értékelni kellett, csakúgy, mint a vonatkozó paramétereket.

Az összetett TOE-ra vonatkozóan nincs életciklus definíció, mivel az elemeket nem fejlesztik tovább.

Egy komponens hibajavításának eredményei nem vonatkoznak az összetett TOE-ra. Ha az összetett TOE esetén belevették a garanciacsomagba a hibajavítást, akkor a „hibajavítás” (ALC_FLR) követelményeket kell alkalmazni az összetett TOE értékelése során (mint minden szigorításnál).

6.2.3.3.1.5. Tesztek

Az összetett TOE tesztelése a kliens komponens értékelésekor végzett „tesztelés” (ATE) tevékenység végrehajtása során fog megtörténni, mivel a kliens komponens teszteléséhez használt konfigurációnak magába kellett foglalnia a kiszolgáló komponenst abból a célból, hogy teljesüljenek a működési környezetre vonatkozó követelmények. Ha a kiszolgáló komponenst nem használták a kliens komponens teszteléséhez a kliens értékelése során, vagy az értékelt konfigurációhoz képest bármelyik komponens konfigurációja megváltozott, akkor az összetett TOE-ra meg kell ismételni a kliens komponens értékelésekor végrehajtott fejlesztői tesztet az ATE osztály követelményeinek kielégítése céljából.

6.2.3.4. Szigorú interfész tesztelés (ACO_CTT.2) értékelése

Ennek az altevékenységnek a célja annak meghatározása, hogy a fejlesztő jól hajtotta-e végre és dokumentálta-e a teszteket a kiszolgáló komponens azon interfészeire, amelyeket a kliens komponens a működése során meghív. Ennek az elemzésnek a részeként az értékelő megismétli a fejlesztői tesztek egy részét, és további teszteket végez, hogy meggyőző módon garantálni lehessen az összetett TOE és a kliens komponens által használt kiszolgáló komponens interfészeinek elvárt működését.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) a tesztelésre alkalmas összetett TOE,
b) az összetett TOE tesztelési bizonyítéka,
c) a környezetfüggőségi információ,
d) a fejlesztési információ.

6.2.3.4.1. Az ACO_CTT.2.1E értékelői akció

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

ACO_CTT.2.1C Az összetett TOE és a kiszolgáló komponens interfész tesztelési dokumentációjának tartalmaznia kell a tesztelési terveket, az elvárt teszteredményeket és a tényleges (kapott) teszteredményeket.

ACO_CTT.2-1 Az értékelőnek meg kell vizsgálnia az összetett TOE tesztelési dokumentációját annak megállapítása érdekében, hogy az tartalmazza-e a tesztelési tervet, a várt teszteredményeket és a tényleges, kapott eredményeket.

Ez a munkaegység teljesíthető a kliens komponens értékeléséből származó tesztelési bizonyítékok által, ha a kiszolgáló komponenst használták a kliens komponens működési környezetére vonatkozó IT követelmények kielégítésére.

Az ATE_FUN.1.1E kielégítéséhez szükséges minden munkaegység alkalmazandó annak meghatározásához, hogy:

a) a tesztelési dokumentáció tartalmazza a tesztelési tervet, a várt teszteredményeket és a tényleges, kapott eredményeket;
b) a tesztelési dokumentáció tartalmazza a tesztek megismételhetőségéhez szükséges információkat;
c) a kiszolgáló komponens tesztelésére fordított fejlesztői munka mennyiségét/szintjét.

ACO_CTT.2-2 Az értékelőnek meg kell vizsgálnia a kiszolgáló komponens interfész tesztelési dokumentációját, annak megállapítása érdekében, hogy az tartalmazza-e a tesztelési tervet, a várt teszteredményeket és a ténylegesen kapott eredményeket.

Ez a munkaegység teljesíthető a kiszolgáló komponens értékeléséből származó tesztelési bizonyítékok által, azon interfészek esetén, amelyeket az összetett TOE-ban a kliens komponens használ, és a kiszolgáló komponens sikeres értékelése során a TSFI részét képezték. Annak megállapítására, hogy a kiszolgáló komponens interfészei, melyeket a kliens használ, valóban a TSFI részei voltak-e, az ACO_COR tevékenység végrehajtása során kerül sor.

Az ATE_FUN.1.1E kielégítéséhez szükséges minden munkaegység alkalmazandó annak meghatározásához, hogy:

a) a tesztelési dokumentáció tartalmazza a tesztelési tervet, a várt teszteredményeket és a tényleges, kapott eredményeket;
b) a tesztelési dokumentáció tartalmazza a tesztek megismételhetőségéhez szükséges információkat;
c) a kiszolgáló komponens tesztelésére fordított fejlesztői munka mennyiségét/szintjét.

ACO_CTT.2.2C Az összetett TOE tesztek fejlesztő által történt elvégzéséből származó tesztelési dokumentációnak meg kell mutatnia, hogy a TSF a specifikáltnak megfelelően működik és teljes.

ACO_CTT.2-3 Az értékelőnek meg kell vizsgálnia a tesztelési dokumentációt, annak megállapítása érdekében, hogy az megadja-e a az összetett TOE tesztelésével kapcsolatos tesztelési dokumentációban lévő tesztek és az összetett TOE biztonsági előirányzatában szereplő összetett TOE SFR-ek közötti megfeleltetést.

A tesztelési megfeleltetés bizonyításához elegendő egy egyszerű kereszttábla. A tesztelési dokumentációban megadott tesztek és az SFR-ek közötti megfeleltetésnek egyértelműnek kell lennie.

ACO_CTT.2-4 Az értékelőnek meg kell vizsgálnia a tesztelési dokumentációt, annak megállapítása érdekében, hogy a fejlesztő által végrehajtott összetett TOE tesztek megmutatják-e, hogy a TSF a specifikációnak megfelelően működik.

E munkaegységhez útmutató található:

a) 7.1 fejezetben és
b) 7.2 fejezetben.

A tesztek sikeres végrehajtásából származó kimenetek (ATE_FUN.1.3C számára) összehasonlíthatók a leképezéssel annak megállapítása érdekében, hogy az összetett TOE SFR-ek –ahogyan azokat a fejlesztő tesztelte- az elvárt módon működnek-e.

ACO_CTT.2.3C A kiszolgáló komponens interfész tesztek fejlesztő által történt elvégzéséből származó tesztelési dokumentációnak meg kell mutatnia, hogy a kliens komponens által használt kiszolgáló komponens interfész a specifikáltnak megfelelően működik és teljes.

ACO_CTT.2-5 Az értékelőnek meg kell vizsgálnia a tesztelési dokumentációt, annak megállapítása érdekében, hogy az megadja-e a kliens komponens által használt kiszolgáló komponens interfészek tesztelésével kapcsolatos dokumentációban lévő tesztek és a környezetfüggőségi információk között specifikált interfészek közötti megfeleltetést.

A tesztelési megfeleltetés bizonyításához elegendő egy egyszerű kereszttábla. A tesztelési dokumentációban megadott tesztek és az interfészek közötti megfeleltetésnek egyértelműnek kell lennie.

ACO_CTT.2-6 Az értékelőnek meg kell vizsgálnia a tesztelési dokumentációt, annak megállapítása érdekében, hogy a fejlesztő által végrehajtott kiszolgáló komponens interfész tesztek megmutatják-e, hogy a kliens komponens által használt kiszolgáló komponens interfészek a specifikációnak megfelelően működnek.

E munkaegységhez útmutató található:

a) 7.1 fejezetben és
b) 7.2 fejezetben.

A tesztek sikeres végrehajtásából származó kimenetek (ATE_FUN.1.3C számára) összehasonlíthatók a leképezéssel annak megállapítása érdekében, hogy kiszolgáló komponens interfészei –ahogyan azokat a fejlesztő tesztelte- az elvárt módon működnek-e.

ACO_CTT.2.4C A kiszolgáló komponensnek tesztelésre alkalmasnak kell lennie.

ACO_CTT.2-7 Az értékelőnek meg kell vizsgálnia az összetett TOE-t, annak megállapítása érdekében, hogy azt megfelelő módon telepítették-e, és az ismert állapotok egyikében van-e.

Annak megállapítása, hogy az összetett TOE-t megfelelően telepítették, és az ismert állapotok valamelyikében van-e, az ATE_IND.2-1 és ATE_IND.2-2 munkaegységek feladata, aminek keretében a fejlesztő által tesztelésre átadott TOE-t vizsgálják.

ACO_CTT.2-8 Az értékelőnek meg kell vizsgálnia a fejlesztő által biztosított erőforrás együttest, annak megállapítása érdekében, hogy azok megegyeznek-e a kiszolgáló komponens funkcionális teszteléséhez a kiszolgáló komponens fejlesztője által használt erőforrásokkal.

Annak megállapítása, hogy a biztosított erőforrások megegyeznek a kiszolgáló komponens összetett TOE-beli használata szerinti funkcionális teszteléséhez használt erőforrásokkal, az ATE_IND.2-3 munkaegység hatásköre.

6.2.3.4.2. Az ACO_CTT.2.2E értékelői akció

ACO_CTT.2.2E Az értékelőnek végre kell hajtania a tesztelési dokumentációban szereplő tesztek egy mintáját a fejlesztői teszteredmények ellenőrzése céljából.

ACO_CTT.2-9 A tesztek kiválasztását és végrehajtását az ATE_IND.2.2E-vel összhangban kell elvégezni, bizonyítandó, hogy az összetett TOE biztonsági előirányzatban specifikált SFR-ek megfelelően működnek.

Az értékelőnek az ATE_IND.2.2E kielégítéséhez szükséges összes munkaegységet alkalmaznia kell, és az összetett TOE ETR-ben rögzítenie kell a kapcsolódó munkaegységek által előírt minden vizsgálatot, kapott eredményt és döntést.

6.2.3.4.3. Az ACO_CTT.2.3E értékelői akció

ACO_CTT.2.3E Az értékelőnek le kell tesztelnie az összetett TOE TSF interfészeinek egy részhalmazát, hogy meggyőződjön arról, hogy az összetett TSF a specifikáltnak megfelelően működik.

ACO_CTT.2-10 Az értékelőnek az ATE_IND.2.3E szerinti tesztelést kell végeznie az összetett TOE biztonsági előirányzatában megadott SFR-ek részhalmazára, azt bizonyítandó, hogy a TSF a specifikációnak megfelelően működik.

Az értékelőnek alkalmaznia kell az ATE_IND.2.3E kielégítéséhez szükséges minden munkaegységet, és rögzítenie kell az összetett TOE ETR-ben minden előírt vizsgálatot, eredményt és döntést.

Amikor az összetett TOE TSF interfészeinek tesztelésre való kiválasztása történik, az értékelőnek figyelembe kell vennie minden olyan módosítást, amely a komponensekben az értékelt verzió vagy konfiguráció óta történt. Ez jelenthet javításokat, a módosított útmutató dokumentációk miatti eltérő konfigurálást, a komponens TSF-jébe nem eső egyéb komponens elemektől való környezeti függőséget. Ezeket a módosításokat a „komponens-összeállítás indoklás” (ACO_COR) tevékenység során kell azonosítani.

ACO_CTT.2-11 Az értékelőnek az ATE_IND.2-nek megfelelően tesztelést kell végeznie a kiszolgáló komponens interfészeinek egy részhalmazára, hogy azok a specifikáltak szerint működnek-e.

Az értékelőnek az ATE_IND.2.3E kielégítéséhez szükséges összes munkaegységet alkalmaznia kell, és az összetett TOE ETR-ben rögzítenie kell a kapcsolódó munkaegységek által előírt minden vizsgálatot, kapott eredményt és döntést.

Amikor a kiszolgáló komponens interfészeinek tesztelésre való kiválasztása történik, az értékelőnek figyelembe kell vennie minden olyan módosítást, amely a kiszolgáló komponensben az értékelt verzió vagy konfiguráció óta történt. Az értékelőnek külön figyelmet kell fordítania a tesztek kidolgozására, hogy azok megmutassák a kiszolgáló komponens azon interfészeinek helyes működését, amelyeket nem vizsgáltak a kiszolgáló komponens értékelése során. Ezeket az egyéb interfészeket és más módosításokat a „komponens-összeállítás indoklás” (ACO_COR) tevékenység során kell azonosítani.

6.2.3.5. Kompozíció sebezhetőség elemzés (ACO_VUL.2) értékelése

Ezen altevékenység célja annak megállapítása, hogy az összetett TOE-nek, működési környezetében vannak-e alap támadási képességgel kihasználható sebezhetőségei.

