InfoCA v2.5
megbízható rendszer
hitelesítés-szolgáltatáshoz

BIZTONSÁGI ELŐIRÁNYZAT

Verzió:	1.1
Dátum:	2009. május 27.
Fájl:	InfoCA_ST_v11.doc
Minősítés:	Nyilvános
Oldalak:	137

Változáskezelés

Verzió	Dátum	Leírás
0.1	2006.07.17.	A szerkezet felállítása, a 3., 4. és 5. fejezetek kezdeti megfogalmazása a CIMC PP figyelembe vételével.
0.2	2006.08.15.	A fejlesztőkkel való konzultációk alapján kiegészített változat (2. fejezet kezdeti megfogalmazása)
0.3	2006.10.01.	A fejlesztőkkel való konzultációk alapján bővített változat (az 5. fejezet kezdeti megfogalmazása)
0.4	2006.11.02	A fejlesztőkkel való konzultációk alapján kiegészített változat (a 6. fejezet kezdeti megfogalmazása)
0.5	2006.11.15.	A 8. fejezet (indoklások) kezdeti megfogalmazása
0.6	2007.01.12.	A telepített szoftver vizsgálata alapján kiegészített változat.
0.9	2007.02.23.	Első teljes változat.
0.92	2007.05.14.	Az értékelőkkel történő első egyeztetés alapján kiegészített és módosított változat.
0.95	2007.05.21.	A biztonsági előirányzat v0.92 verziójára készült értékelési jelentés alapján kiegészített és pontosított változat.
1.0	2007.05.29.	A biztonsági előirányzat v0.95 verziójára készült értékelési jelentés alapján pontosított, a (TCA v2.0) értékelés alapjaként elfogadott végleges változat.
1.1	2009.05.27.	Az időbélyegzés és OCSP szolgáltatásokat, valamint az SHA-256, SHA-348 és SHA-512 algoritmusokat is támogató új TOE verzió (InfoCA v2.5) újraértékelésének alapjaként elfogadott, kiegészített változat.

Tartalomjegyzék

1. Bevezetés

Ez a fejezet dokumentum-kezelő és áttekintő információkat tartalmaz.
Az 1.1 alfejezet a biztonsági előirányzatok azonosításhoz, katalogizálásához, regisztrációba vételéhez, illetve hivatkozásokhoz szükséges azonosító és leíró információkat tartalmazza.
Az 1.2 alfejezet egy potenciális felhasználó számára ad olyan részletességű áttekintést, melynek alapján eldöntheti a témában való érdekeltségét.
Az 1.3 alfejezet felsorolja jelen biztonsági előirányzat elkészítéséhez felhasznált szakirodalmat.
Az 1.4 alfejezet a 2-9. fejezetek rövid leírását tartalmazza.
Az 1.5 alfejezet pedig a CC jelen értékelésnél irányadó verzióját határozza meg.

1.1 Azonosítás

Cím:	InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - Biztonsági előirányzat
Az értékelés tárgya:	InfoCA v2.5megbízható rendszer hitelesítés-szolgáltatáshoz
Az értékelés tárgya rövid neve:	InfoCA v2.5 vagy InfoCA rendszer
Értékelési garancia szint:	CC EAL4 + (kibővített EAL 4)
A biztonsági funkcióerősség:	nincs értelmezve
Verzió szám:	1.1
Dátum:	2009. május 27.
Szerző:	MÁV INFORMATIKA Zrt
Felhasznált védelmi profil[1]:	Certificate Issuing and Management Components Family of Protection Profiles (CIMC-PP) Version 1.0
CC-verzió:	Common Criteria v2.3

1.2 Áttekintés

Az InfoCA v2.5 (InfoCA rendszer) egy olyan speciális elektronikus aláírási termék, amely különböző hitelesítés-szolgáltatást biztosító funkciókkal rendelkezik.

Az InfoCA rendszer az alábbi hitelesítés-szolgáltatásokat támogatja:

Alap (kötelező) szolgáltatások:
- Regisztrációs szolgáltatás (az InfoCA rendszeren kívül valósul meg, de eredményét az InfoCA rendszer használja)
- Tanúsítvány előállítás szolgáltatás,
- Tanúsítvány szétosztás szolgáltatás,
- Visszavonás kezelés szolgáltatás,
- Visszavonás állapot szolgáltatás (CRL, OCSP).

Kiegészítő (opcionális) szolgáltatások:
- titkosító magánkulcs letétbe helyezése szolgáltatás,
- titkosító magánkulcs helyreállítása szolgáltatás,
- aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás (az InfoCA rendszeren kívül valósul meg),
- időbélyegzés szolgáltatás.

[1] A biztonsági előirányzat készítése során a referenciaként megadott védelmi profil számos elemét (többek között néhány, a védelmi profilban definiált, a Common Criteria 2. részében nem található funkcionális biztonsági követelmény is) felhasználásra került, ugyanakkor jelen biztonsági előirányzat védelmi profilnak való megfelelést nem állít (így a CIMC-PP-nek való megfelelést sem).

1.3 Kapcsolódó dokumentumok

Jelen biztonsági előirányzat az alábbi dokumentumok tartalmára épít:

- Certificate Issuing and Management Components Family of Protection Profiles (CIMC-PP) Version 1.0, October 2001
- International Standard ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security (CC) Version 2.3, August 2005
- Common Methodology for Information Security Evaluation (CEM) Version 2.3, August 2005
- CWA 14167-1:2003 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures
- RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol, June 1999
- RFC 3161 X.509 Internet Public Key Infrastructure - Time-Stamp Protocol, August 2001
- RFC 5280: X.509 Internet Public Key Infrastructure - Certificate and CRL Profile, May 2008

1.4 A biztonsági előirányzat szerkezete

A 2., 3., és 4. fejezetek az értékelés tárgya (TOE) leírását, a biztonsági környezetet (feltételezéseket, fenyegetéseket és szervezeti biztonsági szabályzatokat), illetve a biztonsági célokat adják meg.
Az 5.1 alfejezet a környezetre, az 5.2 pedig a TOE-ra vonatkozó funkcionális biztonsági követelményeket tartalmazza.
Az 5.3 alfejezet a TOE garanciális biztonsági követelményeit írja le.
A 6. fejezet részletesen kifejti az értékelés tárgya által megvalósított biztonsági funkciókat.
A 7. fejezet a PP megfelelőségi nyilatkozatot, a 8. fejezet az indoklásokat, a 9. pedig egy terminológiai áttekintést és a használt rövidítések listáját tartalmazza.

1.5 Common Criteria megfelelőség

Ez a biztonsági előirányzat a CC 2.3 verzióján alapul (ISO/IEC 15408 IT biztonság értékelési követelményei, 1. rész: Bevezetés és általános modell, 2. rész: Funkcionális biztonsági követelmények, 3. rész: Garanciális biztonsági követelmények.).
Kiterjeszti a 2. részt, valamint kibővíti a 3. részt, EAL4-es értékelési garanciaszinten /a kibővítés az „ALC_FLR.2 Hibajelentési eljárások” garanciaösszetevő hozzávételét jelenti/

A CC 1.rész 7.4 pontja szerint:

Kiterjeszti a 2. részt: a PP vagy a TOE kiterjeszti a 2. részt, ha a funkcionális követelmények olyan összetevőket foglalnak magukban, amelyek nem szerepelnek a 2. részben.

Kibővíti a 3. részt: a PP vagy a TOE kibővíti a 3. részt, ha a garanciális követelmények valamilyen EAL vagy garancicsomag formájában vannak megfogalmazva, továbbá más garanciális összetevőt is tartalmaznak a 3. részből.

2. Az értékelés tárgyának (TOE) leírása

Az InfoCA rendszer PKI alapú alkalmazásokhoz különböző tanúsítványokat biztosít és kezel. Különböző alrendszerekből áll, ezek különböző speciális funkcionalitást biztosítanak. Bár jelen biztonsági előirányzat elsősorban a biztonsági követelményekre koncentrál, ez a fejezet az egész TOE működéséről ad áttekintést.

2.1 Az InfoCA rendszer alap és kiegészítő szolgáltatásai

Az InfoCA rendszer alap (kötelező) szolgáltatásai az alábbiak:

- tanúsítvány előállítás szolgáltatás (funkciók: kezdeti tanúsítvány előállítás, tanúsítvány megújítás, tanúsítvány módosítás),
- tanúsítvány szétosztás szolgáltatás (funkciók: tanúsítvány exportálás LDAP-ba, LDAP újraépítése adatbázisból),
- visszavonás kezelés szolgáltatás (funkciók: tanúsítvány visszavonás, tanúsítvány felfüggesztés, tanúsítvány újra érvényesítés),
- visszavonás állapot szolgáltatás (funkciók: CRL publikálása LDAP-ba, CRL exportálása állományba, OCSP kérésre OCSP válasz adása).

Az InfoCA rendszer (konfigurációtól függően opcionálisan) az alábbi kiegészítő szolgáltatásokat is támogatja:

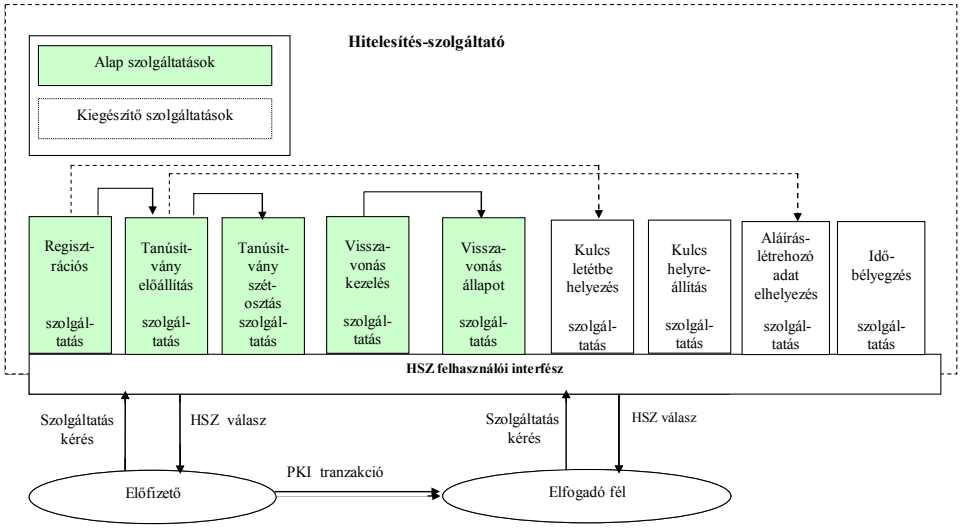
- időbélyegzés szolgáltatás (funkció: időbélyegzés)
- titkosító magánkulcs letétbe helyezése szolgáltatás (funkció: letétbe helyezés),
- titkosító magánkulcs helyreállítása szolgáltatás (funkció: helyreállítás funkció)

2.3 Az InfoCA rendszer felhasználói

Az InfoCA rendszer felhasználói kizárólag megbízható munkakört betöltő, különböző jogosultságokkal rendelkező belső felhasználók, akik telepítik, konfigurálják, adminisztrálják, üzemeltetik, karban tartják, illetve ellenőrzik az InfoCA rendszert. (A bizalmas munkakörök részletesen a 6.1.1 alfejezetben kerülnek kifejtésre.)

2.4 Az InfoCA rendszer általános felépítése

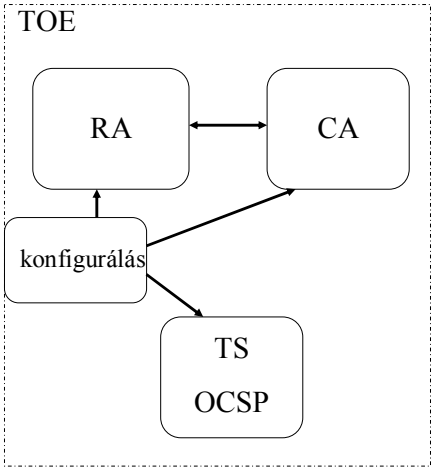
Az InfoCA rendszert alapvetően egy hitesítés-szolgáltató megbízható rendszerének tervezték, mely a hitesítés-szolgáltató által nyújtott (alap és kiegészítő) szolgáltatásokat valósítja meg, vagy nyújt a megvalósításhoz műszaki támogatást, ahogyan azt a 2-1. ábra szemlélteti. (Az ábrán szereplő regisztrációs, valamint aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatást az InfoCA rendszer környezete valósítja meg.)



2-1. ábra: Az InfoCA rendszer általános felépítése

2.5 Az InfoCA rendszer logikai szerkezete

Az InfoCA rendszer logikai felépítését, alrendszereit és külső interfészeit, egyúttal az értékelés tárgya és az informatikai környezet határát mutatják be a 2-2. – 2-4. ábrák.
Az ábrákon szaggatott vonal jelzi az értékelés hatókörébe eső komponenseket.



2-2. ábra: Az InfoCA rendszer logikai felépítése

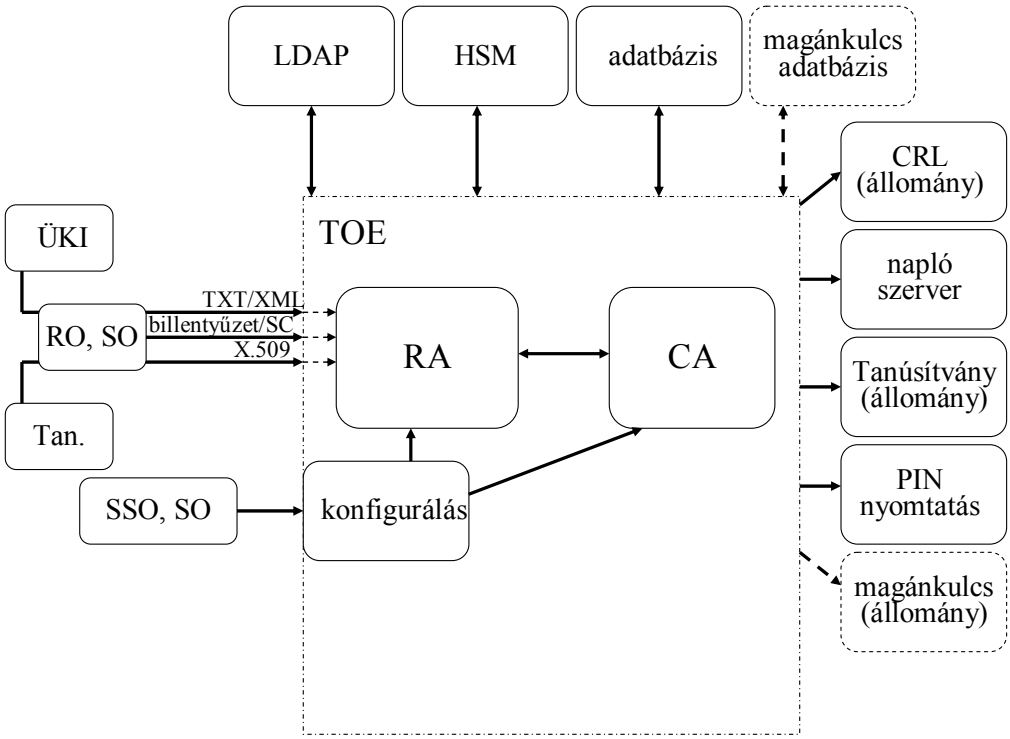
Az InfoCA rendszer (**TOE**) szerverből (a 2-2. ábrán **CA**), egy hozzá kapcsolódó kliensből (a 2-2. ábrán **RA**), valamint egy másik szerveren futó időbélyegzés és OCSP alrendszerből (a 2-2. ábrán TS, OCSP) áll.

Egy CA szerverhez elvileg kapcsolódhat több kliens is, egy kliens pedig több szerverrel is képes kommunikálni (biztosítva ezzel a rendelkezésre állás növelésének, illetve a terhelésmegosztásnak a lehetőségét). A szerver és kliensek közötti belső kommunikáció hitelesített.

A TS és OCSP alrendszerek elvileg futhatnak két különböző szerveren is, de ezek mindenképpen különböznek a CA szervertől.

Az InfoCA rendszer valamennyi alrendszere (RA, CA, TS, OCSP) különböző módon konfigurálható egy külső interfészen keresztül.

Az InfoCA rendszernek számos külső interfésze van, az alábbiak ezekről adnak egy áttekintést.



2-3. ábra: Az InfoCA rendszer határai (RA, CA)

Az InfoCA rendszer (annak RA és CA alrendszerei) különböző helyekről és formákban kaphatja meg a funkcióihoz szükséges adatokat:

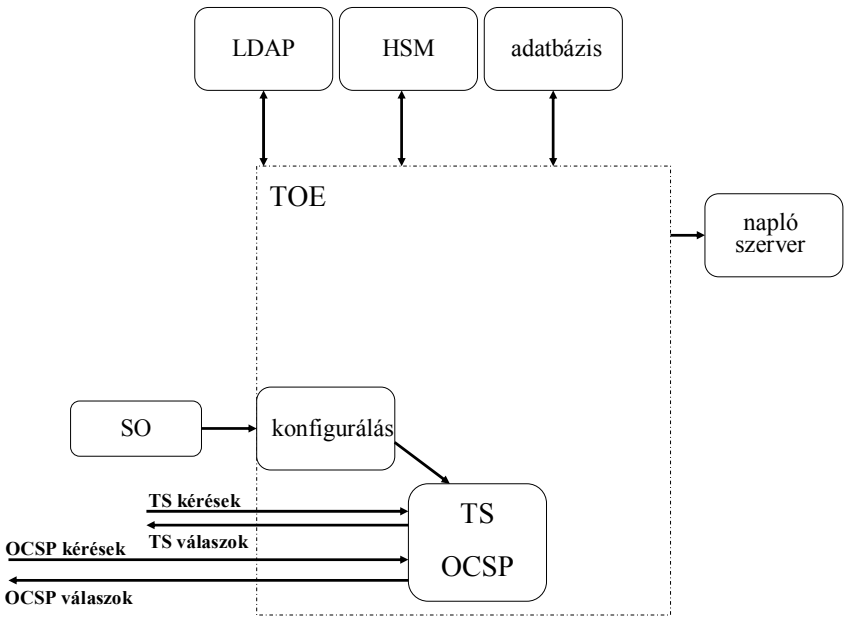
- az Ügyfél Kapcsolati Irodától (**ÜKI**) kapott TXT vagy XML formátumú állomány (RO általi) beolvasásával,
- az RA-t kezelő regisztrációs tisztviselő (**RO**) által **billentyűzet**ről történő beütéssel, illetve intelligens kártyáról (**SC**) történő beolvasással.
- X509-es szerkezetű **tanúsítvány**(oka)t tartalmazó állomány (RO általi) beolvasásával,
- a címtárban (**LDAP**) tárolt adatszerkezet lekérdezésével,
- a kriptográfiai hardver modultól **(HSM)** kapott válaszok fogadásával,
- saját **adatbázis**ából,
- **magánkulcs adatbázis**ából (az opcionális „titkosító magánkulcs letétbe helyezés” és „titkosító magánkulcs helyreállítás” szolgáltatások támogatása esetén).

Az InfoCA rendszer (annak RA és CA alrendszerei) különböző helyekre továbbítja az általa elkészített objektumokat:

- az előállított tanúsítványokat és az aktuális CRL-eket címtárba publikálják (**LDAP**),

- különböző kulcsműveletek végrehajtása érdekében parancsokat küld a kriptográfiai hardver modulnak **(HSM)**,
- különböző adatokat küld saját **adatbázis**ába,
- letétbe helyezett kulcsokat küld **magánkulcs adatbázis**ába (amennyiben támogatja a „titkosító magánkulcs letétbe helyezés” és „titkosító magánkulcs helyreállítás” szolgáltatásokat).
- archiválás céljából **CRL állomány**ba menti az aktuális CRL-t,
- a működés jellemzőit rögzítő naplóeseményeket egy **naplószerver**hez továbbítja,
- ügyfélhez való továbbítás céljából **tanúsítvány állomány**ba menti az aktuálisan előállított tanúsítványokat,
- a PKCS#12-es formátumban kibocsátott tanúsítványokhoz, illetve az opcionálisan kezelt aláírás-létrehozó eszközökhöz (intelligens kártyákhoz) tartozó PIN kódokra védett módon elvégezteti a **PIN nyomtatás**t,
- PKCS#12-es formátumban kiadja a **magánkulcs állomány**t (amennyiben támogatja a „titkosító magánkulcs letétbe helyezés” és „titkosító magánkulcs helyreállítás” szolgáltatásokat).

A 2-4 ábra a TS és OCSP alrendszerek határait és külső interfészeit tekinti át.



2-4. ábra: Az InfoCA rendszer határai (TS, OCSP)

A biztonsági tisztviselők (SO) által konfigurálható TS (időbélyegzés) alrendszer:

- az RFC 3161 szabvány előírásainak megfelelő szabványos időbélyeg kérésekre szabványos időbélyeg válaszokat hoz létre,
- az időbélyeg tokeneket a HSM-ben generált és tárolt magánkulccsal aláírattatja,
- a naplószerverre továbbít (archiválási célból) minden időbélyeg tokent.

A biztonsági tisztviselők (SO) által konfigurálható OCSP alrendszer:

- az RFC 2560 szabvány előírásainak megfelelő szabványos OCSP kérésekre szabványos OCSP válaszokat hoz létre,
- a konfigurált üzemmódtól függően az OCSP válaszokat az LDAP vagy az adatbázis információi alapján állítja össze,
- az OCSP válaszokat a HSM-ben generált és tárolt magánkulccsal aláírattatja,
- a naplószerverre továbbít (archiválási célból) minden OCSP kérést és OCSP választ.

2.6 Az InfoCA rendszer fizikai architektúrája az értékelt kiépítésben

Az InfoCA rendszer működéséhez szükséges főbb elemek a következők:

CA alrendszer (a TOE részét képezi):

- InfoCA.exe (a CA alrendszer funkcionalitását automatikusan megvalósító alkalmazás)
- Setup_InfoCA.exe (az InfoCA.exe telepítését végző alkalmazás)
- InfoCAKeySetup.exe (a telepített InfoCA program kódjába a három SSO tanúsítványt bejuttató alkalmazás)
- InfoCASetup.exe (a telepített InfoCA /s ezen keresztül a InfoRA/ konfigurálását végző alkalmazás)
- CertSigner.dll (3 verzió: az egyik a szoftveres aláíráshoz, a másik kettő a HSM modulokkal (Luna, nShield) történő aláíráshoz)
- ExtConfig.dll (2 verzió: az egyik a kulcsvisszaállítás támogatáshoz, a másik annak tiltáshoz)

CA-kiegészítők (nem része a TOE-nak):

- sql script (adatbázis struktúra)
- ca.config.xml, ca.so.xml, ca.ro.xml (konfigurációs állományok)

RA alrendszer (a TOE részét képezi)**:**

- InfoRA.exe (az RA alrendszer funkcionalitását megvalósító alkalmazás)
- Setup_InfoRA.exe (az InfoRA.exe telepítését végző alkalmazás)

RA-kiegészítők (nem része a TOE-nak):

- CardApi.dll (intelligens kártya API)
- starcertpers.dll (intelligens kártya driver)
- ra.xml (konfigurációs állomány)

TS alrendszer (a TOE részét képezi)**:**

- TSSResponder.dll (az időbélyeg kéréseket kiszolgáló API)
- TSSResponderIsapi.dll (az időbélyeg kéréseket TSSResponder.dll–nek átadó API)

TS-kiegészítők (nem része a TOE-nak):

- Microsoft IIS (futtatási környezetet biztosító webszerver)
- TimeServer.exe (időszinkronizálást megvalósító alkalmazás)
- tss.config.xml (konfigurációs állomány)
- timeserver.config.xml (konfigurációs állomány)
- CertSigner.dll (a HSM modullal történő aláíráshoz)
- HSM modul (Luna vagy nShield)

OCSP alrendszer (a TOE részét képezi)**:**

- OCSPResponder.dll (az OCSP kéréseket kiszolgáló API)
- OCSPResponderIsapi.dll (az OCSP kéréseket OCSPResponder.dll–nek átadó API)

OCSP-kiegészítők (nem része a TOE-nak):

- Microsoft IIS (futtatási környezetet biztosító webszerver)
- ocsp.config.xml (konfigurációs állomány)
- CertSigner.dll (a HSM modullal történő aláíráshoz)
- HSM modul (Luna vagy nShield)

Az InfoCA rendszer különböző fizikai kiépítésekben működőképes.

Egy CA szerverhez (a 2-2. ábrán CA) több kliens (a 2-2. ábrán RA) is kapcsolódhat, egy kliens pedig több szerverrel is képes kommunikálni, biztosítva ezzel többek között a rendelkezésre állás növelésének, illetve a terhelésmegosztásnak a lehetőségét.
Az aláíró modul a tanúsított SafeNet Luna® Luna® PCICryptographic Module v2.2 és az nShield F3 500 PCI kriptográfiai hardver modulok (HSM) egyikét kezeli szabványos PKCS#11-es interfészen keresztül.
A szerver (CA) az értékelt kiépítésekben az alábbi platformokon futott:

- Windows 2003 Szerver, Enterprise edition, SP1
- .Net 3.0 futtató környezet, Microsoft Message Queue

A kliens (RA) az értékelt kiépítésekben az alábbi platformokon futott:

- MS Windows XP, Professional, SP2, Microsoft Message Queue

A szerver és kliens az értékelt kiépítésekben azonos és külön gépeken egyaránt futott.
A szerver és kliens közötti kommunikációs kapcsolat alapja a Queue interface modulok esetén az értékelt kiépítésekben a következő volt:

- MS MessageQueue

Az informatikai környezet részét képező adatbázis szerver (adatbázis) az értékelt kiépítésben a következő volt:

- MS SQL Server 2005 Express edition

Az informatikai környezet részét képező LDAP szerver az értékelt kiépítésben a következő volt:

- Openldap v2.2.29

Az informatikai környezet részét képező Syslog szerver az értékelt kiépítésben a következő volt:

- Syslog-win32-0.3

A TS és OCSP alrendszerek (a 2-2. ábrán TS, OCSP) elvileg futhatnak két különböző szerveren is. Akár egy, akár két szerveren futnak, ezeknek mindenképpen különbözniük kell a CA szervertől. Az informatikai környezet részét képező, a TS és OCSP alrendszereket futtató webszerver az értékelt kiépítésben a következő volt:

- Microsoft Internet Information Server 6.0

A fentieket összefoglalva a TOE és környezete az alábbiak:
CA szerver (CA) TOE elemei:

- InfoCA.exe (2.0.0.31)
- InfoCASetup.exe (2.0.4.2)
- Setup_InfoCA.exe (2.0.0.31)
- CertSigner.dll (2.0.0.14)
- CertSigner_NShield.dll (2.0.0.9)
- ExtConfig.dll (1.0.1.21/1.0.1.22, norec/rec)

CA szerver (CA) környezet elemei:

- Windows 2003 Szerver, Enterprise edition, SP1
- Intel P4, 1,8 GHz
- 256 MB RAM
- MS SQL Szerver 2005
- OpenLDAP 2.2.29
- Syslog-win32-0.3
- nShield F3 500 PCI kriptográfiai hardver modul (egyik HSM)
- SafeNet Luna® PCICryptographic Module v2.2 (másik HSM)

- .NET 3.0

Kliens (RA) TOE elemei:
- InfoRA.exe (2.0.4.3)
- Setup_InfoRA.exe (2.0.4.3)

Kliens (RA) környezet elemei:
- Windows XP, Professional, SP2
- Intel P4 Cel., 2,4 GHz
- 768 MB RAM
- .NET 3.0
- Omnikey CardMan 3121
- Oberthur CosmopolIC SmartCard
- Giesecke, SPK 2.3 Standard V7.0 T=1, SmartCard (StarCert)
- Giesecke, StarSign

Webszerver (TS, OCSP) TOE elemei:
- TSSResponder.dll (2.0.1.14)
- TSSResponderIsapi.dll (2.0.0.67)
- TimeServer.exe (2.0.3.0)
- OCSPResponder.dll (2.0.1.1)
- OCSPResponderIsapi.dll (2.0.0.16)

Webszerver (TS, OCSP) környezet elemei:
- nShield F3 500 PCI kriptográfiai hardver modul (egyik HSM)
- SafeNet SafeNet Luna® PCICryptographic Module v2.2 (másik HSM)
- Microsoft Internet Information Server 6.0

2.7 Az InfoCA rendszer különböző üzemmódjai

Az InfoCA rendszer értékelt kiépítésének működése nagy szabadsági fokkal tovább szabályozható, különböző biztonsági jellemzők (konfigurációs paraméterek) telepítés során történő értékadásával. Bizonyos konfigurációs paraméter csoportok beállításával az InfoCA rendszer jellemző működési módokba, ún. üzemmódokba kapcsolható.

Jelen biztonsági előirányzat az alábbi üzemmódokat különbözteti meg (mindegyik a 2.6 alatt meghatározott értékelt kiépítés egy-egy konfigurációs változata):

- ***Kulcsvisszaállítás lehetőségét támogató/nem támogató üzemmód (KeyRec)***

  Az ExtConfig.dll könyvtárnak (mely az InfoCA rendszer informatikai környezetéhez tartozó egyik CA-kiegészítő) két változata van, az egyik elvileg lehetővé teszi a magánkulcsok visszaállítását, a másik nem. A telepítés során (az InfoCA_installer.exe alkalmazás futtatásakor) a rendszeradminisztrátor választja ki a megfelelő KeyRec üzemmódot).
  Jelen biztonsági előirányzat a KeyRec üzemmód mindkét állapotára vonatkozik.

- ***A kriptográfiai algoritmusok szoftveres/hardveres megvalósítása (Crypto)***

  A CertSigner.dll könyvtárnak (mely az InfoCA rendszer informatikai környezetéhez tartozó egyik CA-kiegészítő) két változata van, az egyik egy hardver kriptográfiai modul (HSM) szolgáltatásait aktivizálja a különböző kriptográfiai algoritmusok (köztük a atnúsítványok digitális aláírásának) megvalósításához, a másik szoftveresen valósítja meg ezeket. A telepítés során (a InfoCA_installer.exe alkalmazás futtatásakor) a rendszeradminisztrátor választja ki a megfelelő Crypto üzemmódot).

Jelen biztonsági előirányzat kizárólag a HSM modul támogatására építő üzemmódra vonatkozik (a szoftveres üzemmód kizárólag tesztelési célokat szolgál).

3. A TOE biztonsági környezete

3.1 Védendő értékek

Az InfoCA rendszer által védendő értékek az alábbiak:

Rendelkezésre állás szempontjából:

Az InfoCA rendszer alábbi tulajdonságai a magas rendelkezésre állás elérhetőségét támogatja:

- nagy megbízhatóságú elemek alkalmazása az értékelt kiépítésben (tanúsított kriptográfiai hardver eszköz, megbízható hardver és operációs rendszer platform),
- szerver – kliens kiépítés szabad konfigurálhatósága,
- rugalmas konfigurálási lehetőség (pl. egy InfoCA rendszeren belül több virtuális CA létrehozásának lehetősége).

A fentiek ellenére az InfoCA rendszer rendelkezésre állását jelen biztonsági előirányzat az informatikai és nem informatika környezet hatókörébe utalja.

Bizalmasság szempontjából:

Az alábbi ügyfél adatok bizalmassága:

- a kulcsvisszaállítás lehetősége érdekében tárolt titkosító magánkulcsok.

A rendszer alábbi kritikus biztonsági paramétereinek a bizalmassága:

- tanúsítvány aláíró magánkulcsok,
- infrastrukturális titkos és magánkulcsok,
- rendszervezérlési titkos és magánkulcsok,
- megbízható munkakört betöltő felhasználók (magánkulcsot aktivizáló) PIN kódjai.

Sértetlenség szempontjából:

Az alábbi ügyfél adatok sértetlensége:

- tanúsítványok,
- a kulcsvisszaállítás lehetősége érdekében tárolt titkosító magánkulcsok,
- időbélyeg kérések,
- időbélyeg tokenek (válaszok),OCSP kérések,
- OCSP válaszok.

Az alábbi rendszeradatok sértetlensége:

- a felhasználói fiókok (account-ok) tartalma (jogosultságok),
- konfigurációs állományok,
- naplórekordok.

Az InfoCA rendszert veszélyeztető külső támadókkal szemben feltételezett támadási képesség: alacsony.

3.2 A biztonságos használatra vonatkozó feltételezések[2]

3.2.1 Személyi feltételek

A.Auditors Review Audit Logs
A biztonság-kritikus eseményekről naplóbejegyzés készül, s ezeket rendszeresen átvizsgálják.

A.Authentication Data Management
A TOE működési környezetében érvényben van egy olyan hitelesítési adat (jelszó vagy PIN kód) kezelésre vonatkozó szabályzat, melynek betartásával a felhasználók hitelesítési adataikat megfelelő időközönként, és megfelelő értékekre (azaz megfelelő hosszúsággal, előtörténettel, változatossággal stb. rendelkező értékekre) változtatják.

A.Competent Administrators, Operators, Officers and Auditors
A bizalmi munkakörök betöltésére szakértő személyek lesznek kijelölve a TOE és az általa tartalmazott információk biztonságának kezelésére.

A.CPS
Minden bizalmi munkakört betöltő személy jól ismeri azt a hitelesítési rendet (CP) és szolgáltatási szabályzatot (CPS), mely alatt a TOE-t működtetik.

A.Disposal of Authentication Data
A hitelesítési adatokat és az ezekhez tartozó jogosultságokat eltávolítják, miután a hozzáférési jogosultság megszűnt (pl. munkahely vagy munkakör változás következtében).

A.Malicious Code Not Signed
A TOE számára küldött rosszindulatú futtatható kódot nem írja alá egy megbízható entitás.

A.Notify Authorities of Security Issues
A bizalmi munkaköröket betöltő személyeknek értesíteniük kell a megfelelő vezetőket a rendszert érintő bármely biztonsági eseményről, a további adatvesztés vagy kompromittálódás lehetőségének minimalizálása érdekében.

A.Social Engineering Training
A bizalmi munkaköröket betöltő személyek képzettek a "social engineering" típusú támadások megakadályozási technikáiban.

A.Cooperative Users
A felhasználóknak néhány olyan feladatot vagy feladatcsoportot is végre kell hajtani, amelyek biztonságos IT környezetet igényelnek. A felhasználóknak a TOE által kezelt információk közül legalább néhányhoz hozzá kell férniük, egyúttal feltételezzük, hogy a felhasználók együttműködő módon tevékenykednek.

3.2.2 Kapcsolódási feltételek

A.Operating System
Az operációs rendszer úgy kerül kiválasztásra, hogy az rendelkezik a TOE által elvárt azon funkciókkal, melyek a 3.3 alfejezetben meghatározott fenyegetések kivédéséhez szükségesek.