A fejlesztő elkészíti a komponensekre vonatkozó és a kiszolgáló-kliens viszonylatban felmerülő maradvány sebezhetőségekkel kapcsolatos elemzést. Az értékelő kutatásokat végez a nyilvánosan hozzáférhető forrásokban, hogy azonosítson minden lehetséges új, a komponenseket fenyegető sebezhetőséget (a komponensek értékelésének befejezése óta felmerült sebezhetőségeket). Az értékelő ezen kívül egy független sebezhetőség elemzést és behatolás tesztelést hajt végre az összetett TOE-ra.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) a tesztelésre alkalmas összetett TOE,
b) az összetett ST,
c) a komponens-összeállítás indoklás,
d) a környezetfüggőségi információ,
e) az útmutató dokumentáció,
f) nyilvánosan elérhető információ a lehetséges biztonsági sebezhetőségek meghatározásának támogatására,
g) az összes komponens értékelése során jelentett maradvány sebezhetőségek.

6.2.3.5.1. 6.2.3.5.1 Az ACO_VUL.2.1E értékelői akció

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

ACO_VUL.2.1C Az összetett TOE-nak tesztelésre alkalmasnak kell lennie.

ACO_VUL.2-1 Az értékelőnek meg kell vizsgálnia az összetett TOE-t, annak megállapítása érdekében, hogy azt megfelelő módon telepítették-e, és az ismert állapotok egyikében van-e.

Annak megállapítása, hogy az összetett TOE-t megfelelően telepítették-e, és az ismert állapotok valamelyikében van-e, az összetett TOE-ra vonatkozó ATE_IND.2-1 és ATE_IND.2-2 munkaegységek feladata.

Ha a garanciacsomag tartalmazza az ACO_CTT családot, akkor az értékelő hivatkozhat az „összetett TOE tesztelése” (ACO_CTT)*-1 eredményére, hogy az teljesül.

ACO_VUL.2-2 Az értékelőnek meg kell vizsgálnia az összetett TOE konfigurációt annak megállapítása érdekében, hogy az ST-ben szereplő, a komponensekre vonatkozó bármilyen feltételezést és célt, amely IT entitásokkal kapcsolatos, más komponensek kielégítenek.

A komponens ST-je tartalmazhat feltételezéseket más komponensekkel kapcsolatban, amelyek használhatják az ST-vel kapcsolatos komponenst; például egy kiszolgáló komponensként alkalmazott operációs rendszerre vonatkozó ST tartalmazhat olyan feltételezést, hogy a rajta működő bármilyen alkalmazás ne fusson privilegizált módban. Ezek a feltételezések és célok az összetett TOE más komponensei által teljesítendők.

6.2.3.5.2. Az ACO_VUL.2.2E értékelői akció

ACO_VUL.2.2E Az értékelőnek végre kell hajtania egy vizsgálatot annak megállapítása érdekében, hogy a kiszolgáló és a kliens komponensre beazonosított bármilyen maradvány sebezhetőség nem aknázható ki az összetett TOE-ban, annak működési környezetében.

ACO_VUL.2-3 Az értékelőnek meg kell vizsgálnia a kiszolgáló komponens értékeléséből származó maradvány sebezhetőségeket annak megállapítása érdekében, hogy azok nem kiaknázhatók-e az összetett TOE működési környezetében.

A kiszolgáló komponens értékelés során a termékre felismert sebezhetőségek listáját – melyeket a kiszolgáló komponensben nem kihasználhatónak ítéltek – kell használni ennek a tevékenységnek a bemeneteként. Az értékelő állapítsa meg, hogy azok a feltételek, amelyek alapján a sebezhetőséget nem kihasználhatónak ítélték, fennállnak-e az összetett TOE-ra, vagy a komponens-összeállítás miatt felmerülhet az adott sebezhetőség kiaknázhatósága. Például, ha a kiszolgáló komponens értékelése során felételezték, hogy egy bizonyos operációs rendszer szolgáltatás le van tiltva, ami viszont engedélyezett az összetett TOE értékelésben, akkor az ehhez a szolgáltatáshoz kapcsolódó bármilyen lehetséges sebezhetőséget, amelyet korábban kizártak, most figyelembe kell venni.

Továbbá, a kiszolgáló komponens értékeléséből származó ismert, nem kihasználható sebezhetőségeket is figyelembe kell venni a többi komponenssel (pl. kliens komponenssel) kapcsolatos minden ismert, nem kihasználható sebezhetőség ismeretében az összetett TOE-n belül. Ez azt az esetet fedi le, amikor egy lehetséges sebezhetőség, ami elszigetelve nem kihasználható volt, egy másik -potenciális sebezhetőséget tartalmazó- IT egyeddel való integrálás után kiaknázhatóvá válik.

ACO_VUL.2-4 Az értékelőnek meg kell vizsgálnia a kliens komponens értékeléséből származó maradvány sebezhetőségeket annak megállapítása érdekében, hogy azok nem kihasználhatók-e az összetett TOE működési környezetében.

A kliens komponens értékelés során a termékre felismert sebezhetőségek listáját –melyeket a kliens komponensben nem kihasználhatóknak ítéltek – kell használni ennek a tevékenységnek a bemeneteként. Az értékelő állapítsa meg, hogy azok a feltételek, amelyek alapján a sebezhetőséget nem kihasználhatónak ítélték, fennállnak-e az összetett TOE-ra, vagy a komponens-összeállítás miatt felmerülhet az adott sebezhetőség kiaknázhatósága. Például, ha a kliens komponens értékelése során azt felételezték, hogy a működési környezet követelményeit kielégítő IT-egyed nem ad vissza egy bizonyos értéket egy szolgáltatás kérésre, amelyet az összetett TOE-ban a kiszolgáló komponens most visszaad, akkor az ehhez a visszatérési értékhez kapcsolódó, korábban kizárt bármilyen lehetséges sebezhetőséget újra figyelembe kell venni.

Továbbá, a kliens komponens értékeléséből származó ismert, nem kihasználható sebezhetőségeket is figyelembe kell venni a többi komponenssel (pl. kiszolgáló komponenssel) kapcsolatos minden ismert, nem kihasználható sebezhetőség ismeretében az összetett TOE-n belül. Ez azt az esetet fedi le, amikor egy lehetséges sebezhetőség, ami elszigetelve nem kihasználható volt, egy másik -potenciális sebezhetőséget tartalmazó- IT egyeddel való integrálás után kiaknázhatóvá válik.

6.2.3.5.3. Az ACO_VUL.2.3E értékelői akció

ACO_VUL.2.3E Az értékelőnek kutatnia kell a nyilvánosan hozzáférhető forrásokat a kiszolgáló és a kliens komponensnek az összetett TOE működési környezetében való használatából származó lehetséges sebezhetőségeinek feltárása céljából.

ACO_VUL.2-5 Az értékelőnek meg kell vizsgálnia a nyilvánosan hozzáférhető információforrásokat annak érdekében, hogy azonosítani lehessen a kiszolgáló komponensben azokat a lehetséges biztonsági sebezhetőségeket, amelyek a kiszolgáló komponens értékelésének befejezése óta váltak ismertté.

Az értékelőnek fel kell használnia a nyilvánosan hozzáférhető információkat –ahogyan azt a [3]-beli AVA_VAN.2-2 leírja- a kiszolgáló komponens sebezhetőségeinek feltárása céljából.

Nem kell tovább vizsgálni azokat a lehetséges sebezhetőségeket, amelyek a kiszolgáló komponens értékelése előtt már nyilvánosan ismertek voltak, kivéve, ha nyilvánvaló az értékelő számára, hogy a szóban forgó sebezhetőség kiaknázásához szükséges támadás képesség jelentős mértékben csökkent. Ez bekövetkezhet a kiszolgáló komponens értékelése óta megjelent új technológia miatt, melynek alkalmazása egyszerűsíti a sebezhetőség kihasználását.

ACO_VUL.2-6 Az értékelőnek meg kell vizsgálnia a nyilvánosan hozzáférhető információforrásokat annak érdekében, hogy azonosítani lehessen a kliens komponensben azokat a lehetséges biztonsági sebezhetőségeket, amelyek a kliens komponens értékelésének befejezése óta váltak ismertté.

Az értékelőnek fel kell használnia a nyilvánosan hozzáférhető információkat –ahogyan azt a [3]-beli AVA_VAN.2-2 leírja- a kiszolgáló komponens sebezhetőségeinek feltárása céljából.

Nem kell tovább vizsgálni azokat a lehetséges sebezhetőségeket, amelyek a kliens komponens értékelése előtt már nyilvánosan ismertek voltak, kivéve, ha nyilvánvaló az értékelő számára, hogy a szóban forgó sebezhetőség kiaknázásához szükséges támadás képesség jelentős mértékben csökkent. Ez bekövetkezhet a kliens komponens értékelése óta megjelent új technológia miatt, melynek alkalmazása egyszerűsíti a sebezhetőség kihasználását.

ACO_VUL.2-7 Az értékelőnek rögzítenie kell az ETR-ben az azonosított lehetséges sebezhetőségeket, melyek szóba jönnek a tesztelésnél, és amelyek az összetett TOE működési környezetében kihasználhatóak lehetnek.

Az ST, az útmutató dokumentumok és a funkcionális specifikáció segítségével meg kell állapítani, hogy a sebezhetőségek valóban relevánsak-e az összetett TOE működési környezetében.

Az értékelő rögzítsen minden olyan indokot, ami miatt sebezhetőségek kizárhatók a további vizsgálatokból, ha úgy ítéli meg, hogy a sebezhetőség nem vonatkoztatható a működési környezetre. Egyébként pedig rögzítse a lehetséges sebezhetőségeket további mérlegelés, vizsgálat céljából.

Az összetett TOE-ra annak működési környezetében vonatkoztatható lehetséges sebezhetőségek listáját, ami a behatolás tesztelési tevékenység (ACO_VUL.2.5E) bemenete, az értékelőknek az ETR-ben meg kell adniuk.

6.2.3.5.4. Az ACO_VUL.2.4E értékelői akció

ACO_VUL.2.4E Az értékelőnek végre kell hajtania egy független sebezhetőség elemzést az összetett TOE-ra, az útmutató dokumentáció, környezetfüggőségi információ és komponens-összeállítás indoklás felhasználásával, az összetett TOE-ban fellelhető lehetséges sebezhetőségek azonosítására.

ACO_VUL.2-8 Az értékelőnek végre kell hajtania egy keresést az összetett TOE ST-n, az útmutató dokumentáción, a környezetfüggőségi információn és a komponens-összeállítás indoklásán, az összetett TOE lehetséges sebezhetőségeinek meghatározása céljából.

A független értékelői sebezhetőségi elemzésben a komponensek vizsgálata kissé eltérő formában történhet, mint ahogyan azt a [3]-beli AVA_VAN.2.3E leírja egy komponens értékelésére, mivel nem feltétlenül kell a garanciacsomag szempontjából fontos tervezési absztrakciós szintek minden rétegét megnézni. Ezeket a kiszolgáló komponens értékelése során már megvizsgálták, de a bizonyíték nem biztos, hogy rendelkezésre áll az összetett TOE értékeléshez. Azonban, a [3]-beli AVA_VAN.2.3E-hez kapcsolódó munkaegységekben leírt általános megközelítés alkalmazható, és az alapja az, hogy az összetett TOE-ban az értékelő lehetséges sebezhetőségek után kutat.

Az összetett TOE értékelésében használt egyedi komponensek sebezhetőségi elemzését már végrehajtották a komponensek értékelése során. Az összetett TOE értékelés során a sebezhetőségi elemzés középpontjában az áll, hogy feltáruljanak azok a sebezhetőségek, amelyek a komponensek integrálása miatt kerültek a rendszerbe, vagy a komponensek konfigurációjának valamilyen változása miatt: a komponens értékelés során megállapított konfiguráció más, mint az összetett TOE-ban használt.

Az értékelő a komponens konstrukció megértéséhez használja a kliens komponensre vonatkozó környezetfüggőségi információt, a kiszolgáló komponensre vonatkozó komponens-összeállítás indoklást és fejlesztési információt, valamint a kliens komponens terv információt. Ezek lehetővé teszik az értékelő számára, hogy megértse, hogyan működik együtt a kliens és a kiszolgáló komponens.