[2] A feltételezésekre A. -tal kezdődő jelölést használunk (A: Assumption)

3.2.3 Fizikai feltételek

A.Communication Protection
A rendszer megfelelő fizikai védelemmel van ellátva a kommunikáció elvesztésével, azaz a kommunikáció rendelkezésre állásának elvesztésével szemben.

A.Physical Protection
A TOE azon hardver, szoftver és förmver elemei, amelyek létfontosságúak a TOE biztonsági politikája (TSP) érvényre juttatásához, védve vannak a jogosulatlan fizikai módosításokkal szemben.

3.3 Fenyegetések[3]

A fenyegetések négy csoportra oszthatók: jogosult felhasználók, rendszer, kriptográfia, illetve külső támadások.

3.3.1 Jogosult felhasználók

T.Administrative errors of omission
Egy bizalmi munkakört betöltő személy elmulaszt végrehajtani bizonyos funkciókat, amelyek alapvetően fontosak a biztonság szempontjából.

T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
Egy bizalmi munkakört betöltő személy véletlenül olyan hibát követ el, amely megváltoztatja a rendszer célul tűzött biztonsági szabályzatát, vagy rosszindulatúan módosítja a rendszer konfigurációját, hogy lehetővé tegye a biztonság megsértését.

T.User abuses authorization to collect and/or send data
Egy felhasználó visszaél jogosultságaival abból a célból, hogy helytelen módon gyűjtsön és/vagy küldjön érzékeny vagy a biztonság szempontjából kritikus adatokat.

T.User error makes data inaccessible
Egy felhasználó véletlenül felhasználói adatokat töröl, amellyel felhasználói adatokat hozzáférhetetlenné tesz.

3.3.2 Rendszer

T.Critical system component fails
Egy vagy több rendszer komponens hibája a rendszer kritikus fontosságú funkcionalitásának elvesztését okozza.

T.Malicious code exploitation
Egy jogosult felhasználó, informatikai rendszer vagy támadó olyan rosszindulatú kódot tölt le és hajt végre, amely rendellenes folyamatokat okoz, s ezzel megsérti a rendszer értékeinek sértetlenségét, rendelkezésre állását vagy bizalmasságát.

T.Message content modification
Egy támadó információt módosít, amelyet két gyanútlan entitás közötti kommunikációs kapcsolatból fog el, mielőtt azt a tervezett címzetthez továbbítaná.

[3] A fenyegetésekre T. -tal kezdődő jelölést használunk (T: Threat)

T.Flawed code
Egy rendszer vagy alkalmazás fejlesztője olyan kódot ad át, amely nem a specifikációnak megfelelően működik, vagy biztonsági réseket tartalmaz.

3.3.3 Kriptográfia

T.Disclosure of private and secret keys
Egy magán vagy titkos kulcsot nem megengedett módon felfednek.

T.Modification of private/secret keys
Egy magán vagy titkos kulcs módosítva lesz.

3.3.4 Külső támadások

T.Hacker gains access
Egy támadó jogosult felhasználónak álcázva magát, a hiányzó, gyenge és/vagy nem helyesen implementált hozzáférés ellenőrzés következtében a jogosult felhasználóhoz vagy egy rendszerfolyamathoz kapcsolódó műveletet végez, illetve nem észlelt hozzáférést nyer a rendszerhez, ami a sértetlenség, bizalmasság vagy rendelkezésre állás lehetséges megsértését eredményezi.

T.Hacker physical access
Egy támadó fizikai kölcsönhatásba lép a rendszerrel, hogy kiaknázza a fizikai környezetben meglévő sebezhetőségeket, ami a biztonság kompromittálódását eredményezheti.

T.Social engineering

Egy támadó a "social engineering" technikát alkalmazza arra, hogy információt szerezzen a rendszerbe lépésről, a rendszer felhasználásáról, a rendszer tervéről vagy a rendszer működéséről.

3.4 Szervezeti biztonsági szabályok[4]

P.Authorized use of information
Információ csak az engedélyezett cél(ok)ra használható fel.

P.Cryptography
Jogszabály vagy hatósági ajánlás által jóváhagyott kriptográfiai algoritmusokat kell használni a kriptográfiai műveletek végrehajtásakor.

P.Archiving
Biztosítani kell a CWA 14167-1 archiválásra vonatkozó mindhárom elvárását: AR1 (Archív adatok generálása), AR2 (Szelektálható keresés) és AR3 (Az archivált adatok sértetlensége).

P.TimeStampToken
A TOE biztonsági funkcióinak (a TSF-nek) biztosítania kell, hogy az RFC 3161 szabványnak megfelelő időbélyeg kérésekre adott időbélyeg válaszok érvényesek legyenek (megfeleljenek az RFC 3161 szabványnak).

[4] A szervezeti biztonsági szabályokra P. -tal kezdődő jelölést használunk (P: Policy)

4. Biztonsági célok[5]

Ez a fejezet a biztonsági célokat határozza meg, a csak a TOE-ra, a csak a környezetre, illetve a mindkettőre vonatkozókat külön-külön.

4.1 A TOE-ra vonatkozó biztonsági célok

O.Certificates
A TOE biztonsági funkcióinak (a TSF-nek) biztosítania kell, hogy a tanúsítványok, tanúsítvány visszavonási listák és tanúsítvány állapot információk érvényesek legyenek.

O.TimeStampToken
A TOE biztonsági funkcióinak (a TSF-nek) biztosítania kell, hogy az RFC 3161 szabványnak megfelelő időbélyeg kérésekre adott időbélyeg válaszok érvényesek legyenek (megfeleljenek az RFC 3161 szabványnak).

4.2 A TOE környezetére vonatkozó biztonsági célok

A csak a TOE környezetére vonatkozó biztonsági célok két csoportra oszthatók: informatikai és nem informatikai biztonsági célok.

4.2.1 A környezetre vonatkozó nem informatikai biztonsági célok

OE.Administrators, Operators, Officers and Auditors guidance documentation
Meg kell gátolni a bizalmi munkakört betöltő személyek hibáit azáltal, hogy megfelelő dokumentációt kell számukra biztosítani a TOE biztonságos konfigurálásához és üzemeltetéséhez.

OE.Auditors Review Audit Logs
A biztonság-kritikus eseményeket azonosítani és felügyelni kell, megkövetelve a rendszervizsgálóktól a naplóbejegyzések kellő (kockázatokkal arányban álló) gyakoriságú átvizsgálását.

OE.Authentication Data Management
A hitelesítési adat kezelésre vonatkozó szabályzat érvényre juttatásával biztosítani kell, hogy a felhasználók hitelesítési adataikat (jelszavaikat, aktivizáló kódjaikat) megfelelő időközönként, és megfelelő értékekre (azaz megfelelő hosszúsággal, előtörténettel, változatossággal stb. rendelkező értékekre) változtassák.

OE.Communication Protection
A rendszert megfelelő fizikai biztonság biztosításával védeni kell a kommunikációs képességekre irányuló fizikai támadásokkal szemben.

OE.Competent Administrators, Operators, Officers and Auditors
Biztosítani kell a TOE megfelelő kezelését a bizalmi munkakörök hozzáértő és feljogosított személyekkel való betöltésével a TOE és az általa tartalmazott információk biztonságának kezelésére.

[5] A biztonsági célokra az alábbi rövidítéseket használjuk: O.xxx TOE-ra vonatkozó célok esetén (O: Object) OE.xxx környezetre vonatkozó célok esetén (OE: Object for Environment), O(E).xxx TOE-re és környezetre vonatkozó célok esetén.

OE.CPS
Minden bizalmi munkakört betöltő személynek jól kell ismernie azt a hitelesítési rendet (CP) és szolgáltatási szabályzatot (CPS), mely alatt a TOE-t működtetik.

OE.Disposal of Authentication Data
Biztosítani kell a hitelesítési adatok és az ezekhez tartozó jogosultságok megfelelő eltávolítását, miután a hozzáférési jogosultság megszűnt (pl. munkahelyváltozás, vagy munkaköri felelősség megváltozása következtében).

OE.Installation
A TOE-ért felelős személyeknek biztosítaniuk kell, hogy a TOE olyan módon legyen szállítva, telepítve, kezelve és üzemeltetve, amely megőrzi az informatikai biztonságot.

OE.Malicious Code Not Signed
A TOE-t védeni kell a rosszindulatú kódokkal szemben, úgy, hogy a rendszerbe letöltött minden kódot aláír egy megbízható entitás.

OE.Notify Authorities of Security Issues
Értesíteni kell a megfelelő vezetőket a rendszert érintő bármely biztonsági eseményről, az adatvesztés vagy kompromittálódás lehetőségének minimalizálása érdekében.

OE.Physical Protection
A TOE-ért felelős személyeknek biztosítaniuk kell, hogy a TOE biztonságkritikus elemei védve legyenek az informatikai biztonságot veszélyeztető fizikai támadásokkal szemben.

OE.Social Engineering Training
A bizalmi munkakört betöltő személyek számára képzést kell biztosítani a "social engineering" típusú támadások megakadályozási technikáira.

OE.Cooperative Users
Biztosítani kell, hogy a felhasználók együttműködőek legyenek néhány olyan feladat vagy feladatcsoport végrehajtásában, amelyek biztonságos IT környezetet, s a TOE által kezelt információkat igényelnek.

OE.Lifecycle security
A fejlesztési fázisban olyan eszközöket és technikákat kell biztosítani, hogy használatukkal biztosítva legyen a biztonság TOE-ba tervezése. A működtetés során észlelni és javítani kell a hibákat.

OE.Repair identified security flaws
A gyártónak javítani kell a felhasználók által azonosított biztonsági hibákat.

4.2.2 A környezetre vonatkozó informatikai biztonsági célok

OE.Cryptographic functions
Jóváhagyott kriptográfiai algoritmusokat kell megvalósítani a titkosításra/dekódolásra, hitelesítésre és aláírás létrehozására/ellenőrzésére, jóváhagyott kulcsgenerálási technikákat kell alkalmazni, valamint tanúsított kriptográfiai modulokat kell használni.

OE.Operating System
A TOE IT környezete csak olyan operációs rendszert használhat, mely garantálja a TOE számára a tartomány szétválasztást és a biztonsági funkciók megkerülhetetlenségét.

OE.Periodically check integrity
Időszakosan ellenőrizni kell mind a rendszer, mind a szoftver sértetlenségét.

OE.Preservation/trusted recovery of secure state
Egy biztonsági komponens hibája esetén meg kell őrizni a rendszer egy biztonságos állapotát, és/vagy helyre kell állítani a rendszert egy biztonságos állapotába.

OE.Sufficient backup storage and effective restoration
Elegendő mentés tárolást és hatékony visszaállítást kell biztosítani a rendszer újra felépíthetősége érdekében.

OE.Trusted Path
Megbízható útvonalat kell biztosítani a felhasználó és a rendszer között. Megbízható útvonalat kell biztosítani a biztonság-kritikus (TSF) adatok számára, aminek mindkét végpontja megbízhatóan azonosított.

OE.Validation of security function
Funkciók és eljárások alkalmazásával biztosítani kell, hogy a biztonság-kritikus szoftver, hardver és förmver elemek helyesen működnek.

OE.Archiving
Biztosítani kell a CWA 14167-1 archiválásra vonatkozó mindhárom elvárását: AR1 (Archív adatok generálása), AR2 (Szelektálható keresés) és AR3 (Az archivált adatok sértetlensége).

4.3 A TOE-ra és környezetére egyaránt vonatkozó biztonsági célok

O(E).Configuration Management
Konfiguráció kezelési tervet kell megvalósítani. A konfiguráció kezelést abból a célból kell alkalmazni, hogy biztosítva legyen a rendszer csatlakoztatások (szoftver, hardver és förmver) és komponensek (szoftver, hardver és förmver) beazonosítása, a konfigurációs adatok naplózása, valamint a konfiguráció tételekben történő változások ellenőrzése.

O(E).Data import/export
Az adatok formájában megjelenő értékeket védeni kell a TOE felé vagy a TOE-tól történő átvitel közben, ahol az átvitel akár egy közbeiktatott nem megbízható komponensen keresztül, akár közvetlenül az emberi felhasználókhoz/tól történik.

O(E).Detect modifications of firmware, software, and backup data
Sértetlenség védelmet kell biztosítani a förmverek, a szoftverek, valamint a mentett adatok megváltozásának észlelése érdekében.

O(E).Individual accountability and audit records
Egyéni felelősségre vonhatóságot kell biztosítani a naplózott események vonatkozásában. A naplóeseményeknek tartalmazniuk kell az alábbiakat: az esemény dátuma és időpontja, az eseményért felelős entitás.

O(E).Integrity protection of user data and software
Megfelelő sértetlenség védelmet kell biztosítani a felhasználói adatokra és a szoftverre.

O(E).Limitation of administrative access
Az adminisztratív funkciókat úgy kell megtervezni, hogy a bizalmi munkakört betöltő személyek automatikusan ne rendelkezzenek hozzáféréssel a felhasználói objektumokhoz, a szükséges kivételeken kívül. Ellenőrizni kell azon bizalmi munkakört betöltő személyek rendszerhez való hozzáférését, akik a rendszer hibák elhárítását, illetve új verziók telepítését végzik.

O(E).Maintain user attributes
Az egyéni felhasználókkal kapcsolatosan kezelni kell egy biztonsági tulajdonság együttest (amely tartalmazhat szerepkörhöz tartozást, hozzáférési privilégiumokat stb.). Ez kiegészíti a felhasználói azonosítót.

O(E).Manage behavior of security functions
Menedzsment funkciókat kell biztosítani a biztonsági mechanizmusok konfigurálására, működtetésére és kezelésére.

O(E).Object and data recovery free from malicious code
Egy rosszindulatú kód bejutása és károkozása után egy működőképes állapotba kell tudni visszaállni. Ennek az állapotnak mentesnek kell lennie az eredeti rosszindulatú programkódtól.

O(E).Procedures for preventing malicious code
A rosszindulatú programkódokat meggátoló beépített eljárásoknak és mechanizmusoknak kell létezniük.

O(E).Protect stored audit records
A naplórekordokat védeni kell a jogosulatlan hozzáféréssel, módosítással vagy törléssel szemben abból a célból, hogy biztosítva legyen a felelősségre vonhatóság a felhasználói tevékenységekért.

O(E).Protect user and TSF data during internal transfer
Biztosítani kell a rendszeren belül átvitt felhasználói és TSF adatok sértetlenségét.

O(E).Require inspection for downloads
Meg kell követelni a letöltések/átvitelek felügyeletét.

O(E).Respond to possible loss of stored audit records
Amennyiben a napló eseménysor tároló területe megtelt vagy majdnem megtelt, a naplózható események korlátozásával meg kell akadályozni a naplórekordok lehetséges elvesztését.

O(E).Restrict actions before authentication
Korlátozni kell azokat a tevékenységeket, amelyeket egy felhasználó végrehajthat, mielőtt a TOE hitelesíti felhasználói azonosítóját.

O(E).Security-relevant configuration management
Kezelni és frissíteni kell a rendszer biztonsági szabályzatok adatait és érvényre juttató funkcióit, valamint a biztonság-kritikus konfigurációs adatokat annak biztosítása érdekében, hogy ezek konzisztensek legyenek a szervezeti biztonsági szabályzatokkal.

O(E).Security roles
Biztonsági szerepköröket kell fenntartani, és kezelni kell a felhasználóknak ezen szerepkörökkel való társítását.

O(E).Time stamps
Pontos időpontot kell biztosítani az időfüggő hitelesítés-szolgáltatásokhoz, valamint a napló események sorrendjének ellenőrizhetőségéhez.

O(E).User authorization management
Kezelni és frissíteni kell a felhasználói jogosultság és privilégium adatokat annak biztosítása érdekében, hogy ezek konzisztensek legyenek a szervezeti biztonsági és személyzeti szabályzatokkal.

O(E).React to detected attacks
Automatizált értesítést (vagy más reagálásokat) kell megvalósítani a TSF által felfedett támadások esetében a támadások azonosítása és elrettentése érdekében.

5. A biztonsági követelmények

Ebben a fejezetben a funkcionális biztonsági követelmény összetevőknél az alábbi jelöléseket alkalmazzuk:

- félkövér betűtípus [ ] jelek között: a jelen biztonsági előirányzat által tett kiegészítések, művelet befejezések, illetve
- aláhúzott betűtípus: szerkesztői finomítások.

5.1 Az informatikai környezetre vonatkozó funkcionális biztonsági követelmények

Ez az alfejezet a TOE informatikai környezetére vonatkozó funkcionális biztonsági követelményeket határozza meg (tehát amelyeket nem az InfoCA rendszernek kell kielégítenie).

Az 5-1. táblázat felsorolja a TOE informatikai környezetére (döntően a TOE számára futási környezetet biztosító operációs rendszerre) vonatkozó funkcionális biztonsági követelményeket (az átláthatóság megkönnyítése érdekében osztályonként csoportosítva).

Az 5-1.táblázatban szereplő összetevők többsége a CC 2. kötetéből való.
Az alábbi összetevők nem szerepelnek a CC 2. kötetében (kiterjesztett összetevők, melyeket a CIMC PP védelmi profilban megfogalmazottak szerint kerültek át jelen biztonsági előirányzatba):

- FCS_CKM_CIMC.5
- FDP_CIMC_BKP.1
- FDP_CIMC_BKP.2
- FMT_MTD_CIMC.4
- FMT_MTD_CIMC.7
- FPT_TST_CIMC.2
- FPT_TST_CIMC.3

A fenti összetevők ahhoz szükségesek, hogy egy olyan egyedi követelményt határozzanak meg, amelyekkel a Common Criteria nem foglalkozik.