Az értékelőnek figyelembe kell vennie az összetett TOE telepítésére, indítására és működtetésére vonatkozó minden új útmutatót, hogy azonosítsa az ezek által bevezetett lehetséges sebezhetőségeket.

Ha az egyedi komponensek bármelyike is garancia folytonossági tevékenységen esett át a komponens értékelés befejeződése óta eltelt időszakban, akkor az értékelőnek számításba kell vennie a javításokat a független sebezhetőségi elemzés során. A módosításokkal kapcsolatos információk a garancia folytonossági tevékenységek nyilvános jelentésében szerepelnek (például karbantartási jelentés). Ez kiegészítendő az útmutató dokumentációk bármilyen frissítésével, ami a módosítások miatt történt, és olyan információkkal, amelyek a módosításokkal kapcsolatban nyilvánosan hozzáférhetők (például gyártó weboldala).

A bizonyíték hiánya miatt azonosított minden olyan kockázatot, amivel kapcsolatban nem állapítható meg a módosítások vagy a komponens konfigurációjának értékelt konfigurációtól való eltérésének teljes kihatása, dokumentálni kell az értékelői sebezhetőségi elemzésben.

6.2.3.5.5. Az ACO_VUL.2.5E értékelői akció

ACO_VUL.2.5E Az értékelőnek behatolás tesztelést kell végeznie, ami az azonosított sebezhetőségeken alapul, annak megmutatása céljából, hogy az összetett TOE ellenáll az alap támadási képességgel rendelkező támadó támadásainak.

ACO_VUL.2-9 Az értékelőnek végre kell hajtania a behatolás tesztelést, ahogyan azt a [3]-beli AVA_VAN.2.4E leírja.

Az értékelő a [3]-beli AVA_VAN.2.4E értékelői feladat teljesítése érdekében alkalmazza az összes szükséges munkaegységet, és az ETR-ben rögzítse az összetett TOE-ra elvégzett összes vizsgálatot és meghozott döntést, melyeket a munkaegységek előírnak.

Az értékelő a [3]-beli AVA_VAN.2.1E értékelői feladathoz is alkalmazza a munkaegységeket annak megállapítása érdekében, hogy a fejlesztő által biztosított összetett TOE alkalmas-e a tesztelésre.

6.2.4. Összetett TOE értékelése CAP-K esetén

6.2.4.1. Környezetfüggőségi információ (ACO_REL.2) értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a fejlesztői környezetfüggőségi bizonyíték kielégítő információt tartalmaz-e annak meghatározásához, hogy a kiszolgáló komponens biztosítja a szükséges funkcionalitást, illetve e funkciók meghívásának módszeréről. Ez a kliens és a kiszolgáló komponens közötti interfészek, illetve a kliens komponens által hívott interfészekből visszakapott értékek segítségével fejezhető ki.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az összetett ST,
b) a kliens komponens funkcionális specifikációja,
c) a kliens komponens terve,
d) a kliens komponens megvalósítási reprezentációja,
e) a kliens komponens architektúra terve,
f) a környezetfüggőségi információ.

Egy olyan kliens komponens, amelynek TSF-je együttműködik a kiszolgáló komponenssel, funkcionalitást vár el a kiszolgáló komponenstől (például távoli hitelesítés, távoli naplóadat tárolás). Ezekben az esetekben a hívott szolgáltatásokat le kell írni azok részére, akik a végfelhasználók számára konfigurálják az összetett TOE-t. E leírási követelmény oka, hogy segíteni kell az összetett TOE integrátorokat annak meghatározásában, hogy a kiszolgáló komponens mely szolgáltatásainak lehet kedvezőtlen (ártalmas) hatása a kliens komponensre, és információk álljanak rendelkezésre, amelyek alapján meg lehet állapítani a komponensek kompatibilitását a fejlesztési bizonyíték (ACO_DEV) család alkalmazása során.

6.2.4.1.1. Az ACO_REL.1.1E értékelői akció

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

ACO_REL.2.1C A környezetfüggőségi információnak le kell írnia a kiszolgáló komponens azon hardver, szoftver és/vagy förmver elemeinek funkcionalitását, melyre a kliens komponens TSF támaszkodik.

ACO_REL.2-1 Az értékelőnek ellenőriznie kell a környezetfüggőségi információt, annak megállapítása érdekében, hogy szerepel-e benne a kiszolgáló komponens hardverei, förmverei és/vagy szoftverei által nyújtott funkcionalitás leírása, amire a kliens komponens TSF-je épít a működése végrehajtása során.

Az értékelő vizsgálja meg annak a biztonsági funkcionalitásnak a leírását, amit a kliens komponens TSF-je igényel a kiszolgáló komponens hardver, szoftver, förmver elemeitől. A munkaegység fókuszában elsősorban e leírás részletessége álljon, és nem annyira az információ pontosságának ellenőrzése. (Ez utóbbira a következő munkaegység összpontosít).

A kiszolgáló komponens leírásának nem kell részletesebbnek lennie, mint egy komponens TSF leírás részletessége, ahogyan azt a TOE terv (ADV_TDS) megadja.

ACO_REL.2-2 Az értékelőnek meg kell vizsgálnia a környezetfüggőségi információt annak megállapítása érdekében, hogy az pontosan tükrözi-e a kliens komponens működtetési környezetére vonatkozó célokat.

A környezetfüggőségi információ tartalmazza a kliens komponens által használt kiszolgáló komponens biztonsági funkcionalitás leírását. Annak biztosítása érdekében, hogy a környezetfüggőségi információ összhangban legyen a kliens komponens működési környezetére vonatkozó elvárásaival, az értékelő hasonlítsa össze a környezetfüggőségi információt a kliens komponens ST-jében megadott környezeti biztonsági célok nyilatkozatával.

Például ha a környezetfüggőségi információban az szerepel, hogy a kliens komponens TSF-je a kiszolgáló komponens funkcióira épít a naplóadatok tárolása és védelme tekintetében, de egy másik értékelési bizonyíték (pl. a kliens komponens tervdokumentációja) egyértelművé teszi, hogy a kliens komponens TSF-je maga tárolja és védi a naplóadatokat, akkor ez pontatlanságot jelez.

Megjegyzendő, hogy a működtetési környezetre vonatkozó célok tartalmazhatnak nem IT eszközökkel kielégíthető célokat. A kiszolgáló komponenstől elvárt szolgáltatások leírhatók a kliens komponens ST-ben a működési környezetre vonatkozó IT biztonsági célokként, de az nem követelmény, hogy minden ilyen környezetre vonatkozó elvárás szerepeljen a környezetfüggőségi információ között.

ACO_REL.2.2C A környezetfüggőségi információnak le kell írnia minden kapcsolatot, amelyen át a kliens komponens TSF-je szolgáltatásokat kér a kiszolgáló komponenstől.

ACO_REL.2-3 Az értékelőnek meg kell vizsgálnia a környezetfüggőségi információt, annak megállapítása érdekében, hogy leírták-e benne a kliens és a kiszolgáló komponens közötti összes kölcsönhatást, mely kölcsönhatások révén a kliens komponens TSF-je szolgáltatásokat kér a kiszolgáló komponenstől.

A kliens komponens TSF-je kérhet olyan szolgáltatásokat a kiszolgáló komponenstől, amelyek nem voltak a kiszolgáló komponens TSF-jén belül. (Lásd B.3 függeléket, CC 3. részben: Összetett IT egyedek közötti kölcsönhatások).

A kiszolgáló komponens funkcionalitásával kapcsolatos interfészeket ugyanolyan szinten kell leírni, mint a kliens TSF funkcionalitását, amint azt a „TOE terv" (ADV_TDS.1) biztosítja az alrendszerek között.

A kliens és a kiszolgáló komponens közötti együttműködés leírásának célja annak megmutatása, hogy a kliens komponens TSF-je hogyan alapoz a kiszolgáló komponens szolgáltatásaira a saját biztonsági funkcionalitásának végrehajtása céljából. Ezeket a kölcsönhatásokat nem kell a megvalósítás szintjén jellemezni (pl. rutinok közötti paraméterátadás szintjén), de egy összetevő által használandó adott összetevőhöz meghatározott adatelemeket tartalmaznia kell e leírásnak. A leírásnak segítenie kell az olvasót annak általános megértésében, hogy miért van szükség az interakcióra.

Az interfészek pontossága és teljessége a kiszolgáló komponens által biztosítandó, TSF által kért biztonsági funkcionalitáson alapul, amint azt az ACO_REL.2-1 és ACO_REL.2-2 munkaegységek elemzik. Lehetséges, hogy a korábbi munkaegységekben leírt összes funkcionalitás leképezhető az ebben a munkaegységben azonosított interfészekre, és fordítva. Egy olyan interfész, ami nem tartozik leírt funkcióhoz, szintén pontatlanságot jelez.

ACO_REL.2.3C A környezetfüggőségi információnak le kell írnia minden egyes interakciót a használt interfész és az általa visszaadott értékek megadásával.

ACO_REL.2-4 A környezetfüggőségi információnak le kell írnia az egyes interakciókat a használt interfész és az interfész által visszaadott visszatérési értékek segítségével.

A kliens komponens által a kiszolgálótól való szolgáltatáskérés során használt interfészek azonosítása lehetővé teszi az integrátor számára annak megállapítását, hogy a kiszolgáló komponens biztosítja-e az összes vonatkozó interfészt. Ez az ismeret kiegészíthető a kliens komponens által elvárt visszatérései eredmények specifikációjából nyert információkkal. Az értékelő győződjön meg arról, hogy minden megadott interakcióra szerepelnek az interfész leírások (amiket az ACO_REL.2-3 vizsgált).

ACO_REL.2.4C A környezetfüggőségi információnak le kell írnia, hogy a kliens TSF hogyan védi magát a kiszolgáló komponens beavatkozásával és manipulálásával szemben.

ACO_REL.2-5 Az értékelőnek meg kell vizsgálnia a környezetfüggőségi információt, annak megállapítása érdekében, hogy szerepel-e benne az, hogy a kliens TSF hogyan védi meg magát a kiszolgáló komponenshez köthető beavatkozás és manipulálás ellen.

A beavatkozás és manipulálás elleni védelem módját az ADV_ARC.1-4-hez szükséges részletességgel kell biztosítani.

6.2.4.2. Részletes tervezési bizonyíték (ACO_DEV.3) értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy a kiszolgáló komponens a megfelelő biztonsági funkcionalitást nyújtja-e a kliens komponens számára. Ez a kiszolgáló komponens interfészeinek és a kapcsolódó biztonsági funkciók működésének arra irányuló vizsgálatával állapítható meg, hogy azok összhangban vannak-e a környezetfüggőségi információban specifikált, kliens komponens által igényelt interfészekkel.

Az interfész leíráson kívül le kell írni a kliens komponens által igényelt biztonsági funkcionalitást biztosító kiszolgáló alrendszereket, hogy az értékelő meg tudja határozni, hogy az interfész a kiszolgáló komponens TSF-elemét jelenti-e vagy sem.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:
a) az összetett ST,
b) a fejlesztési információ,
c) a környezetfüggőségi információ.

6.2.4.2.1. Az ACO_DEV.3.1E értékelői akció

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

ACO_DEV.3.1C A fejlesztési információnak le kell írnia az összetett TOE-ban használt kiszolgáló komponens minden egyes interfészére azok célját és használati módját.

ACO_DEV.3-1 Az értékelőnek meg kell vizsgálnia a fejlesztési információt, annak megállapítása érdekében, hogy az leírja-e az egyes interfészek célját.

A kiszolgáló komponens interfészeket biztosít a kliens komponenssel való együttműködéshez a kliens TSF működésének támogatásához. Az egyes interfészek célját ugyanolyan szinten kell leírni, mint a kliens komponens TSF funkcionalitásához szükséges interfészeket, ahogyan azokat a TOE tervben az alrendszerek között meg kell adni (ADV_TDS.1). Ez a leírás teszi lehetővé az olvasó számára annak megismerését, hogy a kiszolgáló komponens hogyan biztosítja a kliens komponens TSF-je által igényelt szolgáltatásokat.

Ez a munkaegység teljesíthető a kiszolgáló komponens TSFI interfészeire vonatkozó funkcionális specifikáció biztosításával.

ACO_DEV.3-2 Az értékelőnek meg kell vizsgálnia a fejlesztési információt, annak megállapítása érdekében, hogy az leírja-e az egyes interfészek használati módját.

Az interfészek használati módja azt összegzi, hogy az interfészt hogyan kell alkalmazni a műveletek kezdeményezéséhez és az eredmények fogadásához. Az értékelőnek meg kell tudni

határozni a fejlesztési információ ezen része alapján, hogy az egyes interfészeket hogyan kell használni. Ez nem feltétlenül jelenti, hogy minden egyes interfészre külön módszer van, például általánosan is leírható, hogy API hívásokat hogyan kell kezdeményezni, és ezen általános formával azonosíthatók az egyes interfészek.

Ez a munkaegység teljesíthető a kiszolgáló komponens TSFI interfészeire vonatkozó funkcionális specifikáció biztosításával.

ACO_DEV.3.2C A fejlesztési információnak azonosítania kell a kiszolgáló komponens azon alrendszereit, amelyek az összetett TOE-ban használt kiszolgáló komponens interfészeket biztosítják.

ACO_DEV.3-3 Az értékelőnek meg kell vizsgálnia a fejlesztési információt, annak megállapítása érdekében, hogy a kliens komponens számára interfészeket biztosító kiszolgáló összes alrendszert azonosították-e.

A kiszolgáló komponens TSFI-jének részét képező interfészek esetén az interfészhez tartozó alrendszerek lesznek a kiszolgáló komponens értékelés során a „TOE terv” (ADV_TDS) tevékenységben vizsgált alrendszerek. Azokat az interfészeket, amelyeket a kliens komponens használ, de nem képezik a kiszolgáló komponens TSFI részét, a kiszolgáló komponens TSF-jén kívüli alrendszerekre kell leképezni.

ACO_DEV.3.3C A fejlesztési információnak magas szinten le kell írnia a kiszolgáló komponens azon alrendszereinek működését, melyek a kliens komponens SFR-jeinek érvényre juttatását támogatják.

ACO_DEV.3-4 Az értékelőnek meg kell vizsgálnia a fejlesztési információt, annak megállapítása érdekében, hogy az leírja-e a kliens komponens SFR-jeinek érvényre juttatását támogató kiszolgáló komponens alrendszerek működését.

A kliens komponens a kiszolgáló komponens interfészeit hívja meg a kiszolgáló komponens funkcióinak használata céljából. A kiszolgáló komponens meghívott interfészeire a fejlesztési információban meg kell adni a kiszolgáló komponens vonatkozó biztonsági működésének magas szintű leírását. Ez a leírás megmutatja, hogy a kiszolgáló komponens hogyan biztosítja a szükséges szolgáltatásokat az interfészhívás pillanatában. A leírásnak az ADV_TDS.1.4C-hez hasonló szinten kell az információkat megadnia. Ezért a kiszolgáló komponens értékeléséből származó TOE terv bizonyíték biztosítása kielégíti ezt a munkaegységet, amikor a kliens komponens által hívott interfészek a kiszolgáló komponens TSFI-elemei. Ha viszont nem azok, akkor a kapcsolódó biztonsági működést nem feltétlenül kell leírni a kiszolgáló komponens TOE terv bizonyítékban.

ACO_DEV.3.4C A fejlesztési információnak meg kell adnia az interfészeknek a kiszolgáló komponensbeli alrendszerekre való leképezését.

ACO_DEV.3-5 Az értékelőnek meg kell vizsgálnia a fejlesztési információt, annak megállapítása érdekében, hogy pontosak-e a kiszolgáló komponens interfészei és alrendszerei közötti megfeleltetések.

Ha a TOE terv és funkcionális specifikáció bizonyíték rendelkezésre áll a kiszolgáló komponens értékeléséből, akkor az újrahasználható a kiszolgáló komponens interfészei és alrendszerei közötti megfeleltetés pontosságának ellenőrzésére, figyelembe véve ahogyan azokat az összetett TOE-ban használják. A kiszolgáló komponens TSFI részét képező interfészek szerepelnek a kiszolgáló komponens funkcionális specifikációjában, a kapcsolódó alrendszereket pedig a kiszolgáló komponens TOE terv bizonyíték tartalmazza. A kettő közötti megfeleltetést a kiszolgáló komponens TOE terv bizonyítékban kell leírni.

Ha azonban a kiszolgáló komponens interfész nem a kiszolgáló komponens TSFI része, akkor a fejlesztői dokumentációban megadott alrendszer működési leírást kell használni a megfeleltetés pontosságának ellenőrzésére.

ACO_DEV.3.5C A fejlesztési információnak ki kell mutatnia az összetett TOE-ban használt,
- a kliens komponens TSF-jét támogató- kiszolgáló és kliens komponens interfészek közötti megfeleltetéseket.

ACO_DEV.3-6 Az értékelőnek meg kell vizsgálnia a fejlesztési információt, annak megállapítása érdekében, hogy pontos-e a kiszolgáló komponens interfészei és a kliens komponens által használt interfészek közötti megfeleltetés.

A kiszolgáló komponens interfészei és a kliens komponens által használt interfészek közötti megfeleltetés elvégezhető táblázatos vagy mátrix formában. A kliens komponens által használt interfészeket a környezetfüggőségi információ azonosítja (és a „kliens komponens környezetfüggősége” (ACO_REL) során vizsgálják).

E tevékenység során nem követelmény a kliens komponens által használt interfészek teljes lefedettségének a megállapítása, csak az, hogy a megfeleltetés helyes-e, és a kiszolgáló komponens interfészeit leképezték-e a kliens komponens által hívott interfészekre, ahol ez lehetséges. A lefedettség teljességét a „komponens-összeállítás indoklás” (ACO_COR) tevékenység vizsgálja.

6.2.4.2.2. Az ACO_DEV.3.2E értékelői akció

ACO_DEV.3.2E Az értékelőnek meg kell állapítania, hogy a megadott interfész leírás nem mond-e ellent a kliens komponensre megadott környezetfüggőségi információnak.

ACO_DEV.3-7 Az értékelőnek meg kell vizsgálnia a fejlesztési információt és a környezetfüggőségi információt, annak megállapítása érdekében, hogy az interfészek leírása ellentmondásmentes-e.

E munkaegység értékelői célja annak meghatározása, hogy a kiszolgáló komponens fejlesztési információjában és a kliens komponens környezetfüggőségi információjában leírt interfészek összhangban vannak-e egymással.

6.2.4.3. Komponens-összeállítás indoklás (ACO_COR.1) értékelése

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az összetett ST,
b) a komponens-összeállítás indoklás,
c) a környezetfüggőségi információ,
d) a fejlesztési információ,
e) egyedi azonosító.

6.2.4.3.1. Az ACO_COR.1.1E értékelői akció

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

ACO_COR.1.1CA komponens-összeállítás indoklásnak meg kell mutatnia, hogy a garanciaszint legalább olyan magas, mint amit a kliens komponens elért a kiszolgáló komponens támogató funkciójára, amikor a kiszolgáló komponenst a kliens komponens TSF-jének támogatására konfigurálták.

ACO_COR.1-1Az értékelőnek meg kell vizsgálnia a komponens-összeállítás indoklást a fejlesztési információkkal és környezetfüggőségi információkkal együtt a kliens komponens által használt olyan interfészek azonosítása céljából, amelyeket a fejlesztési információk nem részleteznek.

E munkaegység elvégzésének célja kettős:
a) annak meghatározása, hogy a kliens komponens által használt mely interfészek esetén alkalmazták a megfelelő garanciális intézkedéseket;
b) annak megállapítása, hogy a kiszolgáló komponens értékelése során használt garanciacsomag ugyanazon, vagy hierarchikusan magasabb garanciális követelményeket tartalmazta, mint amelyeket a kliens komponens értékelése során figyelembe vettek.

Az értékelő felhasználhatja a „fejlesztési bizonyíték” (ACO_DEV) tevékenységek végzése során létrehozott fejlesztési információkban szereplő megfelelőség visszavezetést (pl. ACO_DEV.l-2, ACO_DEV.2-4, ACO_DEV.3-6) a környezetfüggőségi információban azonosított azon interfészek meghatározására, melyeket a fejlesztési információk figyelmen kívül hagytak.

Az értékelőnek rögzítenie kell az SFR-t érvényre juttató interfészeket, melyek a környezetfüggőségi információban szerepelnek, de a fejlesztési információban nem. Ezek jelentik az ACO_COR.1-3 munkaegység bemenetét, a kiszolgáló komponens további garanciát igénylő részeinek azonosítását segítve.

Amennyiben a kiszolgáló és a kliens komponenst is ugyanazon garanciacsomag szerint értékelték, akkor magától értetődő annak meghatározása, hogy a kiszolgáló komponens értékelésen belüli részeinek garanciaszintje legalább olyan magas-e, mint a kliens komponensé. Amennyiben azonban a komponensek értékelésekor alkalmazott garanciacsomagok különböznek, akkor az értékelőnek meg kell állapítania, hogy a kiszolgáló komponensre alkalmazott garanciális követelmények mindegyike hierarchikusan magasabb-e, mint a kliens komponensre alkalmazott garanciális követelmény.

ACO_COR.1-2 Az értékelőnek meg kell vizsgálnia a komponens-összeállítás indoklását annak meghatározásához, hogy azon kiszolgáló komponens interfészekre, melyekre a kliens TSF a működésében hagyatkozik, az interfészt vizsgálták-e a kiszolgáló komponens értékelése során.

Az összetett ST, valamint a kiszolgáló komponensre vonatkozó nyilvános értékelési jelentés (pl. tanúsítási jelentés) és útmutató dokumentumok információkat adnak a kiszolgáló komponens logikai hatóköréről és határairól. Az összetett ST részletekkel szolgál az összetett TOE logikai hatóköréről és határairól, lehetővé téve az értékelő számára annak megállapítását, hogy egy interfész kapcsolódik-e az értékelés hatókörébe tartozó termékrészhez. Az útmutató dokumentáció részletesen leírja az összetett TOE összes interfészének a használatát. Bár az útmutató dokumentáció olyan interfészeket is tárgyalhat, amelyek nem esnek értékelés alá, minden ilyen interfésznek azonosíthatónak kell lennie, vagy az ST-ben szereplő hatókör meghatározásból vagy az értékelt konfigurációt részletező útmutató részekből. A nyilvános értékelési jelentés további szükséges megszorításokat tartalmazhat az összetett TOE használatára.

Ezért a fenti bemenetek kombinációja lehetővé teszi az értékelő számára, hogy megállapítsa, a komponens-összeállítás indoklásban leírt interfész rendelkezik-e a hozzá kapcsolódó garanciákkal, vagy szükség van további garanciára. Az értékelő rögzítse a kiszolgáló komponens azon interfészeit, melyekre szükséges ilyen további garancia, amit az ACO_COR.1-3 során mérlegelnek.

ACO_COR.1-3 Az értékelőnek meg kell vizsgálnia a komponens-összeállítás indoklást annak megállapítása érdekében, hogy a kiszolgáló komponensre alkalmazták-e a szükséges garanciális intézkedéseket.

A kiszolgáló komponensre vonatkozó értékelői döntés és az abból következő garancia újrahasználható, feltéve, ha az összetett TOE-ban a kiszolgáló komponens ugyanazon részeit használják, és következetesen alkalmazzák azokat.

Annak meghatározásához, hogy a komponensre alkalmazták-e már a szükséges garanciális intézkedéseket, és a komponens mely részeire kell még garanciális intézkedéseket alkalmazni, az értékelőnek használnia kell az ACO_DEV.*.2E tevékenység és az ACO_COR.1-1 és ACO_COR.1-2 munkaegység kimenetét:

a) A környezetfüggőségi információban (ACO_REL) azonosított, de a fejlesztési információ (ACO_DEV) között nem elemzett interfészek esetén további információ szükséges (azonosítva ACO_COR.1-1-ben).
b) A kiszolgáló komponens azon interfészei esetén, melyeket nem konzisztens módon használtak az összetett TOE-ban (különbség van a „fejlesztési bizonyíték” (ACO_DEV) és a „kliens komponens környezetfüggősége” (ACO_REL) között), a különbség kihatását meg kell nézni (ACO_DEV.*.2E).
c) További információra van szükség azon interfészek esetén, melyeket a komponens-összeállítás indoklás azonosít és nincs hozzájuk korábban igazolt garancia (azonosítva ACO_COR.1-2-ben).
d) Azon interfészek esetén pedig, melyeket a környezetfüggőségi információ, a komponens-összeállítás indoklás és a fejlesztési információ ellentmondásmentesen

írnak le, nincs további teendő, mivel a kiszolgáló komponens értékelési eredményei újrahasználhatók.