Biztonsági naplózás (FAU)	Biztonsági riasztások	FAU_ARP.1
	A biztonság potenciális megsértésének vizsgálata	FAU_SAA.1
	Napló áttekintés	FAU_SAR.1
	Kiválogatható napló áttekintés	FAU_SAR.3
	A naplóesemények védett tárolása	FAU_STG.1
	A napló adatok elvesztésének meggátolása	FAU_STG.4
Kriptográfiai támogatás (FCS)	A kriptográfiai kulcsok generálása	FCS_CKM.1
	A kriptográfiai kulcsok megsemmisítése	FCS_CKM.4
	A TOE magán és titkos kulcsának nullázása	FCS_CKM_CIMC.5
	Kriptográfiai eljárás	FCS_COP.1
A felhasználói adatok védelme (FDP)	Részleges hozzáférés ellenőrzés (iteráció 1)	FDP_ACC.1
	Biztonsági tulajdonság alapú hozzáférés ellenőrzés (iteráció 1)	FDP_ACF.1
	CIMC mentés és visszaállítás	FDP_CIMC_BKP.1
	Kiterjesztett CIMC mentés és visszaállítás	FDP_CIMC_BKP.2
	A belső adatátvitel alapszintű védelme (iteráció 1, 2 és 3)	FDP_ITT.1
	Alapszintű adatcsere bizalmasság	FDP_UCT.1
	Archiválás	FDP_CWA_ARC.1
	Szelektálható keresés az archívumban	FDP_CWA_ARC.2
	Kiterjesztett archiválás	FDP_CWA_ARC.3
Azonosítás és hitelesítés (FIA)	Felhasználói tulajdonságok megadása (iteráció 1)	FIA_ATD.1
	Hitelesítési hibák kezelése (iteráció 1)	FIA_AFL.1
	Az azonosítás időzítése (iteráció 1)	FIA_UID.1
	A hitelesítés időzítése (iteráció 1)	FIA_UAU.1
	Felhasználó - szubjektum összerendelése (iteráció 1)	FIA_USB.1
Biztonsági menedzsment (FMT)	Menedzsment funkciók megadása (iteráció 1)	FMT_SMF.1
	Megszorítások a biztonsági szerepkörökre (iteráció 1)	FMT_SMR.2
	A biztonsági funkciók viselkedésének kezelése (iteráció 1 és 2)	FMT_MOF.1
	TSF adatok kezelése (iteráció 1 és 2)	FMT_MTD.1
	Biztonsági tulajdonságok kezelése (iteráció 1)	FMT_MSA.1
	Biztonságos biztonsági tulajdonságok (iteráció 1)	FMT_MSA.2
	Statikus tulajdonságok kezdeti értékadása (iteráció 1)	FMT_MSA.3
	A TSF magánkulcs bizalmasságának védelme	FMT_MTD_CIMC.4
	Kiterjesztett TSF magán és titkos kulcs export	FMT_MTD_CIMC.7
A TOE biztonságának védelme (FPT)	Az absztrakt gép tesztelése	FPT_AMT.1
	A TSF-ek közötti bizalmasság az adatátvitel során	FPT_ITC.1
	A belső adatátvitel alapszintű védelme (iteráció 1, 2 és 3)	FPT_ITT.1
	A TSP megkerülhetetlensége (iteráció 1)	FPT_RVM.1
	TSF tartomány szétválasztás	FPT_SEP.1
	Megbízható időbélyegzés	FPT_STM.1
	Szoftver/förmver sértetlenség teszt	FPT_TST_CIMC.2
	Szoftver/förmver betöltés teszt	FPT_TST CIMC.3
Megbízható útvonal / csatornák (FTP)	Megbízható útvonal	FTP_TRP.1

5-1. táblázat– Az informatikai környezetre vonatkozó funkcionális biztonsági követelmények

5.1.1 Bizalmi munkakörök kezelése

FMT_SMF.1 Menedzsment funkciók megadása (iteráció 1)

Hierarchikus alárendeltség más komponensekhez képest: nincs.

Függések: nincs

FMT_SMF.1.1 Az IT környezetnek képesnek kell lennie a következő (operációs rendszerre vonatkozó) biztonsági menedzsment funkciók végrehajtására:
[fiókok és szerepkörök kezelése, telepítés és konfigurálás, mentés és helyreállítás]

FMT_SMR.2 Megszorítások a biztonsági szerepkörökre (iteráció 1)

Hierarchikus fölérendeltség más összetevőkhöz képest: FMT_SMR.1

Függések: FIA_UID.1 Az azonosítás időzítése

FMT_SMR.2.1 Az IT környezetnek kezelnie kell az alábbi szerepköröket: **[rendszeradminisztrátor, rendszerüzemeltető**, **rendszervizsgáló]**.

FMT_SMR.2.2 Az IT környezetnek össze kell kapcsolnia a felhasználókat a szerepkörökkel.

FMT_SMR.2.3 Az IT környezetnek biztosítania kell az alábbi feltételek teljesülését: **[**
a) egy felhasználó nem tölthet be egyszerre rendszeradminisztrátor és rendszervizsgáló szerepkört,
b) egy felhasználó nem tölthet be egyszerre rendszeradminisztrátor és (a TSF által kezelt) tisztviselői (SSO, SO vagy RO) szerepkört,
c) egy felhasználó nem tölthet be egyszerre rendszervizsgáló és (a TSF által kezelt) tisztviselői (SSO, SO vagy RO) szerepkört.]

FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése (iteráció 1)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_SMR.1 Biztonsági szerepkörök

FMT_MOF.1.1 Az IT környezetnek a **[rendszeradminisztrátor]** szerepkörökre kell korlátoznia a **[fiókok és szerepkörök kezelése, telepítés és konfigurálás]** biztonsági funkciók **[viselkedésének a módosítását]**.

FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése (iteráció 2)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_SMR.1 Biztonsági szerepkörök

FMT_MOF.1.1 Az IT környezetnek a **[rendszerüzemeltető]** szerepkörökre kell korlátoznia a **[mentés és helyreállítás]** biztonsági funkció **[kiváltását]**.

FMT_MTD.1 TSF adatok kezelése (iteráció 1)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_SMR.1 Biztonsági szerepkörök

FMT_MTD.1.1 Az IT környezetnek a **[rendszervizsgáló]** szerepkörre kell korlátoznia a **[naplórekordok] [megtekintését és törlését]**.

FMT_MTD.1 TSF adatok kezelése (iteráció 2)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_SMR.1 Biztonsági szerepkörök

FMT_MTD.1.1 Az IT környezetnek a **[rendszeradminisztrátor]** szerepkörre kell korlátoznia a **[rendszeridő] [módosítását]**.

FMT_MSA.1 Biztonsági tulajdonságok kezelése (iteráció 1)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FDP_ACC Részleges hozzáférés ellenőrzés, vagy
FDP_IFC Részleges információ áramlás ellenőrzés]
FMT_SMR.1 Biztonsági szerepkörök
FMT_SMF.1 Menedzsment funkciók megadása

FMT_MSA.1.1 A TSF-nek érvényt kell szereznie a **[CIMC IT környezet hozzáférés ellenőrzés szabály**[6] **SFP]**-nek, azáltal, hogy a **[rendszeradminisztrátor]** szerepkörre korlátozza az alábbi biztonsági tulajdonság **[módosítását]**: **[szerepkörök]**

FMT_MSA.2 Biztonságos biztonsági tulajdonságok (iteráció 1)
Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: ADV_SPM.1 Informális TSP biztonságpolitikai modell
[FDP_ACC Részleges hozzáférés ellenőrzés, vagy
FDP_IFC Részleges információ áramlás ellenőrzés]
FMT_MSA_1 Biztonsági tulajdonságok kezelése
FMT_SMR.1 Biztonsági szerepkörök

FMT_MSA.2.1 A TSF-nek biztosítania kell, hogy csak biztonságos értékek legyenek elfogadva a biztonsági tulajdonságok számára.

FMT_MSA.3 Statikus tulajdonságok kezdeti értékadása (iteráció 1)
Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_MSA_1 Biztonsági tulajdonságok kezelése
FMT_SMR.1 Biztonsági szerepkörök

FMT_MSA.3.1 A TSF-nek érvényt kell szereznie a **[CIMC TOE környezet hozzáférés ellenőrzés szabály**[7] **SFP[**-nek, **[korlátozó]** alapértékek biztosításával az SFP-t érvényre juttató biztonsági tulajdonságokra.

FMT_MSA.3.2 A TSF-nek lehetővé kell tennie a **[rendszeradminisztrátor]** számára, hogy alternatív kezdeti értékeket adhasson meg az alapértelmezett értékek helyett egy objektum vagy információ létrehozásakor.

[6] melynek meghatározását lásd az 5.1.3.1 pontban
[7] melynek meghatározását lásd az 5.2.3.1 pontban

5.1.2 Azonosítás és hitelesítés

FIA_ATD.1 Felhasználói tulajdonságok megadása (iteráció 1)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FIA_ATD.1.1 Az IT környezetnek az alábbi, egyedi felhasználókhoz tartozó biztonsági tulajdonságokat kell kezelnie: **[a felhasználó által betölthető szerepkörök].**

FIA_AFL.1 Hitelesítési hibák kezelése (iteráció 1)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FIA_UAU.1 A hitelesítés időzítése

FIA_AFL.1.1 Az IT környezetnek észlelnie kell, amikor **[a rendszeradminisztrátor által konfigurálható pozitív egész szám]** sikertelen hitelesítési kísérlet történik **[az érintett felhasználói azonosító legutolsó sikeres hitelesítése óta]**.

FIA_AFL.1.2 Amennyiben a sikertelen hitelesítési kísérletek száma eléri vagy meghaladja a megadott értéket, az IT környezetnek az alábbiakat kell végrehajtania: **[az érintett felhasználó fiókját blokkolni kell].**

FIA_UID.1 Az azonosítás időzítése (iteráció 1)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FIA_UID.1.1 Az IT környezetnek a felhasználó azonosítása előtt az alábbi tevékenységek felhasználó nevében történő végrehajtását lehetővé kell tennie: **[felhasználó név és jelszó bekérése].**

FIA_UID.1.2 Az IT környezetnek meg kell követelnie minden felhasználó sikeres azonosítását, mielőtt bármilyen IT környezet által közvetített más tevékenységet lehetővé tenne az adott felhasználó nevében.

FIA_UAU.1 A hitelesítés időzítése (iteráció 1)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FIA_UID.1 Az azonosítás időzítése

FIA_UAU.1.1 Az IT környezetnek a felhasználó hitelesítése előtt az alábbi tevékenységek felhasználó nevében történő végrehajtását lehetővé kell tennie: **[felhasználó név és jelszó bekérése].**

FIA_UAU.1.2 Az IT környezetnek meg kell követelnie minden felhasználó sikeres hitelesítését, mielőtt bármilyen IT környezet által közvetített más tevékenységet lehetővé tenne az adott felhasználó nevében.

FIA_USB.1 Felhasználó - szubjektum összerendelése (iteráció 1)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs

Függések: FIA_ATD.1 Felhasználói tulajdonságok megadása

FIA_USB.1.1 Az IT környezetnek össze kell kapcsolnia a felhasználó megfelelő biztonsági tulajdonságait az adott felhasználó nevében tevékenykedő szubjektumokkal.

FTP_TRP.1 Megbízható útvonal

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs

Függések: nincs

FTP_TRP.1.1 Az IT környezetnek egy olyan kommunikációs útvonalat kell biztosítania saját maga valamint [**távoli**] felhasználók között, amely logikailag elkülönül minden más kommunikációs útvonaltól, és biztosítja a végpontjainak garantált azonosítását, valamint a kommunikációban résztvevő adatok védelmét a módosításokkal vagy felfedéssel szemben.

FTP_TRP.1.2 Az IT környezetnek lehetővé kell tenni, hogy [**a távoli felhasználók**] kezdeményezzék a kommunikációt a megbízható útvonal felhasználásával.

FTP_TRP.1.3 Az IT környezetnek meg kell követelnie a megbízható útvonal használatát a következőkre: [**kezdeti felhasználói hitelesítés**].

5.1.3 Hozzáférés ellenőrzés

FDP_ACC.1 Részleges hozzáférés ellenőrzés (iteráció 1)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés

FDP_ACC.1.1 Az IT környezetnek érvényt kell szereznie a **[CIMC IT környezet hozzáférés ellenőrzés szabály**[8] **SFP]**-nek, az alábbi szubjektumok és objektumok között, az alábbi műveletekre: **[minden felhasználó, minden fájl és minden fájl hozzáférési művelet]**

FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés (iteráció 1)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FDP_ACC.1 Részleges hozzáférés ellenőrzés
FMT_MSA.3 Statikus tulajdonságok inicializálása

FDP_ACF.1.1 Az IT környezetnek érvényt kell szereznie a **[CIMC IT környezet hozzáférés ellenőrzés szabály**[9] **SFP]**-nek az objektumok vonatkozásában a következők alapján: **[a szubjektum azonossága, a szubjektum által felvehető szerepkörök].**

FDP_ACF.1.2 Az IT környezetnek érvényre kell juttatnia az alábbi szabályt annak megállapítása érdekében, hogy egy művelet megengedett-e az ellenőrzött szubjektumok és ellenőrzött objektumok között**: [nyílt formában lévő magán és titkos kulcsok törlési lehetőségét a rendszeradminisztrátorokra kell korlátozni].**

FDP_ACF.1.3 Az IT környezetnek explicit módon kell megadnia a szubjektumok objektumokhoz való hozzáférési engedélyeit a következő kiegészítő szabályok alapján: **[nincsenek további szabályok].**

FDP_ACF.1.4 Az IT környezetnek explicit módon le kell tiltania a szubjektumok objektumokhoz való hozzáféréseit az alábbiak alapján: **[nincsenek további szabályok].**

FPT_SEP.1 TSF tartomány szétválasztás

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FPT_SEP.1.1 Az IT környezetben minden operációs rendszernek olyan biztonsági tartományt kell kezelnie a saját futásához, ami megvédi a nem megbízható egyedek általi beavatkozástól és hamisítástól.

FPT_SEP.1.2 Az IT környezetben minden operációs rendszernek érvényre kell juttatnia a szétválasztást a szubjektumok biztonsági tartománya között a saját TSC-jében.

[8] melynek meghatározását lásd az 5.1.3.1 pontban
[9] melynek meghatározását lásd az 5.1.3.1 pontban

FPT_RVM.1 A TSP megkerülhetetlensége (iteráció 1)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FPT_RVM.1.1 Az IT környezetben minden operációs rendszernek biztosítania kell, hogy a saját TSP-jét érvényre juttató funkciók valóban meghívódnak, és sikeresen befejeződnek, mielőtt a saját TSF hatáskörén belüli funkciók futása lehetővé válik.

5.1.3.1 CIMC IT környezet hozzáférés ellenőrzés szabály

Az IT környezetnek támogatnia kell egy olyan "CIMC IT környezet hozzáférés ellenőrzési szabály" adminisztrálását és érvényre juttatását, amely az alábbiakban ismertetésre kerülő lehetőségeket biztosítja.

A szubjektumok (emberi felhasználók) számára a következők alapján van biztosítva az objektumokhoz (adatok/fájlok) való hozzáférés:

1. A hozzáférést kérő szubjektum azonossága,
2. Az a szerepkör (vagy szerepkörök), amely(ek)nek a felvételére a szubjektum fel van jogosítva,
3. Az igényelt hozzáférés típusa,
4. A hozzáférési kérelem tartalma, és
5. Egy titkos vagy magánkulcs birtoklása, ha ez szükséges.

A szubjektum azonosítás magában foglalja az alábbiakat:

- különböző hozzáférési jogosultságokkal rendelkező személyek,
- különböző hozzáférési jogosultságokkal rendelkező szerepkörök,
- egy vagy több különböző hozzáférési jogosultságokkal rendelkező szerepkörrel felruházott személyek

Közvetlen engedélyezéssel vagy megtagadással járó hozzáférés típusok:

- olvasás,
- írás,
- végrehajtás.

Minden objektumra közvetlenül meg kell adni egy tulajdonos szubjektumot és egy szerepkört. Az objektum tulajdonosának vagy a szerepkör(ök)nek lesz a kötelessége a jogosultságok a jelen biztonsági előirányzatnak megfelelő kijelölése és kezelése.

5.1.4 Kulcskezelés

A TOE IT környezete egy külön hardver kriptográfiai modult alkalmaz a legtöbb kriptográfiai funkció végrehajtására. Az alábbi követelmények erre a modulra (HSM) vonatkoznak.

5.1.4.1 Kulcs létrehozás

Ez az alfejezet a kriptográfiai kulcsok IT környezet általi előállítására vonatkozó követelményeket adja meg.

FCS_CKM.1 A kriptográfiai kulcsok generálása

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FCS_CKM.2 A kriptográfiai kulcsok szétosztása vagy
FCS_COP.1 Kriptográfiai működés]
FCS_CKM.4 A kriptográfiai kulcsok megsemmisítése
FMT_MSA.2 Biztonságos biztonsági tulajdonságok

FCS_CKM.1.1 A **FIPS 140 szerint tanúsított kriptográfiai modulnak** a kriptográfiai kulcsokat az alábbiaknak megfelelően kell előállítania: [**DES, 3DES, RSA**], **melyek megfelelnek a következőknek:** [**FIPS PUB 186-2 Appendix3 (DES, 3DES), FIPS PUB 186-2 (RSA)**].