A környezetfüggőségi információ által megkövetelt, de a fejlesztési információban nem szereplő kiszolgáló komponens interfészek a kiszolgáló komponens azon elemeit mutatják, ahol további garanciára van szükség. Az interfészek azonosítják a kiszolgáló komponens belépési pontjait.

Azoknál az interfészeknél, melyeket mind a fejlesztési információ, mind a környezetfüggőségi információ tárgyal, az értékelőnek kell megállapítania, hogy az interfészeket az összetett TOE-ban oly módon alkalmazzák-e, ami megfelel a kiszolgáló komponens értékelésének. Az interfész használat módját a „fejlesztési bizonyíték" (ACO_DEV) tevékenység során vizsgálják abból a célból, hogy kiderüljön, az interfész használat megfelel mind a kiszolgáló komponensnek, mind az összetett TOE-nak. A fennmaradó vizsgálat tárgya annak megállapítása, hogy nem mondanak-e ellent egymásnak a kiszolgáló komponens és az összetett TOE konfigurációi. Ennek meghatározásához az értékelő vizsgálja meg a vonatkozó útmutató dokumentációkat, hogy azok ellentmondásmentesek-e (további útmutató a konzisztens dokumentációkról jelen anyag további részeiben olvasható). A dokumentációban talált bármilyen eltérés esetén újabb vizsgálat következik a lehetséges következmények felmérése céljából.

Azon interfészek esetén, melyekre fennáll a környezetfüggőségi és fejlesztési információ ellentmondás-mentessége, és amelyeknél a kiszolgáló komponens és az összetett TOE útmutatója összhangban van egymással, biztosított a megkívánt garancia szintje.

Az alábbi bekezdések támpontot adnak ahhoz, hogyan lehet meghatározni a konzisztenciát a kiszolgáló komponensre érvényes garancia és az összetett TOE-hez adott bizonyíték között, valamint az értékelő által végrehajtott elemzéshez olyan esetekben, amikor ellentmondásokra derül fény.

6.2.4.3.1.1. Fejlesztés

A környezetfüggőségi információ azonosítja a kliens komponens interfészeit, amiket a kiszolgáló komponenshez kell illeszteni. Ha a környezetfüggőségi információ között azonosított interfész nem szerepel a fejlesztési információ között, akkor a komponens-összeállítás indoklásnak kell gondoskodnia annak bizonyításáról, hogy a kiszolgáló komponens hogyan biztosítja az igényelt interfészt.

Ha a környezetfüggőségi információkban azonosított interfész szerepel a fejlesztési információk között, de ellentmondások lelhetők fel a leírások között, akkor további elemzésre van szükség. Az értékelő beazonosítja a kiszolgáló komponens használatában felmerülő különbségeket a kiszolgáló komponens értékelése és az összetett TOE értékelés alapján. Az értékelő tesztelés végrehajtását állapítja meg (az „összetett TOE tesztelése" (ACO_CTT) végrehajtása során) az interfész tesztelése céljából.

A kiszolgáló és a kliens komponensek összetett TOE-beli javítási állapotát (patch-ek alkalmazását) össze kell vetni a komponens értékelések során fennálló komponens frissítési státuszokkal. Ha bármilyen patch-et alkalmaztak a komponensekre, akkor a komponens-

összeállítás indoklásban szerepeltetni kell a javítások információit, ideértve az értékelt komponens SFR-jeire gyakorolt minden lehetséges hatást. Az értékelőnek mérlegelnie kell a megadott módosításokat, és ellenőriznie kell a komponens SFR-ekre gyakorolt lehetséges következmények pontosságát. Az értékelőnek ezután meg kell vizsgálnia, hogy a javítások által bevezetett módosításokat ellenőriznie kell-e teszteléssel, valamint azonosítania kell a szükséges tesztelési módszert. A tesztelés elvégezhető a komponens értékelés során elvégzett megfelelő értékelői/fejlesztői tesztelések megismétlésével, vagy az értékelő elrendelhet új teszteket a módosított komponens helyes működésének ellenőrzésére.

Amennyiben az egyedi komponensek garancia folytonossági tevékenység tárgyát képezték a komponens értékelés befejezése óta eltelt időszakban, az értékelő mérlegelje a garancia folytonosság tevékenység során felmért módosításokat az összetett TOE-ra vonatkozó független sebezhetőségi elemzés során (ACO_VUL).

6.2.4.3.1.2. Útmutatók

Az összetett TOE-ra vonatkozó útmutatók nagy eséllyel hivatkoznak az egyedi komponensek útmutatóira. Az elvárt minimális útmutató, hogy azonosítva legyen a kliens és kiszolgáló komponensek útmutatóinak alkalmazásához a sorrendi függőség, különös tekintettel az összetett TOE előkészületi (telepítési) szakaszára.

Az előkészítő eljárások (AGD_PRE) és „üzemeltetési felhasználói útmutató” (AGD_OPE) családok összetett TOE-ra vonatkozó alkalmazásán kívül vizsgálni kell a komponensek és az összetett TOE útmutatóit ellentmondás-mentesség szempontjából, és jelezni kell minden eltérést.

Ha az összetett TOE útmutató hivatkozik a kiszolgáló és kliens komponensek útmutató dokumentációira, akkor az ellentmondás-mentesség mérlegelése az egyes komponensekhez adott útmutatók közötti konzisztenciára korlátozódik (a kiszolgáló és a kliens komponens útmutatói közötti ellentmondás-mentességre). Ha azonban az összetett TOE-ra további útmutatókat is készítettek, akkor alaposabb elemzésre van szükség, hiszen a komponensekhez készített és az összetett TOE-ra vonatkozó útmutató dokumentációk közötti ellentmondás-mentességet is garantálni kell.

Ekkor az ellentmondás-mentesség azt jelenti, hogy az útmutató vagy ugyanaz, vagy további megszorításokat szab az egyedi komponensekre azok integrálása esetére, hasonló módon a funkcionális/garanciális összetevők pontosítási módjához.

A rendelkezésre álló információk segítségével (melyeket a „fejlesztési bizonyíték” (ACO_DEV) használ bemenetként) az értékelő képes lehet annak megállapítására, hogy a komponens értékelés során specifikált kiszolgáló komponens konfigurációtól való eltérések milyen lehetséges következményekkel járnak. Magas EAL-ok esetén azonban (amikor a kiszolgáló komponens értékelés tartalmazta a „TOE terv” (ADV_TDS) követelményeket) előfordulhat, hogy az útmutató módosításainak lehetséges kihatásai nem határozhatók meg teljes mértékben, - hacsak az összetett TOE-hoz nem bocsátják rendelkezésre a fejlesztési információ részeként a részletes tervezési leírásokat-, mivel a belső részletek nem ismertek. Ekkor az értékelőnek jelentést kell írnia a maradvány kockázatokról.

Ezeket a maradvány kockázatokat szerepeltetni kell az összetett TOE-ről szóló minden nyilvános értékelési jelentésben.

Az értékelőnek rögzítenie kell az útmutatók eltéréseit, ami az értékelő független tesztelési tevékenység („összetett TOE tesztelése”, ACO_CTT) bemenete lesz.

Az összetett TOE útmutatója kiegészítheti a komponensek útmutatóit, elsősorban a telepítésre, illetve a kiszolgáló és kliens komponens telepítési lépéseinek egymáshoz viszonyított végrehajtási sorrendjére vonatkozóan. Az egyedi komponensekre nézve a telepítési lépések sorrendje nem módosulhat, azonban előfordulhat a lépések összefésülésének szükségessége. Az értékelő vizsgálja meg az útmutatót, hogy az továbbra is teljesíti-e a komponensek értékelése során végrehajtott AGP_PRE tevékenység követelményét.

Előfordulhat olyan eset, hogy a környezetfüggőségi információ a kiszolgáló komponens olyan TSFI-n kívüli interfészeit is azonosítja, amelyekre a környezetfüggőségi információ szerint a kliens komponens hagyatkozik. A kiszolgáló komponens ilyen további interfészeihez útmutatóra lehet szükség. Feltéve, hogy az összetett TOE felhasználója megkapja a kiszolgáló komponensre vonatkozó útmutató dokumentációt, a kiszolgáló komponens AGP_PRE és AGP_OPE döntéseinek eredményei újrahasználhatók azokra az interfészekre, melyeket a kiszolgáló komponens értékelése során vizsgáltak. Azonban, ha a kliens komponens egyéb interfészeket is használ, az értékelőnek meg kell állapítania, hogy a kiszolgáló komponens útmutató dokumentációja megfelel-e az AGP_PRE és AGP_OPE követelményeinek, ahogyan azokat a kiszolgáló komponens értékelése során alkalmazták.

A kiszolgáló komponens értékelés során vizsgált interfészekre, vagyis amelyekre már igazolt a garancia, az értékelő győződjön meg arról, hogy az összetett TOE minden egyes interfész használati leírása összhangban van-e a kiszolgáló komponensnél írtakkal. Ennek megállapításához az értékelőnek minden interfész esetén végre kell hajtania egy leképezést az összetett TOE és a kiszolgáló komponens útmutatóira. Az értékelő ezután hasonlítsa össze az útmutatókat az ellentmondás-mentesség megállapításához.

Példák összetett TOE útmutatóban megadott olyan egyéb megszorításokra, melyeket vizsgálni kell abból a szempontból, hogy összhangban vannak-e a komponens útmutatóval (egy adott komponens útmutatót követi egy összetett TOE útmutató példa, ami további megszorításnak tekintendő):

- Komponens: A jelszó hosszt minimum 8 karakter hosszúra kell beállítani, és tartalmaznia kell alfabetikus és numerikus karaktereket.
- Összetett TOE: A jelszó hosszt minimum 10 karakter hosszúra kell beállítani, és tartalmaznia kell alfabetikus és numerikus karaktereket, és legalább egyet a következő speciális karakterekből: ( ) { } ^ < > -_
- Megjegyzés: A jelszóhosszt csak növelni lehet [egész szám>8] karakterre, míg az alfabetikus és numerikus karakterek használatának elhagyása csak akkor elfogadható, ha ugyanolyan vagy magasabb mértéket ér el az erősségi besorolás (figyelembe véve a jelszó találgatás valószínűségét).
- Komponens: A következő szolgáltatásokat le kell tiltani a registry beállításokban: WWW Publishing Service és ICDBReporter Service.

- Összetett TOE: A következő szolgáltatásokat le kell tiltani a registry beállításokban: WWW Publishing Service és ICDBReporter Service, Remote Procedure Call (RPC) Locator and Procedure Call (RPC) Service
- Komponens: Válassza ki a következő tulajdonságokat a biztonsági naplóállományban való szerepeltetéshez: dátum, idő, esemény típusa, szubjektum azonosítója, siker/sikertelenség.
- Összetett TOE: Válassza ki a következő tulajdonságokat a biztonsági naplóállományban való szerepeltetéshez: dátum, idő, esemény típusa, szubjektum azonosítója, siker/sikertelenség, esemény szövege és folyamat szál.

Amennyiben az összetett TOE útmutató eltér a kiszolgáló komponensétől (nem pontosítása annak), az értékelő mérje fel az útmutató változásainak lehetséges kockázatait. Ehhez használja a rendelkezésre álló információt (ideértve a nyilvánosan elérhető információkat, a kiszolgáló komponens nyilvánosan elérhető értékelési jelentésében (tanúsítási jelentésben) szereplő architektúra leírást, valamint az útmutató egyéb részeit), azért, hogy azonosítani tudja az útmutató módosításainak az összetett TOE SFR-jeire gyakorolt valószínű hatását.

Amennyiben a kliens komponens értékelése során a próbatelepítés a kiszolgáló komponenst használta a környezeti követelmények teljesítésére, akkor az összetett TOE-ra vonatkozó ezen munkaegység teljesítettnek tekinthető. Ha nem a kiszolgáló komponenst használták az AGD_PRE.1-3 munkaegység kielégítésére a kliens komponens értékelése folyamán, akkor az értékelő alkalmazza az összetett TOE-hoz biztosított felhasználói eljárásokat az összetett TOE előkészítéséhez, ahogyan azt az AGD_PRE.1-3-ban megadott útmutató leírja. Ez lehetővé teszi az értékelő számára annak megállapítását, hogy az összetett TOE-hoz készített előkészítő útmutató kielégítő-e az összetett TOE és annak működési környezete biztonságos előkészítéséhez.