5.1.4.2 Kulcs megsemmisítés

Ez az alfejezet a nyílt formában lévő magán és titkos kulcsok IT környezet általi nullázására/megsemmisítésére vonatkozó követelményeket adja meg.

FCS_CKM.4 A kriptográfiai kulcsok megsemmisítése

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FDP_ITC.1 A biztonsági jellemzők nélküli felhasználói adatok importja vagy
FCS_CKM.1 A kriptográfiai kulcsok generálása]
FMT_MSA.2 Biztonságos biztonsági tulajdonságok

FCS_CKM.4.1 Az IT környezetnek a kriptográfiai kulcsokat a következő kriptográfiai kulcs megsemmisítési módszernek megfelelően kell megsemmisítenie: [**bármely FIPS által jóváhagyott vagy javasolt kulcs megsemmisítési mód**], amelyek megfelelnek a következőnek: [**FIPS 140-2**].

FCS_CKM_CIMC.5 A TOE magán és titkos kulcsának nullázása

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FCS_CKM.4 A kriptográfiai kulcsok megsemmisítése, vagy
FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés]

FCS_CKM_CIMC.5.1 Az IT környezetnek lehetőséget kell biztosítania a FIPS 140 szerint tanúsított kriptográfiai modulon belül nyílt formában tárolt titkos és magán kulcsok nullázására.

FMT_MTD_CIMC.4 A TSF magánkulcs bizalmasságának védelme

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FMT_MTD_CIMC.4.1 Az IT környezetben a CIMC (tanúsítványokat aláíró) magánkulcsokat vagy egy FIPS 140 szerint tanúsított kriptográfiai modulban, vagy titkosított formában kell tárolni. Ha a CIMC (tanúsítványokat aláíró) magánkulcsokat titkosított formában tárolják, a titkosítást egy FIPS 140 szerint tanúsított kriptográfiai modulban kell végrehajtani.

FMT_MTD_CIMC.7 Kiterjesztett TSF titkos és magán kulcs export

Hierarchikus fölérendeltség más összetevőkhöz képest: FMT_MTD_CIMC.6
Függések: nincs

FMT_MTD_CIMC.7.1 Az IT környezetben magán és titkos kulcsokat csak titkosított formában, vagy megosztott tudáson alapuló eljárások („m az n-ből" technikák) alkalmazásával lehet exportálni a TOE-ból. Az elektronikus úton szétosztott TSF magán és titkos kulcsokat csak titkosított formában lehet exportálni a TOE-ból.

FCS_COP.1 Kriptográfiai eljárás

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FDP_ITC.1 A biztonsági tulajdonságok nélküli felhasználói adatok importja,
vagy FCS_CKM.1 A kriptográfiai kulcsok generálása]
FCS_CKM.4 A kriptográfiai kulcsok megsemmisítése
FMT_MSA.2 Biztonságos biztonsági tulajdonságok

FCS_COP.1.1 A **FIPS 140 szerint tanúsított hardver kriptográfiai modulnak** a következő műveleteket: [**titkosítás, dekódolás, aláírás létrehozás, aláírás ellenőrzés, lenyomat generálás, lenyomat ellenőrzés**] olyan algoritmussal kell végrehajtania, amely megfelel a következőknek: [**FIPS PUB 46-3 (DES, 3DES titkosítás és dekódolás), FIPS PUB 186-2 (RSA aláírás létrehozás és aláírás ellenőrzés), FIPS 180-2 (SHA1 lenyomat generálás és lenyomat ellenőrzés)**].

5.1.5 Biztonsági naplózás

FPT_STM.1 Megbízható időbélyegzés

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FPT_STM.1.1 Az IT környezetnek képesnek kell lennie arra, hogy megbízható időpontot állítson elő.

Megjegyzés: az IT környezet (operációs rendszer) független időforrás (rendszeridő) biztosításával támogatja a megbízható időpont előállítását.

FAU_SAR.1 Napló áttekintés

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FAU_GEN.1 Napló adatok generálása

FAU_SAR.1.1 Az IT környezetnek biztosítania kell a [**rendszervizsgálók**] számára azt a lehetőséget, hogy a naplóbejegyzésekből kiolvassanak [**minden információt**].

FAU_SAR.1.2 Az IT környezetnek a naplóbejegyzéseket olyan formában kell szolgáltatnia, amely alkalmas arra, hogy a felhasználó értelmezze az információkat.

FAU_SAR.3 Kiválogatható napló áttekintés

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FAU_SAR.1 Napló áttekintés

FAU_SAR.3.1 Az IT környezetnek lehetőséget kell biztosítania a naplóbejegyzésben történő [**keresések**] végrehajtására az alábbiak szerint: [**események típusa, valamint az esemény kiváltásáért felelős felhasználó**].

FAU_STG.1 A naplóesemények védett tárolása

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FAU_GEN.1 Napló adatok generálása

FAU_STG.1.1 Az IT környezetnek védenie kell a tárolt naplóállományokat a jogosulatlan törléssel szemben.

FAU_STG.1.2 Az IT környezetnek képesnek kell lennie arra, hogy [**észlelje**] a naplóállományok megváltoztatását.

FAU_STG.4 A napló adatok elvesztésének meggátolása

Hierarchikus fölérendeltség más összetevőkhöz képest: FAU_STG.3
Függések: FAU_STG.1 A naplóesemények védett tárolása

FAU_STG.4.1 Az IT környezetnek [**felül kell írnia a legrégebben tárolt naplórekordokat**], ha a naplóbejegyzések számára rendelkezésre álló tárhely betelt.

FAU_SAA.1 A biztonság potenciális megsértésének vizsgálata

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FAU_GEN.1 Napló adatok generálása

FAU_SAA.1.1 Az IT környezetnek képesnek kell lennie szabályok egy halmazának alkalmazására a naplóesemények figyelemmel kísérése során, valamint ezen szabályok alapján a TSP potenciális megsértésének jelzésére.

FAU_SAA.1.2 Az IT környezetnek a következő szabályokat kell érvényre juttatnia a naplóesemények figyelemmel kísérése során:

a) Az alábbi naplóesemények összegzése vagy kombinálása [**egy órán belül öt egymást követő sikertelen hitelesítési kísérlet bekövetkezése a rendszeradminisztrátor nevében**], melyek a biztonság potenciális megsértését jelzik.

b) [**nincs egyéb szabály**].

FAU_ARP.1 Biztonsági riasztások

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FAU_SAA.1 A biztonság potenciális megsértésének vizsgálata

FAU_ARP.1.1 Az IT környezetnek a biztonság potenciális megsértése esetén az alábbiakat kell tennie: [**a biztonság potenciális megsértéséről értesítés küldése az ügyelet számára**]

5.1.6 Mentés és helyreállítás

A mentés és helyreállítás magában foglalja egy rendszer helyreállítását rendszer hiba vagy más súlyos hiba esetén. Annak érdekében, hogy hiba vagy más váratlan nemkívánatos esemény után a rendszer vissza tudjon állni, a TOE-nak vagy környezetének képeseknek kell lennie arra, hogy a rendszert lementsék. A mentés segítségével a TOE-t egy korábbi időpontban létező működőképes állapotba állíthatják vissza.

FDP_CIMC_BKP.1 CIMC mentés és visszaállítás

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése

FDP_CIMC_BKP.1.1 Az IT környezetnek tartalmaznia kell egy mentés funkciót.

FDP_CIMC_BKP.1.2 Az IT környezetnek biztosítania kell a mentés funkció igény esetén való elindíthatóságát.

FDP_CIMC_BKP.1.3 A rendszer mentésében tárolt adatoknak elégségeseknek kell lenniük arra, hogy a rendszernek a mentés készítésekor meglévő állapotát vissza lehessen állítani, csak a következők felhasználásával:

a) a TOE ugyanazon verziójának egy másolata, mint amelyet a mentési adatok előállításánál használtak;
b) a lementett adatok egy tárolt másolata;
c) az(ok) a kriptográfiai kulcs(ok), amelyek szükségesek a mentést védő digitális aláírás ellenőrzéséhez (ha voltak ilyenek)
d) az(ok) a kriptográfiai kulcs(ok), amelyek szükségesek a titkosított kritikus biztonsági paraméterek dekódolásához (ha voltak ilyenek).

FDP_CIMC_BKP.1.4 Az IT környezetnek tartalmaznia kell egy visszaállítási funkciót, mely képes egy mentésből a rendszer állapotának visszaállítására. A rendszer állapotának visszaállítása során kizárólag a visszaállítási funkció segítségével a rendszer egy olyan, a korábbival "egyenértékű" állapota áll elő, mely kezelni képes a TOE valamennyi lényeges tranzakciójára vonatkozó információt is.

A fenti követelményeken túl az FDP_CIMC_BKP.2-t is alkalmazni kell:

FDP_CIMC_BKP.2 Kiterjesztett CIMC mentések és visszaállítások

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FDP_CIMC_BKP.1 CIMC mentés és visszaállítás

FDP_CIMC_BKP.2.1 A mentett adatokat védeni kell a módosításokkal szemben digitális aláírások felhasználásával.

FDP_CIMC_BKP.2.2 Kritikus biztonsági paraméterek és más bizalmas információk csak titkosított formában tárolhatók.

5.1.7 A szolgáltatások által létrehozott és fogadott üzenetek védelme

FDP_ITT.1 A belső adatátvitel alapszintű védelme (iteráció 1)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FDP_ACC.1 Részleges hozzáférés ellenőrzés, vagy
FDP_IFC.1 Részleges információ áramlás ellenőrzés]

FDP_ITT.1.1 Az IT környezetnek érvényre kell juttatnia a [**CIMC IT környezet hozzáférés ellenőrzés szabályt**[10]], a biztonság-kritikus felhasználói adatok [**módosításának**] megakadályozása érdekében, az IT környezet fizikailag elkülönülő részei közötti átvitel közben.

FDP_ITT.1 A belső adatátvitel alapszintű védelme (iteráció 2)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FDP_ACC.1 Részleges hozzáférés ellenőrzés, vagy
FDP_IFC.1 Részleges információ áramlás ellenőrzés]

FDP_ITT.1.1 Az IT környezetnek érvényre kell juttatnia a [**CIMC IT környezet hozzáférés ellenőrzés szabályt**[11]], a bizalmas felhasználói adatok [**felfedésének**] megakadályozása érdekében, az IT környezet fizikailag elkülönülő részei közötti átvitel közben.

FDP_ITT.1 A belső adatátvitel alapszintű védelme (iteráció 3)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FDP_ACC.1 Részleges hozzáférés ellenőrzés, vagy
FDP_IFC.1 Részleges információ áramlás ellenőrzés]

FDP_ITT.1.1 Az IT környezetnek érvényre kell juttatnia a [**CIMC IT környezet hozzáférés ellenőrzés szabályt**[12]], a bizalmas felhasználói adatok [**felfedésének**] megakadályozása érdekében, a TOE fizikailag elkülönülő részei közötti átvitel közben.

FDP_UCT.1 Alapszintű adatcsere bizalmasság

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FTP_ITC.1 TSF-ek közötti védett csatorna, vagy
FTP_TRP.1 Megbízható útvonal]
[FDP_ACC.1 Részleges hozzáférés ellenőrzés, vagy
FDP_IFC.1 Részleges információ áramlás ellenőrzés]

FDP_UCT.1.1 Az IT környezetnek érvényre kell juttatnia a [**CIMC IT környezet hozzáférés ellenőrzés szabályt**[13]], hogy képes legyen objektumokat a jogosulatlan felfedésekkel szemben védett módon [**küldeni és fogadni**].

[10] melynek meghatározását lásd az 5.1.3.1 pontban
[11] melynek meghatározását lásd az 5.1.3.1 pontban
[12] melynek meghatározását lásd az 5.1.3.1 pontban
[13] melynek meghatározását lásd az 5.1.3.1 pontban

FPT_ITC.1 A TSF-ek közötti bizalmasság az adatátvitel során

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FPT_ITC.1.1 Az IT környezetnek az adatátvitel során védenie kell a jogosulatlan felfedéssel szemben azokat a bizalmas IT környezet adatokat, amelyeket az IT környezetből visznek át egy távoli megbízható IT termék felé.

FPT_ITT.1 A belső adatátvitel alapszintű védelme (iteráció 1)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FPT_ITT.1.1 Az IT környezetnek az adatátvitel során védenie kell a [**módosítással**] szemben a biztonság-kritikus IT környezet adatokat, az IT környezet fizikailag elkülönülő részei közötti átvitel közben.

FPT_ITT.1 A belső adatátvitel alapszintű védelme (iteráció 2)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FPT_ITT.1.1 Az IT környezetnek az adatátvitel során védenie kell a [**felfedéssel**] szemben a bizalmas IT környezet adatokat, az IT környezet fizikailag elkülönülő részei közötti átvitel közben.

FPT_ITT.1 A belső adatátvitel alapszintű védelme (iteráció 3)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FPT_ITT.1.1 Az IT környezetnek az adatátvitel során védenie kell a [**felfedéssel**] szemben a bizalmas TSF adatokat, a TOE fizikailag elkülönülő részei közötti átvitel közben.

5.1.8 Ön-tesztek

Az IT környezetnek meg kell valósítania a következő ön-teszteket.

FPT_AMT.1 Az absztrakt gép tesztelése

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FPT_AMT.1.1 Az IT környezetnek tesztek egy összességét kell futtatnia [**a kezdeti rendszer indításkor**] abból a célból, hogy bizonyítsa azon biztonsági előfeltételek helyes működését, amelyeket az IT környezetnek alátámasztást szolgáltató absztrakt gép nyújt.

FPT_TST_CIMC.2 Szoftver/förmver sértetlenség teszt

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FPT_AMT.1 Az absztrakt gép tesztelése

FPT_TST_CIMC.2.1 Egy hiba detektáló kódot (EDC: error detection code) vagy egy FIPS által jóváhagyott vagy ajánlott hitelesítési technikát (pl. egy hitelesítési kód, kulcsolt lenyomat vagy digitális aláírási algoritmus kiszámítását és ellenőrzését) kell alkalmazni minden, a biztonság-kritikus szoftverre és förmverre, amelyek a TOE-n belül (pl. egy EEPROM-ban vagy RAM-ban) helyezkednek el. Az EDC-nek legalább 16 bit hosszúságúnak kell lennie.

FPT_TST_CIMC.2.2 A hiba detektáló kódot, hitelesítési kódot, kulcsolt lenyomatot vagy digitális aláírást ellenőrizni kell bekapcsoláskor és igény esetén. Ha az ellenőrzés sikertelen, az IT környezetnek végre kell hajtania az alábbiakat: [**a teszt sikertelenségének naplózása**].

FPT_TST_CIMC.3 Szoftver/förmver betöltés teszt

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FPT_AMT.1 Az absztrakt gép tesztelése

FPT_TST_CIMC.3.1 Egy hitelesítési technikát (pl. egy hitelesítési kódot, kulcsolt lenyomatot vagy digitális aláírási algoritmust) használó kriptográfiai mechanizmust kell alkalmazni minden, a biztonság-kritikus szoftverre és förmverre, amely kívülről tölthető be a TOE-be.

FPT_TST_CIMC.3.2 Az IT környezetnek ellenőrizni kell a hitelesítési kódot, kulcsolt lenyomatot vagy digitális aláírást minden esetben, amikor a szoftver vagy förmver kívülről kerül a TOE-be betöltésre. Ha az ellenőrzés sikertelen, az IT környezetnek végre kell hajtania az alábbiakat: [**azon szoftver vagy förmver elem futtatásának letiltása, melyre a teszt hibát jelzett**].

5.1.9 Archiválás

Az IT környezetnek meg kell valósítania egy archiválási funkciót, mely biztosítja a rendszer által kezelt adatok elérhetőségét a jogszabályok által meghatározott adatkörre és időtartamra nézve.

Az adatok archiválása annyiban különbözik az adatok mentésétől, hogy az archivált adatok leválaszthatók a TOE által aktuálisan kezelt adatoktól.

FDP_CWA_ARC.1 Archiválás

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése

FDP_CWA_ARC.1.1 Az IT környezet-nek tartalmaznia kell egy archiválási funkciót.

FDP_CWA_ARC.1.2 Az IT környezet-nek biztosítania kell az archiválási funkció igény esetén való elindíthatóságát.

FDP_CWA_ARC.1.3 Az archiválási funkciónak legalább az alábbi adatok archiválását lehetővé kell tennie:

a) a TOE által előállított minden tanúsítvány;
b) a TOE által előállított minden tanúsítvány visszavonási lista;
c) a TOE-ban keletkezett minden napló állomány;
d) a TOE-ban keletkezett minden időbélyeg válasz;
e) a TOE-be érkezett minden OCSP kérés;
f) a TOE-ban keletkezett minden OCSP válasz.

FDP_CWA_ARC.1.4 Minden archiválási bejegyzésnek tartalmaznia kell az archiválás időpontját.

FDP_CWA_ARC.2 Szelektálható keresés az archívumban

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FDP_CWA_ARC.1 Archiválás

FDP_CWA_ARC.2.1 Az IT környezet-nek az archívumra vonatkozóan biztosítani kell egy keresési lehetőséget az események típusa szerint.

FDP_CWA_ARC.3 Kiterjesztett archiválás

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FDP_CWA_ARC.1 Archiválás

FDP_CWA_ARC.3.1 Az archivált adatokat védeni kell a módosításokkal szemben digitális aláírások, kulcsolt lenyomatok vagy hitelesítési kódok felhasználásával.

FDP_CWA_ARC.3.2 Az archívum nem tartalmazhat védtelen formában kritikus biztonsági paramétereket és más bizalmas információkat.

5.2 A TOE-ra vonatkozó funkcionális biztonsági követelmények

Ez az alfejezet a TOE-ra vonatkozó funkcionális biztonsági követelményeket határozza meg.

Az 5-2. táblázat felsorolja a TOE-ra vonatkozó funkcionális biztonsági követelményeket.

Biztonsági naplózás (FAU)	Napló adatok generálása	FAU_GEN.1
	A felhasználói azonosítóval való összekapcsolás	FAU_GEN.2
A felhasználói adatok védelme (FDP)	Részleges hozzáférés ellenőrzés (iteráció 2)	FDP_ACC.1
	Biztonsági tulajdonság alapú hozzáférés ellenőrzés (iteráció 2)	FDP_ACF.1
	A felhasználói magánkulcs bizalmasságának védelme	FDP_ACF_CIMC.2
	A felhasználói titkos kulcs bizalmasságának védelme	FDP_ACF_CIMC.3
	Tanúsítvány előállítás	FDP_CIMC_CER.1
	Tanúsítvány visszavonási lista érvényesítés	FDP_CIMC_CRL.1
	Tanúsítvány állapot export	FDP_CIMC_CSE.1
	OCSP alap-válasz érvényesítés	FDP_CIMC_OCSP.1
	Időbélyeg válasz érvényesítés	FDP_CWA_TS.1
	Kiterjesztett felhasználói magán és titkos kulcs export	FDP_ETC_CIMC.5
	A belső adatátvitel alapszintű védelme (iteráció 4)	FDP_ITT.1
	A tárolt nyilvános kulcs sértetlenségének figyelése és reagálás	FDP_SDI CIMC.3
Azonosítás és hitelesítés (FIA)	Felhasználói tulajdonságok megadása (iteráció 2)	FIA_ATD.1
	Hitelesítési hibák kezelése (iteráció 2)	FIA_AFL.1
	Az azonosítás időzítése (iteráció 2)	FIA_UID.1
	A hitelesítés időzítése (iteráció 2)	FIA_UAU.1
	Felhasználó - szubjektum összerendelése (iteráció 2)	FIA_USB.1
Biztonsági menedzsment (FMT)	A biztonsági funkciók viselkedésének kezelése (iteráció 3)	FMT_MOF.1
	Kiterjesztett tanúsítvány profil menedzsment	FMT_MOF_CIMC.3
	Kiterjesztett tanúsítvány visszavonási lista profil menedzsment	FMT_MOF_CIMC.5
	OCSP profil menedzsment	FMT_MOF_CIMC.6
	Időbélyeg profil menedzsment	FMT_MOF_CWA.1
	Biztonsági tulajdonságok kezelése (iteráció 2 és 3)	FMT_MSA.1
	Biztonságos biztonsági tulajdonságok (iteráció 2)	FMT_MSA.2
	Statikus tulajdonságok kezdeti értékadása (iteráció 2)	FMT_MSA.3
	Menedzsment funkciók megadása (iteráció 2)	FMT_SMF.1
	Megszorítások a biztonsági szerepkörökre (iteráció 2)	FMT_SMR.2
A TOE biztonságának védelme (FPT)	Napló lista aláírása	FPT_CIMC_TSP.1
	A TSP megkerülhetetlensége (iteráció 2)	FPT_RVM.1
	A belső adatátvitel alapszintű védelme (iteráció 4)	FPT_ITT.1

5-2. táblázat– A TOE-ra vonatkozó funkcionális biztonsági követelmények

Az 5-2. táblázatban szereplő összetevők többsége a CC 2. kötetéből való.
Az alábbi összetevő nem szerepelnek a CC 2. kötetében (kiterjesztett összetevők, melyek a CIMC PP védelmi profilban megfogalmazottak szerint kerültek át jelen biztonsági előirányzatba):

- FDP_ACF_CIMC.2
- FDP_ACF_CIMC.3
- FDP_CIMC_CER.1
- FDP_CIMC_CRL.1
- FDP_CIMC_CSE.1
- FDP_CIMC_OCSP.1
- FDP_CWA_TS.1
- FDP_ETC_CIMC.5
- FDP_SDI_CIMC.3
- FMT_MOF_CIMC.3
- FMT_MOF_CIMC.5
- FMT_MOF_CIMC.6
- FMT_MOF_CWA.1
- FPT_CIMC_TSP.1

Ezek az összetevők ahhoz szükségesek, hogy olyan egyedi követelményeket határozzanak meg, amelyekkel a Common Criteria nem foglalkozik. Nevükben szerepel a CIMC betűnégyes, jelezve, hogy a CIMC-PP védelmi profilban kerültek meghatározásra. A többi (melyek nevében a CWA betűhármas szerepel) jelen biztonsági előirányzat egyedi meghatározása (kiterjesztett követelménye).

5.2.1 Bizalmi munkakörök kezelése

FMT_SMF.1 Menedzsment funkciók megadása (iteráció 2)

Hierarchikus alárendeltség más komponensekhez képest: nincs.

Függések: nincs

FMT_SMF.1.1 A TSF-nek képesnek kell lennie a következő biztonsági menedzsment funkciók végrehajtására: **[fiókok és szerepkörök kezelése, konfigurálás, tanúsítvány profilok kezelése, visszavonási lista (CRL) profilok kezelése]**

FMT_SMR.2 Megszorítások a biztonsági szerepkörökre (iteráció 2)

Hierarchikus fölérendeltség más összetevőkhöz képest: FMT_SMR.1
Függések: FIA_UID.1 Az azonosítás időzítése

FMT_SMR.2.1 A TSF-nek kezelnie kell az alábbi szerepköröket: **[rendszer biztonsági tisztviselő (SSO), biztonsági tisztviselő (SO), regisztrációs tisztviselő (RO)]**

FMT_SMR.2.2 A TSF-nek össze kell kapcsolnia a felhasználókat a szerepkörökkel.

FMT_SMR.2.3 Az IT környezetnek biztosítania kell, hogy: [
a) egy felhasználó nem tölthet be egyszerre rendszer biztonsági tisztviselő (SSO) és regisztrációs tisztviselő (RO) szerepkört]

FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése (iteráció 3)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_SMR.1 Biztonsági szerepkörök

FMT_MOF.1.1 A TSF-nek az **[5-3. táblázatban meghatározott]** szerepkörökre kell korlátoznia az **[5-3. táblázatban felsorolt]** biztonsági funkciók viselkedésének **[módosítását]**.

Funkció	Esemény
Fiókok (account) és szerepkörök kezelése	A rendszer biztonsági tisztviselőkre (SSO) kell korlátozni a biztonsági tisztviselői (SO) fiókok létrehozásának a lehetőségét. (Két SSO együtt hozhat csak létre SO fiókot.) A biztonsági tisztviselőkre kell korlátozni a regisztrációs tisztviselői (RO) fiókok létrehozásának a lehetőségét. (Két SO együtt hozhat csak létre RO fiókot.) A biztonsági tisztviselőkre kell korlátozni az RO fiókokhoz tartozó jogosultságok beállításának lehetőségét. (Két SO együtt állíthat, módosíthat csak RO jogosultságot.)
Konfigurálás	A biztonsági tisztviselőkre (SO) kell korlátozni a TOE valamennyi biztonsági funkcionalitásának a konfigurálását.
Tanúsítvány profilok kezelése	A biztonsági tisztviselőkre kell korlátozni azt a lehetőséget, hogy új tanúsítvány profilt hozzanak létre, illetve létező tanúsítvány profilt módosítsanak. (Két SO együtt hozhat csak létre, illetve módosíthat egy tanúsítvány profilt.)
Visszavonási lista (CRL) profilok kezelése	A biztonsági tisztviselőkre kell korlátozni azt a lehetőséget, hogy új visszavonási lista (CRL) profilt hozzanak létre, illetve létező visszavonási lista profilt módosítsanak. (Két SO együtt hozhat csak létre, illetve módosíthat egy visszavonási lista profilt.)
OCSP profilok kezelése	A biztonsági tisztviselőkre kell korlátozni azt a lehetőséget, hogy új OCSP profilt hozzanak létre, illetve létező OCSP profilt módosítsanak. (Két SO együtt hozhat csak létre, illetve módosíthat egy OCSP profilt.)
TS profilok kezelése	A biztonsági tisztviselőkre kell korlátozni azt a lehetőséget, hogy új TS profilt hozzanak létre, illetve létező TS profilt módosítsanak. (Két SO együtt hozhat csak létre, illetve módosíthat egy TS profilt.)

5-3. táblázat: Jogosult szerepkörök a biztonsági funkciók viselkedésének kezelésére

FMT_MSA.1 Biztonsági tulajdonságok kezelése (iteráció 2)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FDP_ACC Részleges hozzáférés ellenőrzés, vagy
FDP_IFC Részleges információ áramlás ellenőrzés]
FMT_SMR.1 Biztonsági szerepkörök
FMT_SMF.1 Menedzsment funkciók megadása

FMT_MSA.1.1 A TSF-nek érvényt kell szereznie a **[CIMC TOE hozzáférés ellenőrzés szabály**[14] **SFP]**-nek, azáltal, hogy a **[rendszer biztonsági tisztviselő]** szerepkörre korlátozza az alábbi biztonsági tulajdonság **[módosítását]**: **[SO szerepkör]**

FMT_MSA.1 Biztonsági tulajdonságok kezelése (iteráció 3)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FDP_ACC Részleges hozzáférés ellenőrzés, vagy
FDP_IFC Részleges információ áramlás ellenőrzés]
FMT_SMR.1 Biztonsági szerepkörök
FMT_SMF.1 Menedzsment funkciók megadása

FMT_MSA.1.1 A TSF-nek érvényt kell szereznie a **[CIMC TOE hozzáférés ellenőrzés szabály**[15] **SFP]**-nek, azáltal, hogy a **[biztonsági tisztviselő]** szerepkörre korlátozza az alábbi biztonsági tulajdonságok **[módosítását]**: **[RO szerepkör, RO jogosultságai]**

FMT_MSA.2 Biztonságos biztonsági tulajdonságok (iteráció 2)
Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: ADV_SPM.1 Informális TSP biztonságpolitikai modell
[FDP_ACC Részleges hozzáférés ellenőrzés, vagy
FDP_IFC Részleges információ áramlás ellenőrzés]
FMT_MSA_1 Biztonsági tulajdonságok kezelése
FMT_SMR.1 Biztonsági szerepkörök

FMT_MSA.2.1 A TSF-nek biztosítania kell, hogy csak biztonságos értékek legyenek elfogadva a biztonsági tulajdonságok számára.

FMT_MSA.3 Statikus tulajdonságok kezdeti értékadása (iteráció 2)
Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_MSA_1 Biztonsági tulajdonságok kezelése
FMT_SMR.1 Biztonsági szerepkörök

FMT_MSA.3.1 A TSF-nek érvényt kell szereznie a **[CIMC TOE hozzáférés ellenőrzés szabály**[16] **SFP[**-nek, **[korlátozó]** alapértékek biztosításával az SFP-t érvényre juttató biztonsági tulajdonságokra.

FMT_MSA.3.2 A TSF-nek lehetővé kell tennie a **[biztonsági tisztviselő]** számára, hogy alternatív kezdeti értékeket adhasson meg az alapértelmezett értékek helyett egy objektum vagy információ létrehozásakor.

[14] melynek meghatározását lásd az 5.2.3.1 pontban
[15] melynek meghatározását lásd az 5.2.3.1 pontban
[16] melynek meghatározását lásd az 5.2.3.1 pontban

5.2.2 Azonosítás és hitelesítés

FIA_ATD.1 Felhasználói tulajdonságok megadása (iteráció 2)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FIA_ATD.1.1 A TSF-nek az alábbi, egyedi felhasználókhoz tartozó biztonsági tulajdonságokat kell kezelnie: **[a felhasználó által betölthető szerepkörök halmaza (SSO, SO, RO), RO esetén az adott RO jogosultságai].**

FIA_UID.1 Az azonosítás időzítése (iteráció 2)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FIA_UID.1.1 A TSF-nek a felhasználó azonosítása előtt az alábbi tevékenységek felhasználó nevében történő végrehajtását lehetővé kell tennie: **[saját tanúsítvány kiválasztása].**

FIA_UID.1.2 A TSF-nek meg kell követelnie minden felhasználó sikeres azonosítását, mielőtt bármilyen TSF-által közvetített más tevékenységet lehetővé tenne az adott felhasználó nevében.

FIA_UAU.1 A hitelesítés időzítése (iteráció 2)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FIA_UID.1 Az azonosítás időzítése

FIA_UAU.1.1 A TSF-nek a felhasználó hitelesítése előtt az alábbi tevékenységek felhasználó nevében történő végrehajtását lehetővé kell tennie: **[egy véletlen sorozat aláírásának kiváltása a kiválasztott tanúsítványhoz tartozó magánkulccsal].**

FIA_UAU.1.2 A TSF-nek meg kell követelnie minden felhasználó sikeres hitelesítését, mielőtt bármilyen TSF-által közvetített más tevékenységet lehetővé tenne az adott felhasználó nevében.

FIA_AFL.1 Hitelesítési hibák kezelése (iteráció 2)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FIA_UAU.1 A hitelesítés időzítése

FIA_AFL.1.1 A TSF-nek észlelnie kell, amikor sikertelen hitelesítési kísérlet történik.

FIA_AFL.1.2 Amennyiben sikertelen hitelesítési kísérlet történt, a TSF-nek az alábbiakat kell végrehajtania: **[a futó alkalmazás leállítása].**

FIA_USB.1 Felhasználó - szubjektum összerendelése (iteráció 2)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs

Függések: FIA_ATD.1 Felhasználói tulajdonságok megadása

FIA_USB.1.1 A TSF-nek össze kell kapcsolnia a felhasználó megfelelő biztonsági tulajdonságait az adott felhasználó nevében tevékenykedő szubjektumokkal.

5.2.3 Hozzáférés ellenőrzés

FDP_ACC.1 Részleges hozzáférés ellenőrzés (iteráció 2)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés

FDP_ACC.1.1 A TSF-nek érvényt kell szereznie a **[CIMC TOE hozzáférés ellenőrzés szabály**[17] **SFP]**-nek, az alábbi szubjektumok és objektumok között, az alábbi műveletekre: **[az InfoCA rendszer minden sikeresen azonosított és hitelesített felhasználójára (szubjektumok), az InfoCA rendszer parancsaira (objektumok) és a parancsok végrehajtására (műveletek)]**.

FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés (iteráció 2)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FDP_ACC.1 Részleges hozzáférés ellenőrzés
FMT_MSA.3 Statikus tulajdonságok inicializálása

FDP_ACF.1.1 A TSF-nek érvényt kell szereznie a **[CIMC TOE hozzáférés ellenőrzés szabály**[18] **SFP]**-nek az objektumok vonatkozásában a következők alapján: **[a szubjektum azonossága, a szubjektum által felvehető szerepkörök, a szubjektumnak az adott szerepkörben meghatározott jogosultságai]**.

FDP_ACF.1.2 A TSF-nek érvényre kell juttatnia **[az 5-4. táblázatban felsorolt]** szabályokat annak megállapítása érdekében, hogy egy művelet megengedett-e az ellenőrzött szubjektumok és ellenőrzött objektumok között**.**

FDP_ACF.1.3 A TSF-nek explicit módon kell megadnia a szubjektumok objektumokhoz való hozzáférési engedélyeit a következő kiegészítő szabályok alapján: **[nincsenek további szabályok].**

FDP_ACF.1.4 A TSF-nek explicit módon le kell tiltania a szubjektumok objektumokhoz való hozzáféréseit az alábbiak alapján: **[nincsenek további szabályok].**

[17] melynek meghatározását lásd az 5.2.3.1 pontban
[18] melynek meghatározását lásd az 5.2.3.1 pontban

Funkció	Esemény
SO fiók (account) létrehozása, módosítása, törlése	Az SO fiókok létrehozását, módosítását és törlését a rendszer biztonsági tisztviselőkre kell korlátozni /a három SSO-ból kettőnek az aláírása kell/.
RO fiók (account) létrehozása, módosítása, törlése	Az RO fiókok létrehozását, módosítását és törlését a biztonsági tisztviselőkre kell korlátozni /két SO együttes aláírása kell/.
konfigurációs állományok megadása)	A konfigurációs állományok (köztük a tanúsítvány és CRL profilok) megadását, módosítását és törlését a biztonsági tisztviselőkre kell korlátozni /két SO együttes aláírása kell/.
LDAP fa újraépítése	Az LDAP fa újraépítését (adatbázisból) a biztonsági tisztviselőkre kell korlátozni.
Tanúsítvány kérelem elkészítése	A tanúsítvány kérelem elkészítését a regisztrációs tisztviselőkre kell korlátozni (szükséges még, hogy az adott RO az adott tanúsítványprofilban megkapja az alábbi jogot: Issue)
Visszavonási kérelem beadása	A visszavonási kérelem elkészítését a regisztrációs tisztviselőkre kell korlátozni (szükséges még, hogy az adott RO az adott tanúsítványprofilban megkapja az alábbi jogot: Revocation)
Felfüggesztési kérelem beadása	A felfüggesztési kérelem elkészítését a regisztrációs tisztviselőkre kell korlátozni (szükséges még, hogy az adott RO az adott tanúsítványprofilban megkapja az alábbi jogot: Hold)
Felfüggesztett tanúsítvány újra aktiválása	A felfüggesztett tanúsítvány újra aktiválását a regisztrációs tisztviselőkre kell korlátozni (szükséges még, hogy az adott RO az adott tanúsítványprofilban megkapja az alábbi jogot: Activate)
Magánkulcs visszaállítási kérelem beadása	A magánkulcs (és a hozzá tartozó tanúsítvány) visszaállítási kérelem beadását a regisztrációs tisztviselőkre kell korlátozni (szükséges még, hogy az adott RO az adott tanúsítványprofilban megkapja az alábbi jogot: Key Recovery)
Magánkulcshoz tartozó PIN kódok újranyomtatása	A magánkulcshoz tartozó PIN kódok újranyomtatási kérelmét a regisztrációs tisztviselőkre kell korlátozni (szükséges még, hogy az adott RO az adott tanúsítványprofilban megkapja az alábbi jogot: PIN reprint)
Külső fájlból beolvasott kérések tartalmának módosítása	Külső fájlból beolvasott kérések tartalmának módosítását (egy tanúsítványprofilon belül) a regisztrációs tisztviselőkre kell korlátozni (szükséges még, hogy az adott RO az adott tanúsítványprofilban megkapja az alábbi jogot: May modify setting).