6.2.4.3.1.3. Életciklus - Szállítás

Ha az összetett TOE esetén különböző szállítási mechanizmusokat alkalmaznak (azaz nem a komponensek értékelése során definiált és értékelt biztonságos szállítási eljárásoknak megfelelően juttatják el a komponenseket a felhasználóhoz), akkor az összetett TOE szállítási eljárásait a komponens értékelések során alkalmazott „szállítás” (ALC_DEL) követelményei szerinti értékelésnek kell alávetni.

Az összetett TOE szállítható integrált termékként vagy a komponenseket külön is lehet szállítani.

Ha a komponenseket külön-külön szállítják, akkor a kiszolgáló és kliens komponensek szállítás értékelési eredményei újrahasználhatók. A kiszolgáló komponensek szállítását a kliens komponens értékelői próbatelepítése során ellenőrzik a kiszolgáló komponens útmutatója alapján, alkalmazva a vonatkozó útmutatókat és a szállítást ellenőrző szempontokat, ami a felhasználó felelőssége.

Ha az összetett TOE-t egy egységként szállítják, akkor ennek szállítási eljárásait az összetett TOE értékelési tevékenység részeként kell vizsgálni.

Az összetett TOE elemeinek szállítási eljárásaira vonatkozó értékelést a TOE komponensekre alkalmazott „szállítás” (ALC_DEL) módszertan szerint kell elvégezni, biztosítva, hogy minden további elemet (például kiegészítő útmutatók az összetett TOE-ra) figyelembe vesznek a szállítási eljárásokban.

6.2.4.3.1.4. Életciklus - CM képességek

Az ALC_CMC.1 értékelési altevékenység vizsgálja az összetett TOE egyedi azonosítását, az ALC_CMS.2 értékelési altevékenység pedig azokat az elemeket, melyek az összetett TOE-t alkotják.

Bár az összetett TOE-ra kiegészítő útmutatók készíthetők, ezen útmutató egyedi azonosítása (az ALC_CMC.1 során az összetett TOE egyedi azonosításának részeként) elegendő az útmutató kezeléséhez.

A fennmaradó (fentebb nem vizsgált) ALC osztály (Életciklus támogatás) tevékenységek során hozott döntések újrahasználhatók a kiszolgáló komponens értékeléséből, mivel az összetett TOE integrálása során nem történik további fejlesztés.

A fejlesztés biztonságára nézve nincsenek további szempontok, mivel az integráció vélhetően a felhasználó telephelyén történik, vagy (ha az összetett TOE-t egy egységként szállítják) a kliens komponens fejlesztői telephelyén. A felhasználó telephelye a CC hatókörén kívül esik. Akkor sincsenek további követelmények vagy útmutatók, ha az integrálás ugyanott történik, mint a kliens komponens kialakítása, mivel minden komponens az összetett TOE konfiguráció elemeinek számít, és ezért mindenképp a kliens komponens fejlesztés biztonsági eljárásai értelmében kell vizsgálni.

Az integrálás során alkalmazott eszközök és technikák vizsgálata a kliens komponens fejlesztője által szolgáltatott bizonyítékok segítségével történik. A kiszolgáló komponens szempontjából lényeges összes eszköz/technika ellenőrzését a kiszolgáló komponens értékelése során kell végrehajtani. Például, ha a kiszolgáló komponenst forráskód formájában szállítják, és a felhasználónak kell fordítania, összeszerkesztenie (például az integrációt végző kliens komponens fejlesztőjének), a fordítóprogramot a kiszolgáló komponens értékelése során specifikálni és értékelni kellett, csakúgy, mint a vonatkozó paramétereket.

Az összetett TOE-ra vonatkozóan nincs életciklus definíció, mivel az elemeket nem fejlesztik tovább.

Egy komponens hibajavításának eredményei nem vonatkoznak az összetett TOE-ra. Ha az összetett TOE esetén belevették a garanciacsomagba a hibajavítást, akkor a „hibajavítás” (ALC_FLR) követelményeket kell alkalmazni az összetett TOE értékelése során (mint minden szigorításnál).

6.2.4.3.1.5. Tesztek

Az összetett TOE tesztelése a kliens komponens értékelésekor végzett „tesztelés” (ATE) tevékenység végrehajtása során fog megtörténni, mivel a kliens komponens teszteléséhez

használt konfigurációnak magába kellett foglalnia a kiszolgáló komponenst abból a célból, hogy teljesüljenek a működési környezetre vonatkozó követelmények. Ha a kiszolgáló komponenst nem használták a kliens komponens teszteléséhez a kliens értékelése során, vagy az értékelt konfigurációhoz képest bármelyik komponens konfigurációja megváltozott, akkor az összetett TOE-ra meg kell ismételni a kliens komponens értékelésekor végrehajtott fejlesztői tesztet az ATE osztály követelményeinek kielégítése céljából.

6.2.4.4. Szigorú interfész tesztelés (ACO_CTT.2) értékelése

Ennek az altevékenységnek a célja annak meghatározása, hogy a fejlesztő jól hajtotta-e végre és dokumentálta-e a teszteket a kiszolgáló komponens azon interfészeire, amelyeket a kliens komponens a működése során meghív. Ennek az elemzésnek a részeként az értékelő megismétli a fejlesztői tesztek egy részét, és további teszteket végez, hogy meggyőző módon garantálni lehessen az összetett TOE és a kliens komponens által használt kiszolgáló komponens interfészeinek elvárt működését.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) a tesztelésre alkalmas összetett TOE,
b) az összetett TOE tesztelési bizonyítéka,
c) a környezetfüggőségi információ,
d) a fejlesztési információ.

6.2.4.4.1. Az ACO_CTT.2.1E értékelői akció

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

ACO_CTT.2.1C Az összetett TOE és a kiszolgáló komponens interfész tesztelési dokumentációjának tartalmaznia kell a tesztelési terveket, az elvárt teszteredményeket és a tényleges (kapott) teszteredményeket.

ACO_CTT.2-1 Az értékelőnek meg kell vizsgálnia az összetett TOE tesztelési dokumentációját annak megállapítása érdekében, hogy az tartalmazza-e a tesztelési tervet, a várt teszteredményeket és a tényleges, kapott eredményeket.

Ez a munkaegység teljesíthető a kliens komponens értékeléséből származó tesztelési bizonyítékok által, ha a kiszolgáló komponenst használták a kliens komponens működési környezetére vonatkozó IT követelmények kielégítésére.

Az ATE_FUN.1.1E kielégítéséhez szükséges minden munkaegység alkalmazandó annak meghatározásához, hogy:

a) a tesztelési dokumentáció tartalmazza a tesztelési tervet, a várt teszteredményeket és a tényleges, kapott eredményeket;
b) a tesztelési dokumentáció tartalmazza a tesztek megismételhetőségéhez szükséges információkat;
c) a kiszolgáló komponens tesztelésére fordított fejlesztői munka mennyiségét/szintjét.

ACO_CTT.2-2 Az értékelőnek meg kell vizsgálnia a kiszolgáló komponens interfész tesztelési dokumentációját, annak megállapítása érdekében, hogy az tartalmazza-e a tesztelési tervet, a várt teszteredményeket és a ténylegesen kapott eredményeket.

Ez a munkaegység teljesíthető a kiszolgáló komponens értékeléséből származó tesztelési bizonyítékok által, azon interfészek esetén, amelyeket az összetett TOE-ban a kliens komponens használ, és a kiszolgáló komponens sikeres értékelése során a TSFI részét képezték. Annak megállapítására, hogy a kiszolgáló komponens interfészei, melyeket a kliens használ, valóban a TSFI részei voltak-e, az ACO_COR tevékenység végrehajtása során kerül sor.

Az ATE_FUN.1.1E kielégítéséhez szükséges minden munkaegység alkalmazandó annak meghatározásához, hogy:

a) a tesztelési dokumentáció tartalmazza a tesztelési tervet, a várt teszteredményeket és a tényleges, kapott eredményeket;
b) a tesztelési dokumentáció tartalmazza a tesztek megismételhetőségéhez szükséges információkat;
c) a kiszolgáló komponens tesztelésére fordított fejlesztői munka mennyiségét/szintjét.

ACO_CTT.2.2C Az összetett TOE tesztek fejlesztő által történt elvégzéséből származó tesztelési dokumentációnak meg kell mutatnia, hogy a TSF a specifikáltnak megfelelően működik és teljes.

ACO_CTT.2-3 Az értékelőnek meg kell vizsgálnia a tesztelési dokumentációt, annak megállapítása érdekében, hogy az megadja-e a az összetett TOE tesztelésével kapcsolatos tesztelési dokumentációban lévő tesztek és az összetett TOE biztonsági előirányzatában szereplő összetett TOE SFR-ek közötti megfeleltetést.

A tesztelési megfeleltetés bizonyításához elegendő egy egyszerű kereszttábla. A tesztelési dokumentációban megadott tesztek és az SFR-ek közötti megfeleltetésnek egyértelműnek kell lennie.

ACO_CTT.2-4 Az értékelőnek meg kell vizsgálnia a tesztelési dokumentációt, annak megállapítása érdekében, hogy a fejlesztő által végrehajtott összetett TOE tesztek megmutatják-e, hogy a TSF a specifikációnak megfelelően működik.

E munkaegységhez útmutató található:

a) 7.1 fejezetben és
b) 7.2 fejezetben.

A tesztek sikeres végrehajtásából származó kimenetek (ATE_FUN.1.3C számára) összehasonlíthatók a leképezéssel annak megállapítása érdekében, hogy az összetett TOE SFR-ek –ahogyan azokat a fejlesztő tesztelte- az elvárt módon működnek-e.

ACO_CTT.2.3C A kiszolgáló komponens interfész tesztek fejlesztő által történt elvégzéséből származó tesztelési dokumentációnak meg kell mutatnia, hogy a kliens komponens által használt kiszolgáló komponens interfész a specifikáltnak megfelelően működik és teljes.

ACO_CTT.2-5 Az értékelőnek meg kell vizsgálnia a tesztelési dokumentációt, annak megállapítása érdekében, hogy az megadja-e a kliens komponens által használt kiszolgáló komponens interfészek tesztelésével kapcsolatos dokumentációban lévő tesztek és a környezetfüggőségi információk között specifikált interfészek közötti megfeleltetést.

A tesztelési megfeleltetés bizonyításához elegendő egy egyszerű kereszttábla. A tesztelési dokumentációban megadott tesztek és az interfészek közötti megfeleltetésnek egyértelműnek kell lennie.

ACO_CTT.2-6 Az értékelőnek meg kell vizsgálnia a tesztelési dokumentációt, annak megállapítása érdekében, hogy a fejlesztő által végrehajtott kiszolgáló komponens interfész tesztek megmutatják-e, hogy a kliens komponens által használt kiszolgáló komponens interfészek a specifikációnak megfelelően működnek.

E munkaegységhez útmutató található:

a) 7.1 fejezetben és
b) 7.2 fejezetben.

A tesztek sikeres végrehajtásából származó kimenetek (ATE_FUN.1.3C számára) összehasonlíthatók a leképezéssel annak megállapítása érdekében, hogy kiszolgáló komponens interfészei –ahogyan azokat a fejlesztő tesztelte- az elvárt módon működnek-e.

ACO_CTT.2.4C A kiszolgáló komponensnek tesztelésre alkalmasnak kell lennie.

ACO_CTT.2-7 Az értékelőnek meg kell vizsgálnia az összetett TOE-t, annak megállapítása érdekében, hogy azt megfelelő módon telepítették-e, és az ismert állapotok egyikében van-e.

Annak megállapítása, hogy az összetett TOE-t megfelelően telepítették, és az ismert állapotok valamelyikében van-e, az ATE_IND.2-1 és ATE_IND.2-2 munkaegységek feladata, aminek keretében a fejlesztő által tesztelésre átadott TOE-t vizsgálják.

ACO_CTT.2-8 Az értékelőnek meg kell vizsgálnia a fejlesztő által biztosított erőforrás együttest, annak megállapítása érdekében, hogy azok megegyeznek-e a kiszolgáló komponens funkcionális teszteléséhez a kiszolgáló komponens fejlesztője által használt erőforrásokkal.

Annak megállapítása, hogy a biztosított erőforrások megegyeznek a kiszolgáló komponens összetett TOE-beli használata szerinti funkcionális teszteléséhez használt erőforrásokkal, az ATE_IND.2-3 munkaegység hatásköre.