5-4. táblázat: Hozzáférés ellenőrzések

FPT_RVM.1 A TSP megkerülhetetlensége (iteráció 2)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FPT_RVM.1.1 A TSF-nek biztosítania kell, hogy a TSP-t érvényre juttató funkciók valóban meghívódnak, és sikeresen befejeződnek, mielőtt a TSF hatáskörén belüli funkciók futása lehetővé válik.

5.2.3.1 CIMC TOE hozzáférés ellenőrzés szabály

A TOE-nek támogatnia kell egy olyan "CIMC TOE hozzáférés ellenőrzési szabály" adminisztrálását és érvényre juttatását, amely az alábbiakban ismertetésre kerülő lehetőségeket biztosítja.

A szubjektumok (emberi felhasználók) számára a következők alapján van biztosítva az objektumokhoz (adatok/fájlok) való hozzáférés:

1. A hozzáférést kérő szubjektum azonosítója,
2. Az a szerepkör (vagy szerepkörök), amely(ek)nek a felvételére a szubjektum fel van jogosítva,
3. Az igényelt hozzáférés típusa,
4. A hozzáférési kérelem tartalma, és
5. Egy titkos vagy magánkulcs birtoklása.

A szubjektum azonosítás magában foglalja az alábbiakat:

- különböző hozzáférési jogosultságokkal rendelkező személyek,
- különböző hozzáférési jogosultságokkal rendelkező szerepkörök,
- egy vagy több különböző hozzáférési jogosultságokkal rendelkező szerepkörrel felruházott személyek

Közvetlen engedélyezéssel vagy megtagadással járó hozzáférés típusok:

- olvasás,
- írás,
- végrehajtás.

Minden objektumra közvetlenül meg kell adni egy tulajdonos szubjektumot és egy szerepkört. Az objektum tulajdonosának vagy a szerepkör(ök)nek lesz a kötelessége a jogosultságok jelen biztonsági előirányzatnak megfelelő kijelölése és kezelése.

5.2.4 Kulcskezelés

Jelen biztonsági előirányzat a kulcsokat az alábbi kategóriákba sorolja:

1. **CIMC (tanúsítványokat aláíró) kulcsok** - a tanúsítvány előállítás szolgáltatás kulcspárja, amellyel a TOE a különböző tanúsítványokat írja alá.
2. **Komponens (infrastrukturális) kulcsok** - a TOE által az alábbi folyamatokhoz használt kulcsok: tanúsítvány állapot válaszok aláírása, kulcs-egyeztetés, alrendszer hitelesítés, napló aláírás, tárolt vagy továbbított adatok titkosítása. (A rövid távú munkaszakasz kulcsokat nem tekintjük infrastrukturális kulcsoknak.)
3. **CIMS személyi (rendszervezérlési kulcsok)** - személyek által a TOE használatára vagy kezelésére használt kulcsok, melyek hitelesítési-, aláírási- vagy bizalmassági szolgáltatásokat biztosítanak a TOE-val kölcsönhatásba kerülő személyek számára.
4. **Tanúsítvány alany (végfelhasználói) kulcsok** - a tanúsítvány alanyának kulcspárja (melynek nyilvános részét a tanúsítvány foglalja magában)

5.2.4.1 Magánkulcs tárolás

FDP_ACF_CIMC.2 A felhasználói magánkulcs bizalmasságának védelme

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FDP_ACF_CIMC.2.1 A CIMS személyi (rendszervezérlési) magánkulcsokat vagy egy FIPS 140 szerint tanúsított kriptográfiai modulban, vagy titkosított formában kell tárolni. Ha a CIMS személyi (rendszervezérlési) magánkulcsokat titkosított formában tárolják, a titkosítást egy FIPS 140 szerint tanúsított kriptográfiai modulban kell végrehajtani.

FDP_ACF_CIMC.2.2 Ha a TOE-ben vannak tárolva tanúsítvány alany (végfelhasználói) magánkulcsok, akkor ezeket egy "hosszú távú, magánkulcs védelmi kulcs"-csal kell titkosítani. A titkosítást egy FIPS 140 szerint tanúsított kriptográfiai modulban kell végrehajtani.

5.2.4.2 Nyilvános kulcs tárolás

FDP_SDI_CIMC.3 A tárolt nyilvános kulcs sértetlenségének figyelése és ehhez kapcsolódó reagálás

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FDP_SDI_CIMC.3.1 A TOE-ben, és nem egy FIPS 140 szerint tanúsított kriptográfiai modulban tárolt nyilvános kulcsokat védeni kell az észrevétlen módosításokkal szemben, digitális aláírások, kulcsolt lenyomatok vagy hitelesítési kódok használatával.

FDP_SDI_CIMC.3.2 Egy nyilvános kulcs védelmére szolgáló digitális aláírást, kulcsolt lenyomatot vagy hitelesítési kódot a kulcshoz való minden hozzáférés során ellenőrizni kell. Ha az ellenőrzés sikertelen, a TSF-nek az alábbiakat kell végrehajtania **[az eseményről hibajelzés naplózása, és a nyilvános kulcs felhasználásának visszautasítása].**

5.2.4.3 Titkos kulcs tárolás

FDP_ACF_CIMC.3 A felhasználói titkos kulcs bizalmasságának védelme

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FDP_ACF_CIMC.3.1 Azokat a felhasználói titkos kulcsokat, amelyek a TOE-ben, de nem egy FIPS 140 szerint tanúsított kriptográfiai modulban vannak tárolva, titkosított formában kell tárolni. A titkosítást egy FIPS 140 szerint tanúsított kriptográfiai modulban kell végrehajtani.

5.2.4.4 Magán és titkos kulcs export

FDP_ETC_CIMC.5 Kiterjesztett felhasználói magán és titkos kulcs export

Hierarchikus fölérendeltség más összetevőkhöz képest: FDP_ETC_CIMC.4
Függések: nincs

FDP_ETC_CIMC.5.1 A felhasználói magán és titkos kulcsokat csak titkosított formában, vagy megosztott tudáson alapuló eljárások („m az n-ből” technikák) alkalmazásával lehet exportálni a TOE-ból. Az elektronikus úton szétosztott felhasználói magán és titkos kulcsokat csak titkosított formában lehet exportálni a TOE-ból.

5.2.5 Biztonsági naplózás

FAU_GEN.1 Napló adatok generálása

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FPT_STM.1 Megbízható időbélyegzés

FAU_GEN.1.1 A TSF-nek képesnek kell lennie arra, hogy naplóbejegyzést generáljon a következő naplózható eseményekről:
a) A naplózási funkciók indítása és leállítása;
b) Minden, a naplózás [**alap**] szintjére vonatkozó naplózható esemény;
c) [**Az 5-5. táblázatban felsorolt események**]**.**

FAU_GEN.1.2 A TSF-nek minden naplóbejegyzésben rögzítenie kell legalább a következő információkat:
a) Az esemény dátuma és időpontja, az esemény típusa, a szubjektum azonosítója és az esemény kimenetele (siker vagy sikertelenség);
b) [**Az 5-5. táblázatban szereplő xxx-ek helyett konkrét nevek szerepelnek.**)].

A napló nem tartalmazhat továbbá nyílt formában magánkulcsot, titkos kulcsot, vagy egyéb kritikus biztonsági paramétert (pl. jelszót, vagy PIN kódot).

FAU_GEN.2 A felhasználói azonosítóval való összekapcsolás

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FAU_GEN.1 Napló adatok generálása
FIA_UID.1 Az azonosítás időzítése

FAU_GEN.2.1 A TSF-nek képesnek kell lennie arra, hogy minden naplózható eseményt összekapcsoljon az eseményt kiváltó felhasználó azonosítójával.

FPT_CIMC_TSP.1 Napló lista aláírása

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FAU_GEN.1 Napló adatok generálása
FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése

FPT_CIMC_TSP.1.1 A TSF-nek periodikusan létre kell hoznia egy napló állomány aláírási eseményt, amelynek során kiszámol egy digitális aláírást, egy kulcsolt lenyomatot vagy hitelesítési kódot, amely átfogja a napló állományban tárolt bejegyzéseket.

FPT_CIMC_TSP.1.2 A digitális aláírást, kulcsolt lenyomatát vagy hitelesítési kódot úgy kell kiszámolni, hogy az átfogja legalább azokat a bejegyzéseket, amelyek a megelőző napló állomány aláírási esemény óta kerültek a napló állományba, valamint a megelőző napló állomány aláírási esemény digitális aláírását, kulcsolt lenyomatát, vagy hitelesítési kódját.

FPT_CIMC_TSP.1.3 A napló állomány aláírási esemény gyakoriságának konfigurálhatónak kell lennie.

FPT_CIMC_TSP.1.4 A napló állomány aláírási esemény során előállított digitális aláírást, kulcsolt lenyomatot vagy hitelesítési kódot bele kell venni a napló állományba.

5-5. táblázat – Naplózandó események és naplóadatok (típusonként)

Típus: **Kritikus**	
	Unable to allocate memory
	Unable to process caprofile files
	Unable to process crlprofile files
Típus: **Veszélyes**	
	Critical error loading CRL profile: xxx.
	Database error!!!
	Failed to calculate computer hash key. Internal memory error.
	Failed to calculate computer hash key.
	Failed to get CRL SN.
	Failed to get embedded certificate.
	Failed to get embedded certificates.
	Failed to load ro file.
	Failed to load so file.
	Failed to parse so/ro file.
	Failed to process crl profiles.: xxx
	Failed to process crl profiles.
	Failed to put crl to LDAP: xxx.
	Failed to save Base CRL SN.
	Failed to save Base CRL SN: xxx.
	Failed to start server...
	Failed to validate ADM keys.
	Failed to validate SO.
	Failed to validate ro file.
	Failed to validate so file.
	Failed to validate so. Internal memory error.
	Invalid ca profile file xxx. Failed to parse.
	Unable to get next CA SN.
	Unable to get next Crl SN.
Típus: **Hiba**	
	Bad request type. DN=(xxx)
	Could not fill LDAP.
	Error building PKCS12. DN=(xxx), Serial=xxx
	Error building PKCS7. DN=(xxx), Serial=xxx
	Error building certificate. DN=(xxx)
	External config does not allow recovery.
	Failed to create certificate: xxx
	Failed to insert certificate to LDAP (xxx): xxx., DN=(xxx), Serial=xxx
	Failed to insert certificate to LDAP: xxx., DN=(xxx), Serial=xxx
	Failed to insert certificate to LDAP
	Failed to insert crl to LDAP.
	Failed to load Ca profile: xxx.
	Failed to load double signed Ca profile: xxx. Valid signer not found.
	Failed to load double signed Ca profile: xxx.
	Failed to load double signed Crl profile: xxx. Valid signer not found.
	Failed to load double signed Crl profile: xxx.
	Failed to move message to error folder.
	Failed to move message to error queue.
	Failed to publish Crl to LDAP: xxx., No serial
	Failed to publish Crl to LDAP: xxx., Serial=xxx
	Failed to recover p12. Failed to save XML output.
	Failed to recover p12. Failed to send output to queue.
	Failed to save output file: xxx.
	Failed to send error message to queue.
	Failed to send info message to queue.
	Failed to send response to queue: xxx.

	Failed to send response to the queue.
	Failed to validate Ca profile: xxx. Invalid key source modification tag.
	Failed to validate Ca profile: xxx. Invalid key source tag.
	Failed to valídate Ca profile: xxx. Invalid recovery modification tag.
	Failed to validate Ca profile: xxx. Invalid recovery tag.
	Internal error encrypting p12.
	Internal error encrypting pin.
	Internal error generating key. DN=(xxx)
	Internal error generating pin. DN=(xxx)
	Internal error inserting certificate into database. DN=(xxx), Serial=xxx
	Internal error processing subject.
	Internal error saving crl file.
	Internal error saving file.
	Internal error searching in database. DN=(xxx)
	Internal error setting issuer name.
	Internal error setting issuer.
	Internal error setting time. DN=(xxx)
	Internal error signing crl.
	Internal error writing DER file. DN=(xxx), Serial=xxx
	Internal error writing PEM file. DN=(xxx), Serial=xxx
	Internal error. Certificate profile not found. Request could not be executed.
	Internal error. DN=(xxx)
	Internal error. Failed to recover p12.
	Internal error. Invalid parameters defined.
	Internal error. No parameters defined.
	Internal error. No serial defined.
	Internal error. Request could not be executed. Only RO users allowed to reprint PIN mail.
	Internal error. Request could not be executed. Only RO users can recover keys.
	Internal error. Request could not be executed. Only admin users allowed.
	Internal error. Request could not be executed. RO has no right.
	Internal error. Request could not be executed. Serial=xxx.
	Internal format error. Faild to create delta indicator.
	Internal format error. Failed to add delta indicator.
	Internal format error. Failed to add issuer key id to delta CRL.
	Internal format error. Failed to add issuer key id.
	Internal format error. Failed to create issuer key id.
	Internal format error. Failed to set CRL version.
	Internal format error. Failed to set delta CRL version.
	Internal format error. Invalid issuer key id.
	Internal format error. Invalid serial number found in DB.
	Internal format error. Issuer key id is invalid.
	Internal format error. Subject key identifier not found in CA certificate...
	Internal format error.
	Internal memory error. DN=(xxx), Serial=xxx
	Internal memory error. DN=(xxx)
	Internal memory error
	Invalid key recovery field in request. DN=(xxx)
	Invalid profile name. Profile not found.
	Invalid request, failed to execute...
	Invalid request, no profile found. Failed to execute...
	Key length constraint error. DN=(xxx)
	Key recovery constraint error. DN=(xxx)
	Key source constraint error. DN=(xxx)
	Memory error. Request processed, but no response...
	No CN in request. DN=(xxx)
	Officer has no permisson to the profile: xxx
	Originial user with the key does not exist. DN=(xxx)
	Public key already exists. DN=(xxx)

	Public key does not exist. DN=(xxx)
	Request type not supported.
	Subject already exists. DN=(xxx)
	User does not exist. DN=(xxx)
	with the public key does not exist. DN=(xxx)
	User with the same key already exists. DN=(xxx)
	Validation error. Invalid request, failed to execute...
	Validation failed. Invalid request, failed to execute...
	Validation failed. RO has no right, failed to execute...
	Validity constraint error. DN=(xxx)
Típus: **Információ**	
	xxx has been stopped.
	'xxx' request, Serial=xxx
	Admin request: xxx.
	CA profile loaded. File: xxx, Format: xxx, Version: xxx, TimeStamp: xxx, Comment: xxx.
	CRL profile loaded. File: xxx, Format: xxx, Version: xxx, TimeStamp: xxx, Comment: xxx.
	Certificate generated. DN=(xxx), Profile=xxx, Serial=xxx
	Certificate published to LDAP (xxx): xxx., DN=(xxx), Serial=xxx
	Certificate published to LDAP: xxx., DN=(xxx), Serial=xxx
	Certificate request: xxx.
	Crl generated: xxx.
	Crl published to LDAP: xxx., No serial
	Crl published to LDAP: xxx., Serial=xxx
	Key generated (hw). DN=(xxx)
	Key generated (sw). DN=(xxx)
	Key recovery request Serial=xxx.
	Key recovery request: xxx.
	LDAP rebuilt result: %ld certificates inserted
	No Crl profile found.
	OK sent to RA. DN=(xxx), Serial=xxx
	OK sent to RA. Serial=xxx
	P12 generated. DN=(xxx), Profile=xxx, Serial=xxx
	Pinmail sent to printer. DN=(xxx), Serial=xxx
	Reprint request Serial=xxx.
	Reprint request: xxx.
	Request DN=(xxx).
	Request type=xxx DN=(xxx).
	Revocation request: xxx.
	Starting CA xxx xxx...
	TEST MODE!
Típus: **Figyelmeztetés**	
	Message queue: xxx not exist.

5.2.6 A szolgáltatások által létrehozott és fogadott üzenetek védelme

FDP_ITT.1 A belső adatátvitel alapszintű védelme (iteráció 4)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FDP_ACC.1 Részleges hozzáférés ellenőrzés, vagy
FDP_IFC.1 Részleges információ áramlás ellenőrzés]

FDP_ITT.1.1 A TSF-nek érvényre kell juttatnia a [**CIMC TOE hozzáférés ellenőrzés szabályt**[19]**]**, a biztonság-kritikus felhasználói adatok [**módosításának]** megakadályozása érdekében, a TOE fizikailag elkülönülő részei közötti átvitel közben.