6.2.4.4.2. Az ACO_CTT.2.2E értékelői akció

ACO_CTT.2.2E Az értékelőnek végre kell hajtania a tesztelési dokumentációban szereplő tesztek egy mintáját a fejlesztői teszteredmények ellenőrzése céljából.

ACO_CTT.2-9 A tesztek kiválasztását és végrehajtását az ATE_IND.2.2E-vel összhangban kell elvégezni, bizonyítandó, hogy az összetett TOE biztonsági előirányzatban specifikált SFR-ek megfelelően működnek.

Az értékelőnek az ATE_IND.2.2E kielégítéséhez szükséges összes munkaegységet alkalmaznia kell, és az összetett TOE ETR-ben rögzítenie kell a kapcsolódó munkaegységek által előírt minden vizsgálatot, kapott eredményt és döntést.

6.2.4.4.3. Az ACO_CTT.2.3E értékelői akció

ACO_CTT.2.3E Az értékelőnek le kell tesztelnie az összetett TOE TSF interfészeinek egy részhalmazát, hogy meggyőződjön arról, hogy az összetett TSF a specifikáltnak megfelelően működik.

ACO_CTT.2-10 Az értékelőnek az ATE_IND.2.3E szerinti tesztelést kell végeznie az összetett TOE biztonsági előirányzatában megadott SFR-ek részhalmazára, azt bizonyítandó, hogy a TSF a specifikációnak megfelelően működik.

Az értékelőnek alkalmaznia kell az ATE_IND.2.3E kielégítéséhez szükséges minden munkaegységet, és rögzítenie kell az összetett TOE ETR-ben minden előírt vizsgálatot, eredményt és döntést.

Amikor az összetett TOE TSF interfészeinek tesztelésre való kiválasztása történik, az értékelőnek figyelembe kell vennie minden olyan módosítást, amely a komponensekben az értékelt verzió vagy konfiguráció óta történt. Ez jelenthet javításokat, a módosított útmutató dokumentációk miatti eltérő konfigurálást, a komponens TSF-jébe nem eső egyéb komponens elemektől való környezeti függőséget. Ezeket a módosításokat a „komponens-összeállítás indoklás” (ACO_COR) tevékenység során kell azonosítani.

ACO_CTT.2-11 Az értékelőnek az ATE_IND.2-nek megfelelően tesztelést kell végeznie a kiszolgáló komponens interfészeinek egy részhalmazára, hogy azok a specifikáltak szerint működnek-e.

Az értékelőnek az ATE_IND.2.3E kielégítéséhez szükséges összes munkaegységet alkalmaznia kell, és az összetett TOE ETR-ben rögzítenie kell a kapcsolódó munkaegységek által előírt minden vizsgálatot, kapott eredményt és döntést.

Amikor a kiszolgáló komponens interfészeinek tesztelésre való kiválasztása történik, az értékelőnek figyelembe kell vennie minden olyan módosítást, amely a kiszolgáló komponensben az értékelt verzió vagy konfiguráció óta történt. Az értékelőnek külön figyelmet kell fordítania a tesztek kidolgozására, hogy azok megmutassák a kiszolgáló komponens azon interfészeinek helyes működését, amelyeket nem vizsgáltak a kiszolgáló komponens értékelése során. Ezeket az egyéb interfészeket és más módosításokat a „komponens-összeállítás indoklás” (ACO_COR) tevékenység során kell azonosítani.

6.2.4.5. Megemelt alap kompozíció sebezhetőség elemzés (ACO_VUL.3) értékelése

Ezen altevékenység célja annak megállapítása, hogy az összetett TOE-nek, működési környezetében vannak-e megemelt alap támadási képességgel kihasználható sebezhetőségei.

A fejlesztő elkészíti a komponensekre vonatkozó és a kiszolgáló-kliens viszonylatban felmerülő maradvány sebezhetőségekkel kapcsolatos elemzést. Az értékelő kutatásokat végez a nyilvánosan hozzáférhető forrásokban, hogy azonosítson minden lehetséges új, a komponenseket fenyegető sebezhetőséget (a komponensek értékelésének befejezése óta felmerült sebezhetőségeket). Az értékelő ezen kívül egy független sebezhetőség elemzést és behatolás tesztelést hajt végre az összetett TOE-ra.

Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) a tesztelésre alkalmas összetett TOE,
b) az összetett ST,
c) a komponens-összeállítás indoklás,
d) a környezetfüggőségi információ,
e) az útmutató dokumentáció,
f) nyilvánosan elérhető információ a lehetséges biztonsági sebezhetőségek meghatározásának támogatására,
g) az összes komponens értékelése során jelentett maradvány sebezhetőségek.

6.2.4.5.1. Az ACO_VUL.3.1E értékelői akció

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

ACO_VUL.3.1C Az összetett TOE-nak tesztelésre alkalmasnak kell lennie.

ACO_VUL.3-1 Az értékelőnek meg kell vizsgálnia az összetett TOE-t, annak megállapítása érdekében, hogy azt megfelelő módon telepítették-e, és az ismert állapotok egyikében van-e.

Annak megállapítása, hogy az összetett TOE-t megfelelően telepítették-e, és az ismert állapotok valamelyikében van-e, az összetett TOE-ra vonatkozó ATE_IND.2-1 és ATE_IND.2-2 munkaegységek feladata.

Ha a garanciacsomag tartalmazza az ACO_CTT családot, akkor az értékelő hivatkozhat az „összetett TOE tesztelése” (ACO_CTT)*-1 eredményére, hogy az teljesül.

ACO_VUL.3-2 Az értékelőnek meg kell vizsgálnia az összetett TOE konfigurációt annak megállapítása érdekében, hogy az ST-ben szereplő, a komponensekre vonatkozó bármilyen feltételezést és célt, amely IT entitásokkal kapcsolatos, más komponensek kielégítenek.

A komponens ST-je tartalmazhat feltételezéseket más komponensekkel kapcsolatban, amelyek használhatják az ST-vel kapcsolatos komponenst; például egy kiszolgáló komponensként alkalmazott operációs rendszerre vonatkozó ST tartalmazhat olyan feltételezést, hogy a rajta működő bármilyen alkalmazás ne fusson privilegizált módban. Ezek a feltételezések és célok az összetett TOE más komponensei által teljesítendők.

6.2.4.5.2. Az ACO_VUL.3.2E értékelői akció

ACO_VUL.3.2E Az értékelőnek végre kell hajtania egy vizsgálatot annak megállapítása érdekében, hogy a kiszolgáló és a kliens komponensre beazonosított bármilyen maradvány sebezhetőség nem aknázható ki az összetett TOE-ban, annak működési környezetében.

ACO_VUL.3-3 Az értékelőnek meg kell vizsgálnia a kiszolgáló komponens értékeléséből származó maradvány sebezhetőségeket annak megállapítása érdekében, hogy azok nem kiaknázhatók-e az összetett TOE működési környezetében.

A kiszolgáló komponens értékelés során a termékre felismert sebezhetőségek listáját – melyeket a kiszolgáló komponensben nem kihasználhatónak ítéltek – kell használni ennek a tevékenységnek a bemeneteként. Az értékelő állapítsa meg, hogy azok a feltételek, amelyek alapján a sebezhetőséget nem kihasználhatónak ítélték, fennállnak-e az összetett TOE-ra, vagy a komponens-összeállítás miatt felmerülhet az adott sebezhetőség kiaknázhatósága. Például, ha a kiszolgáló komponens értékelése során felételezték, hogy egy bizonyos operációs rendszer szolgáltatás le van tiltva, ami viszont engedélyezett az összetett TOE értékelésben, akkor az ehhez a szolgáltatáshoz kapcsolódó bármilyen lehetséges sebezhetőséget, amelyet korábban kizártak, most figyelembe kell venni.

Továbbá, a kiszolgáló komponens értékeléséből származó ismert, nem kihasználható sebezhetőségeket is figyelembe kell venni a többi komponenssel (pl. kliens komponenssel) kapcsolatos minden ismert, nem kihasználható sebezhetőség ismeretében az összetett TOE-n belül. Ez azt az esetet fedi le, amikor egy lehetséges sebezhetőség, ami elszigetelve nem kihasználható volt, egy másik - lehetséges sebezhetőséget tartalmazó - IT egyeddel való integrálás után kiaknázhatóvá válik.

ACO_VUL.3-4 Az értékelőnek meg kell vizsgálnia a kliens komponens értékeléséből származó maradvány sebezhetőségeket annak megállapítása érdekében, hogy azok nem kihasználhatók-e az összetett TOE működési környezetében.

A kliens komponens értékelés során a termékre felismert sebezhetőségek listáját –melyeket a kliens komponensben nem kihasználhatóknak ítéltek – kell használni ennek a tevékenységnek a bemeneteként. Az értékelő állapítsa meg, hogy azok a feltételek, amelyek alapján a sebezhetőséget nem kihasználhatónak ítélték, fennállnak-e az összetett TOE-ra, vagy a komponens-összeállítás miatt felmerülhet az adott sebezhetőség kiaknázhatósága. Például, ha a kliens komponens értékelése során azt felételezték, hogy a működési környezet követelményeit kielégítő IT-egyed nem ad vissza egy bizonyos értéket egy szolgáltatás kérésre, amelyet az összetett TOE-ban a kiszolgáló komponens most visszaad, akkor az ehhez a visszatérési értékhez kapcsolódó, korábban kizárt bármilyen lehetséges sebezhetőséget újra figyelembe kell venni.

Továbbá, a kliens komponens értékeléséből származó ismert, nem kihasználható sebezhetőségeket is figyelembe kell venni a többi komponenssel (pl. kiszolgáló komponenssel) kapcsolatos minden ismert, nem kihasználható sebezhetőség ismeretében az összetett TOE-n belül. Ez azt az esetet fedi le, amikor egy lehetséges sebezhetőség, ami elszigetelve nem kihasználható volt, egy másik -potenciális sebezhetőséget tartalmazó- IT egyeddel való integrálás után kiaknázhatóvá válik.

6.2.4.5.3. Az ACO_VUL.3.3E értékelői akció

ACO_VUL.3.3E Az értékelőnek kutatnia kell a nyilvánosan hozzáférhető forrásokat a kiszolgáló és a kliens komponensnek az összetett TOE működési környezetében való használatából származó lehetséges sebezhetőségeinek feltárása céljából.

ACO_VUL.3-5 Az értékelőnek meg kell vizsgálnia a nyilvánosan hozzáférhető információforrásokat annak érdekében, hogy azonosítani lehessen a kiszolgáló komponensben azokat a lehetséges biztonsági sebezhetőségeket, amelyek a kiszolgáló komponens értékelésének befejezése óta váltak ismertté.

Az értékelőnek fel kell használnia a nyilvánosan hozzáférhető információkat –ahogyan azt a [3]-beli AVA_VAN.3-2 leírja- a kiszolgáló komponens sebezhetőségeinek feltárása céljából.

Nem kell tovább vizsgálni azokat a lehetséges sebezhetőségeket, amelyek a kiszolgáló komponens értékelése előtt már nyilvánosan ismertek voltak, kivéve, ha nyilvánvaló az értékelő számára, hogy a szóban forgó sebezhetőség kiaknázásához szükséges támadás képesség jelentős mértékben csökkent. Ez bekövetkezhet a kiszolgáló komponens értékelése óta megjelent új technológia miatt, melynek alkalmazása egyszerűsíti a sebezhetőség kihasználását.

ACO_VUL.3-6 Az értékelőnek meg kell vizsgálnia a nyilvánosan hozzáférhető információforrásokat annak érdekében, hogy azonosítani lehessen a kliens komponensben azokat a lehetséges biztonsági sebezhetőségeket, amelyek a kliens komponens értékelésének befejezése óta váltak ismertté.

Az értékelőnek fel kell használnia a nyilvánosan hozzáférhető információkat –ahogyan azt a [3]-beli AVA_VAN.3-2 leírja- a kiszolgáló komponens sebezhetőségeinek feltárása céljából.

Nem kell tovább vizsgálni azokat a lehetséges sebezhetőségeket, amelyek a kliens komponens értékelése előtt már nyilvánosan ismertek voltak, kivéve, ha nyilvánvaló az értékelő számára, hogy a szóban forgó sebezhetőség kiaknázásához szükséges támadás képesség jelentős mértékben csökkent. Ez bekövetkezhet a kliens komponens értékelése óta megjelent új technológia miatt, melynek alkalmazása egyszerűsíti a sebezhetőség kihasználását.

ACO_VUL.3-7 Az értékelőnek rögzítenie kell az ETR-ben az azonosított lehetséges sebezhetőségeket, melyek szóba jönnek a tesztelésnél, és amelyek az összetett TOE működési környezetében kihasználhatóak lehetnek.

Az ST, az útmutató dokumentumok és a funkcionális specifikáció segítségével meg kell állapítani, hogy a sebezhetőségek valóban relevánsak-e az összetett TOE működési környezetében.

Az értékelő rögzítsen minden olyan indokot, ami miatt sebezhetőségek kizárhatók a további vizsgálatokból, ha úgy ítéli meg, hogy a sebezhetőség nem vonatkoztatható a működési környezetre. Egyébként pedig rögzítse a lehetséges sebezhetőségeket további mérlegelés, vizsgálat céljából.

Az összetett TOE-ra annak működési környezetében vonatkoztatható lehetséges sebezhetőségek listáját, ami a behatolás tesztelési tevékenység (ACO_VUL.3.5E) bemenete, az értékelőknek az ETR-ben meg kell adniuk.

6.2.4.5.4. Az ACO_VUL.3.4E értékelői akció

ACO_VUL.3.4E Az értékelőnek végre kell hajtania egy független sebezhetőség elemzést az összetett TOE-ra, az útmutató dokumentáció, környezetfüggőségi információ és komponens-összeállítás indoklás felhasználásával, az összetett TOE-ban fellelhető lehetséges sebezhetőségek azonosítására.

ACO_VUL.3-8 Az értékelőnek végre kell hajtania egy keresést az összetett TOE ST-n, az útmutató dokumentáción, a környezetfüggőségi információn és a komponens-összeállítás indoklásán, az összetett TOE lehetséges sebezhetőségeinek meghatározása céljából.

A független értékelői sebezhetőségi elemzésben a komponensek vizsgálata kissé eltérő formában történhet, mint ahogyan azt a [3]-beli AVA_VAN.3.3E leírja egy komponens értékelésére, mivel nem feltétlenül kell a garanciacsomag szempontjából fontos tervezési absztrakciós szintek minden rétegét megnézni. Ezeket a kiszolgáló komponens értékelése során már megvizsgálták, de a bizonyíték nem biztos, hogy rendelkezésre áll az összetett TOE értékeléshez. Azonban, a [3]-beli AVA_VAN.3.3E-hez kapcsolódó munkaegységekben leírt általános megközelítés alkalmazható, és az alapja az, hogy az összetett TOE-ban az értékelő lehetséges sebezhetőségek után kutat.

Az összetett TOE értékelésében használt egyedi komponensek sebezhetőségi elemzését már végrehajtották a komponensek értékelése során. Az összetett TOE értékelés során a sebezhetőségi elemzés középpontjában az áll, hogy feltáruljanak azok a sebezhetőségek, amelyek a komponensek integrálása miatt kerültek a rendszerbe, vagy a komponensek konfigurációjának valamilyen változása miatt: a komponens értékelés során megállapított konfiguráció más, mint az összetett TOE-ban használt.

Az értékelő a komponens konstrukció megértéséhez használja a kliens komponensre vonatkozó környezetfüggőségi információt, a kiszolgáló komponensre vonatkozó komponens-összeállítás indoklást és fejlesztési információt, valamint a kliens komponens terv információt. Ezek lehetővé teszik az értékelő számára, hogy megértse, hogyan működik együtt a kliens és a kiszolgáló komponens.

Az értékelőnek figyelembe kell vennie az összetett TOE telepítésére, indítására és működtetésére vonatkozó minden új útmutatót, hogy azonosítsa az ezek által bevezetett lehetséges sebezhetőségeket.

Ha az egyedi komponensek bármelyike is garancia folytonossági tevékenységen esett át a komponens értékelés befejeződése óta eltelt időszakban, akkor az értékelőnek számításba kell vennie a javításokat a független sebezhetőségi elemzés során. A módosításokkal kapcsolatos információk a garancia folytonossági tevékenységek nyilvános jelentésében szerepelnek (például karbantartási jelentés). Ez kiegészítendő az útmutató dokumentációk bármilyen frissítésével, ami a módosítások miatt történt, és olyan információkkal, amelyek a módosításokkal kapcsolatban nyilvánosan hozzáférhetők (például gyártó weboldala).

A bizonyíték hiánya miatt azonosított minden olyan kockázatot, amivel kapcsolatban nem állapítható meg a módosítások vagy a komponens konfigurációjának értékelt konfigurációtól való eltérésének teljes kihatása, dokumentálni kell az értékelői sebezhetőségi elemzésben.

6.2.4.5.5. Az ACO_VUL.3.5E értékelői akció

ACO_VUL.3.5E Az értékelőnek behatolás tesztelést kell végeznie, ami az azonosított sebezhetőségeken alapul, annak megmutatása céljából, hogy az összetett TOE ellenáll a megemelt alap támadási képességgel rendelkező támadó támadásainak.

ACO_VUL.3-9 Az értékelőnek végre kell hajtania a behatolás tesztelést, ahogyan azt a [3]-beli AVA_VAN.3.4E leírja.

Az értékelő a [3]-beli AVA_VAN.3.4E értékelői feladat teljesítése érdekében alkalmazza az összes szükséges munkaegységet, és az ETR-ben rögzítse az összetett TOE-ra elvégzett összes vizsgálatot és meghozott döntést, melyeket a munkaegységek előírnak.

Az értékelő a [3]-beli AVA_VAN.3.1E értékelői feladathoz is alkalmazza a munkaegységeket annak megállapítása érdekében, hogy a fejlesztő által biztosított összetett TOE alkalmas-e a tesztelésre.

6.2.5. A kiegészítő garancia-összetevők értékelése

A következő alfejezetek megadják az egyes kiegészítő garancia-összetevők elvárásait. A vastag betűvel szedett részek azokat az elvárásokat jelölik, melyek kifejezetten az összetett termékekre vonatkoznak csak (termékekre tehát nem).

6.2.5.1. Előkészítő eljárások (AGD_PRE.1) 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.

6.2.5.1.1. 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.

6.2.5.1.2. 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.

Amennyiben a TOE-t egy összetett termékben kliens komponensként fogják használni, az értékelőnek meg kell győződni arról, hogy az összetett termékben a kiszolgáló komponens kielégíti az üzemeltetési környezetet.

6.2.5.2. Üzemeltetési felhasználói útmutató (AGD_OPE.1) 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. 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.

6.2.5.3. A TOE megcímkézése (ALC_CMC.1) értékelése

Ennek az altevékenységnek a célja annak megállapítása, hogy az összetett termék integrátora egyértelműen megcímkézte-e az összetett terméket (azaz hozzárendelt-e egy egyértelmű hivatkozást).
Az ehhez az altevékenységhez szükséges értékelési bizonyíték:

a) az (összetett termékre vonatkozó) ST,
b) a tesztelésre alkalmas TOE.

6.2.5.3.1. Az ALC_CMC.1.1E értékelői akció

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

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

ALC_CMC.1-1 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.

Összetett TOE esetén alternatív megoldásként a TOE által biztosított egyedi hivatkozás lehet a TOE-t alkotó összes összetevő egyedi hivatkozásának kombinációja.
ALC_CMC.1-2 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.

Összetett TOE esetében a következők érvényesek: Az összetett IT TOE-t nem szükséges felcímkézni az egyedi (összetett) hivatkozásával, elég ha az egyes komponensek vannak felcímkézve saját megfelelő TOE hivatkozásukkal. Az IT TOE továbbfejlesztését igényelné, hogy az indítás és/vagy az üzemeltetés során fel legyen címkézve az összetett hivatkozással. Ha az összetett TOE-t az alkotóelem TOE-k formájában szállítják le, akkor a leszállított TOE elemek nem fogják tartalmazni az összetett hivatkozást. Az összetett TOE ST-je azonban 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.

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

6.2.5.4.1. 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 az összetett TOE;
b) az összetett TOE-t alkotó komponensek;
c) az összetett TOE-ra vonatkozó 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.

6.2.6. Összetett TOE garancia folyamatosságának biztosítása

Az összetett TOE garancia folyamatosságának biztosítására ugyanazok az alapelvek és követelmények vonatkoznak, mint amelyeket [4] a termék TOE-k esetén meghatározott.

Összetett TOE-k esetén a garancia folyamatosság biztosítása érdekében az alábbi kiegészítő követelményeknek is eleget kell tenni:

A garancia folyamatosságot biztosító rendszerbe csak olyan összetett TOE kerülhet, melynek legalább a kliens komponensére biztosított a garancia folyamatossága.

Amennyiben a kliens vagy kiszolgáló komponens garancia folyamatossági tevékenység tárgyát képezte a komponens értékelés befejezése óta eltelt időszakban, az összetett TOE értékelője mérlegelje a garancia folyamatosság tevékenység során felmért módosításokat (köztük a javításokat) az összetett TOE-ra vonatkozó független sebezhetőségi elemzés során (ACO_VUL).

A módosításokkal (köztük a javításokkal) kapcsolatos információk a garancia folyamatossági tevékenységek jelentéseiben szerepelnek (karbantartási jelentés és tanúsítvány karbantartás jegyzőkönyv). Ez kiegészítendő az útmutató dokumentációk bármilyen frissítésével, ami a módosítások miatt történt, és olyan információkkal, amelyek a módosításokkal kapcsolatban nyilvánosan hozzáférhetők (például gyártó weboldala).

7. Mellékletek

7.1. 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.

7.2. Tesztelés és más 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.

7.3. 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.

8. Bibliográfia

-

9. Rövidítésgyűjtemény

Jelen dokumentum a 6. táblázatban megadott rövidítéseket használja.

6. táblázat – A dokumentumban használt rövidítések

Rövidítés	**Angol**	**Magyar**
ACO	Assurance: Composition	“Kompozíció-összeállítás” garanciaosztály
ADV	Assurance: Development	“Fejlesztés” garanciaosztály
ADV_FSP	ADV: Functional specification	Funkcionális specifikáció 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_FLR	ALC: Flaw remediation	Hibajavítás 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

Rövidítés	Angol	Magyar
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_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
ACO_COR	ACO: Composition rationale	Komponens-összeállítás indoklás garanciacsalád
ACO_DEV	ACO: Development evidence	Fejlesztési bizonyíték garanciacsalád
ACO_REL	ACO: Reliance of dependent component	A kliens komponens környezetfüggősége garanciacsalád
ACO_CTT	ACO: Composed TOE testing	Összetett TOE tesztelése garanciacsalád
ACO_VUL	ACO: Composition vulnerability analysis	Kompozíció sebezhetőségi elemzése garanciacsalád
CAP	Composed Assurance Package	Összetett garanciacsomag
CAP-A	Composed Assurance Package-A	Alap összetett garanciacsomag
CAP-F	Composed Assurance Package-F	Fokozott összetett garanciacsomag
CAP-K	Composed Assurance Package-K	Kiemelt összetett garanciacsomag
CC	Common Criteria	Közös szempontok
CEM	Common Evaluation Methodology	Közös értékelési módszertan
DBMS	Data Base Management System	Adatbázis kezelő rendszer
EAL	Evaluation Assurance Level	Értékelési garanciaszint
ETR	Evaluation Technical Report	Értékelési jelentés
FAU	Functionality: Security audit	„Biztonsági naplózás" funkcionális osztály
FAU_GEN	FAU: Security audit data generation	A biztonsági naplók adatainak generálása funkcionális család
FDP	User data protection	"A felhasználói adatok védelme" funkcionális osztály
FDP_ACC	FDP: Access control policy	Hozzáférés ellenőrzési szabályzat funkcionális család
FDP_RIP	FDP: Residual information protection	Maradványinformáció védelem funkcionális család
FDP_ROL	FDP: Rollback	Visszagörgetés funkcionális család
FIA	Identification and authentication	"Azonosítás és hitelesítés" funkcionális osztály
FPR	Privacy	"A magántitok védelme" funkcionális osztály
FPR_UNO	FPR: Unobservability	Észrevétlenség funkcionális család
IT	Information Technology	Információs technológia, informatika
MIBÉTS	-	Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma
OS	Operational System	Operációs rendszer
OSP	Organisational Security Policy	Szervezeti biztonsági szabályzat
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