FPT_ITT.1 A belső adatátvitel alapszintű védelme (iteráció 4)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FPT_ITT.1.1 A TSF-nek az adatátvitel során védenie kell a [**módosítással**] szemben a biztonság-kritikus TSF adatokat, a TOE fizikailag elkülönülő részei közötti átvitel közben.

[19] melynek meghatározását lásd az 5.2.3.1 pontban

5.2.7 Tanúsítvány előállítás

5.2.7.1 Tanúsítványok létrehozása

Az InfoCA rendszer által kibocsátott X.509 nyilvános kulcs tanúsítványoknak meg kell felelniük az X.509 szabványnak. Minden X.509 tanúsítványba kerülő mezőt és kiterjesztést vagy az InfoCA rendszernek kell előállítania az X.509 szabvány szabályainak megfelelően, vagy a megfelelést ellenőriznie kell.

Minden tanúsítványba kerülő mezőt és kiterjesztést jóvá kell hagyni. Egy tanúsítvány mező vagy kiterjesztés értéke általában a következő négyféle mód valamelyikével hagyható jóvá:

1. Az adatot jóváhagyhatja egy regisztrációs tisztviselő (RO) manuális úton.
2. Egy automatizált eljárás alkalmazható az adatok átvizsgálására és jóváhagyására.
3. A mező vagy kiterjesztés értékét generálhatja automatikusan az InfoCA rendszer.
4. A mezőre vagy kiterjesztésre vonatkozó érték származhat a tanúsítvány profilból.

FDP_CIMC_CER.1 Tanúsítvány előállítás

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FDP_CIMC_CER.1.1 A TSF csak olyan tanúsítványokat állíthat elő, amelyek formátuma megfelelnek a következőknek: **[nyilvános kulcs tanúsítványra vonatkozó X.509 szabvány].**

FDP_CIMC_CER.1.2 A TSF csak olyan tanúsítványokat állíthat elő, amelyek megfelelnek az aktuálisan meghatározott tanúsítvány profilnak.

FDP_CIMC_CER.1.3 Amennyiben a magánkulcs digitális aláírás létrehozására is alkalmazható, a TSF-nek a tanúsítvány kibocsátása előtt ellenőriznie kell, hogy a leendő tanúsítvány alany birtokolja-e a tanúsítvány kérelemben szereplő nyilvános kulcshoz tartozó magánkulcsot, kivéve, ha a nyilvános/magán kulcspárt a TSF állította elő.

FDP_CIMC_CER.1.4 Ha a TSF X.509 nyilvános kulcsú tanúsítványokat állít elő, akkor csak olyan tanúsítványokat állíthat elő, mely megfelel az ITU-T Recommendation X.509-ben a tanúsítványokra megadott követelményeknek. A TSF-nek legalább az alábbiakat biztosítania kell:

a.) A version mező a 0, 1, vagy 2 egész számot tartalmazza.
b.) Ha a tanúsítvány tartalmaz egy issuerUniqueID-t vagy subjectUniqueID-t, akkor a version mező tartalma csak az 1 vagy 2 egész szám lehet.
c.) Ha a tanúsítvány tartalmaz kiterjesztéseket (extensions), akkor a version mező tartalma csak a 2 egész szám lehet.
d.) A serialNumber-nek egyedinek kell lennie a kibocsátó Hitelesítés-szolgáltatóra vonatkozóan.

e.) A validity mezőnek specifikálnia kell egy notBefore értéket, amely nem előzheti meg az aktuális időpontot, és egy notAfter értéket, ami nem előzheti meg a notBefore-ban megadott értéket.
f.) Ha az issuer mező egy null Name értéket tartalmaz (pl. nullák sorozatából álló megkülönböztetett neveket), akkor a tanúsítványnak tartalmaznia kell egy kritikus issuerAltName kiterjesztést.
g.) Ha a subject mező egy null Name értéket tartalmaz (pl. nullák sorozatából álló megkülönböztetett neveket), akkor a tanúsítványnak tartalmaznia kell egy kritikus subjectAltName kiterjesztést.
h.) A signature mező és a subjectPublicKeyInfo mezőben szereplő algorithm-nak egy FIPS-által jóváhagyott algoritmus OID-jét kell tartalmaznia.

5.2.7.2 Tanúsítvány profil menezsment

Egy tanúsítvány profil a tanúsítványokban előforduló mezőkre és kiterjesztésekre elfogadható értékek egy összességét határozza meg.

FMT_MOF_CIMC.3 Kiterjesztett tanúsítvány profil menedzsment

Hierarchikus fölérendeltség más összetevőkhöz képest: FMT_MOF_CIMC.2
Függések: FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése
FMT_SMR.1 Biztonsági szerepkörök

FMT_MOF_CIMC.3.1 A TSF-nek meg kell valósítania egy tanúsítvány profilt, és biztosítania kell, hogy a kiadott tanúsítványok megfelelnek az adott profilnak.

FMT_MOF_CIMC.3.2 A TSF-nek meg kell követelnie, hogy a biztonsági tisztviselők megadják a következő mezőkre és kiterjesztésekre vonatkozó elfogadható értékek összességét:
- a kulcs tulajdonosának azonosítója;
- az alany nyilvános/magán kulcspárjára vonatkozó algoritmus azonosítója;
- a tanúsítvány kibocsátójának azonosítója;
- a tanúsítvány érvényességi időtartamának hossza.

FMT_MOF_CIMC.3.3 Ha az előállított tanúsítványok X.509 tanúsítványok, a TSF-nek meg kell követelnie, hogy a biztonsági tisztviselők megadják a következő mezőkre és kiterjesztésekre vonatkozó elfogadható értékek összességét:
- keyUsage;
- basicConstraints;
- certificatePolicies.

FMT_MOF_CIMC.3.4 A biztonsági tisztviselőknek meg kell adniuk a tanúsítvány kiterjesztések elfogadható összességét.

5.2.8 Tanúsítvány visszavonás kezelés

5.2.8.1 Tanúsítvány visszavonási lista érvényesítés

A TOE által kibocsátott tanúsítvány visszavonási listáknak (CRL-ek) meg kell felelniük az X.509 szabványnak. Egy CRL-be kerülő minden mezőt vagy kiterjesztést a TOE-nek kell előállítania az X.509 szabványnak megfelelően.

FDP_CIMC_CRL.1 Tanúsítvány visszavonási lista érvényesítés

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FDP_CIMC_CRL.1.1 Egy CRL-t kibocsátó TSF-nek ellenőriznie kell, hogy minden, a CRL-ben kötelezően szereplő mező megfelel az ITU-T Recommendation X.509-nek. Legalább a következő tételeket érvényesíteni (ellenőrizni) kell:

1. Ha a version mező szerepel, akkor annak 1-et kell tartalmaznia.
2. Ha a CRL tartalmaz kritikus kiterjesztést, akkor a version mezőnek szerepelnie kell, s az 1 egész számot kell tartalmaznia.
3. Ha az issuer mező egy null Name értéket tartalmaz (pl. nullák sorozatából álló megkülönböztetett neveket), akkor a CRL-nek tartalmaznia kell egy kritikus issuerAltName kiterjesztést.
4. A signature mezőnek és a signatureAlgorithm mezőnek egy FIPS által jóváhagyott algoritmus OID-jét kell tartalmaznia.
5. A thisUpdate mezőnek a CRL kibocsátásának dátumát kell jeleznie.
6. A nextUpdate mezőben (ha ki van töltve) megadott idő nem előzheti meg a thisUpdate mezőben megadott időt.

5.2.8.2 OCSP alap-válasz érvényesítés

A TOE által kiadott OCSP alap-válaszoknak meg kell felelniük az IETF RFC 2560-nek. Egy OCSP válaszban lévő minden mezőt és kiterjesztést a TOE-nek kell előállítania az IETF RFC 2560-nek megfelelően.

FDP_CIMC_OCSP.1 OCSP alap-válasz érvényesítés

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FDP_CIMC_OCSP.1.1 A TSF-nek ellenőriznie kell, hogy az OCSP válasz minden kötelező mezője az IETF RFC 2560-ben megadottaknak megfelelő értéket tartalmaz. Legalább a következő tételeket kell érvényesíteni:

1. A **version** mezőnek egy **0**-t kell tartalmaznia.
2. Ha az **issuer** mező egy null **Name** értéket tartalmaz (pl. nullák sorozatából álló megkülönböztetett neveket), akkor a válasznak tartalmaznia kell egy kritikus **issuerAltName** kiterjesztést.
3. A **signatureAlgorithm** mezőnek egy FIPS által jóváhagyott algoritmus OID-jét kell tartalmaznia.
4. A **thisUpdate** mezőnek azt az időpontot kell jeleznie, amikor a jelzett állapotot helyesnek tudják.

5. A **producedAt** mezőnek azt az időpontot kell jeleznie, amikor az OCSP válaszadó aláírta a választ.
6. A **nextUpdate** mezőben (ha ki van töltve) megadott idő nem előzheti meg a **thisUpdate** mezőben megadott időt.

5.2.8.3 Tanúsítvány állapot export

A TOE-nek képesnek kell lennie tanúsítvány állapot információk exportálására. Minden olyan TOE által küldött üzenetnek, amely tanúsítvány állapot információkat tartalmaz, az adat exportálásra megadott követelményeken túl ki kell elégítenie az alábbi követelményt is:

FDP_CIMC_CSE.1 Tanúsítvány állapot export

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FDP_CIMC_CSE.1.1 Tanúsítvány állapot információt a TOE-ból csak olyan üzenetben lehet exportálni, melynek formátuma megfelel az alábbiaknak: [**CRL esetén: RFC 5280, OCSP esetén: RFC 2560**].

5.2.8.4 Tanúsítvány visszavonási lista profil menedzsment

Egy tanúsítvány visszavonási lista profil arra szolgál, hogy egy tanúsítvány visszavonási listában szereplő mezőkre és kiterjesztésekre elfogadható értékeket határozzon meg. A tanúsítvány visszavonási lista profilban megadható információkra példák az alábbiak:

- extensions – azon kiterjesztések összessége, amelyeket bele lehet/kell venni egy tanúsítvány visszavonási listába, és minden kiterjesztés esetében a kritikusságot mutató bit értéke;
- issuer, issuerAltName – a tanúsítvány visszavonási lista kibocsátójának a neve;
- nextUpdate – egy tanúsítvány visszavonási lista élettartama.

FMT_MOF_CIMC.5 Kiterjesztett tanúsítvány visszavonási lista profil menedzsment

Hierarchikus fölérendeltség más összetevőkhöz képest: FMT_MOF_CIMC.4
Függések: FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése
FMT_SMR.1 Biztonsági szerepkörök

FMT_MOF_CIMC.5.1 Ha a TSF tanúsítvány visszavonási listákat (CRL) bocsát ki, akkor a TSF-nek meg kell valósítania egy tanúsítvány visszavonási lista profilt, és biztosítania kell, hogy a kibocsátott tanúsítvány visszavonási listák megfelelnek az adott profilnak.

FMT_MOF_CIMC.5.2 Ha a TSF tanúsítvány visszavonási listákat (CRL) bocsát ki, akkor a TSF-nek meg kell követelnie, hogy a rendszeradminisztrátor megadja a következő mezőkre és kiterjesztésekre vonatkozó elfogadható értékek összességét:
- issuer;
- issuerAltName (Megjegyzés: ha a TOE nem bocsát ki tanúsítvány visszavonási listákat ezzel a kiterjesztéssel, akkor ezt nem kell belevenni a tanúsítvány visszavonási lista profilba);
- nextUpdate (vagyis a tanúsítvány visszavonási lista élettartama).

FMT_MOF_CIMC.5.3 Ha a TSF tanúsítvány visszavonási listákat (CRL) bocsát ki, akkor a rendszeradminisztrátornak meg kell adnia a tanúsítvány visszavonási listák és tanúsítvány visszavonási lista bejegyzés kiterjesztések elfogadható összességét.

5.2.8.5 Valós idejű tanúsítvány állapot protokoll (OCSP) profil menedzsment

Egy valós idejű tanúsítvány állapot protokoll (OCSP) profil arra szolgál, hogy meghatározza az OCSP válaszban szereplő mezőkre vonatkozó elfogadható értékek összességét. Az OCSP profil specifikálhatja azon válaszok típusát (típusait), amelye(ke)t a TOE előállíthat (vagyis a responseType-ra elfogadható értékeket), és az elfogadható válasz típusokban szereplő mezőkre vonatkozó elfogadható értékeket. Példa egy OCSP profil által az alap-válasz típusra megadható értékre: **ResponderID (**az OCSP válaszadó azonosítója).

FMT_MOF_CIMC.6 OCSP profil menedzsment

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése
FMT_SMR.1 Biztonsági szerepkörök

FMT_MOF_CIMC.6.1 A TSF-nek meg kell valósítania egy OCSP profilt, és biztosítania kell, hogy a kibocsátott OCSP válaszok megfelelnek az OCSP profilnak.

FMT_MOF_CIMC.6.2 A TSF-nek meg kell követelnie, hogy a biztonsági adminisztrátor megadja a responseType mezőre vonatkozó elfogadható értékek összességét (kivéve, ha a TOE csak alap-válasz típusú válaszokat tud kibocsátani).

FMT_MOF_CIMC.6.3 A TSF-nek meg kell követelnie, hogy a biztonsági adminisztrátor megadja az alap-válasz típusban szereplő ResponderID mezőre vonatkozó elfogadható értékek összességét.

5.2.9 Időbélyegzés

Ez az alfejezet az időbélyegzés szolgáltatásra vonatkozó követelményekkel foglalkozik.

5.2.9.1 Időbélyeg létrehozása

A TOE által kiadott időbélyeg válaszokban lévő minden mezőt és kiterjesztést a TOE-nek kell előállítania az IETF RFC 3161-nek megfelelően.

FDP_CWA_TS.1 Időbélyeg válasz érvényesítés

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FDP_CWA_TS.1.1 Egy időbélyeg válaszokat kibocsátó TSF-nek ellenőriznie kell, hogy az időbélyeg válaszban kötelezően szereplő minden mező megfelel az IETF RFC 3161-nek. Legalább a következő tételeket érvényesíteni (ellenőrizni) kell:

1. Csak olyan időbélyeg kérésre szabad időbélyeg választ kibocsátani, mely a **hashAlgorithm** mezőben egy NHH által jóváhagyott algoritmus OID-jét tartalmazza.
2. Amennyiben a válaszban a status mező 0 vagy 1 értéket vesz fel (van időbélyeg token az időbélyeg válaszban), akkor a **digestAlgorithm DigestAlgorithmIdentifier** és a **signatureAlgorithm SignatureAlgorithmIdentifier** mezőknek egy-egy NHH által jóváhagyott algoritmus OID-jét kell tartalmaznia.

5.2.9.2 Időbélyeg profil menedzsment

Az időbélyeg profil arra szolgál, hogy meghatározza az időbélyeg válaszban szereplő mezőkre és kiterjesztésekre vonatkozó elfogadható értékek összességét. Az időbélyeg profil azt is specifikálhatja, hogy milyen típusú (az RFC 3161 szabvány előírásainak megfelelő) időbélyeg kérésekre adható csak válasz (pl. a nonce opcionális értékét elvárja-e kötelezően kitöltöttnek).

FMT_MOF_CWA.1 Időbélyeg profil menedzsment

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése
FMT_SMR.1 Biztonsági szerepkörök

FMT_MOF_CWA.1.1 Ha a TSF időbélyeg válaszokat bocsát ki (időbélyegzés szolgáltatást biztosít), akkor a TSF-nek meg kell valósítania egy időbélyeg profilt, és biztosítania kell, hogy a kibocsátott időbélyeg válaszok megfelelnek az időbélyeg profilnak.

FMT_MOF_CWA.1.2 Ha a TSF időbélyeg válaszokat bocsát ki (időbélyegzés szolgáltatást biztosít), akkor a TSF-nek meg kell követelnie, hogy a rendszeradminisztrátor megadja az időbélyeg kérésekben a nonce mezőre vonatkozó elfogadható értékek összességét.

FMT_MOF_CWA.1.3 Ha a TSF időbélyeg válaszokat bocsát ki (időbélyegzés szolgáltatást biztosít), akkor a rendszeradminisztrátornak meg kell adnia az időbélyeg válasz kiterjesztések elfogadható összességét.

5.3 A TOE garanciális biztonsági követelményei

Jelen biztonsági előirányzat a kibővített EAL4 értékelési garanciaszintet követeli meg. /A kibővítés az ALC_FLR.2 (Hibajelentési eljárások) garanciális összetevő hozzávételét jelenti./

A kibővített EAL4 értékelési garanciaszint összetevőit az 5-6. táblázat tekinti át.

Garancia-osztály	**Garancia-család**	**EAL4 garanciaszint**	
		garanciaösszetevők sorszáma és elnevezése	
Konfiguráció kezelés	ACM_AUT	1	ACM_AUT.1 Részleges konfiguráció kezelés automatizálás
	ACM_CAP	4	ACM_CAP.4 A generálás támogatása és elfogadási eljárások
	ACM_SCP	2	ACM_SCP.2 A biztonsági hibákat követő konfiguráció kezelés
Kiszállítás és működtetés	ADO_DEL	2	ADO_DEL.2 A módosítás kimutatása
	ADO_IGS	1	ADO_IGS.1 Hardver telepítés, szoftver telepítés, a beindítás eljárásai
Fejlesztés	ADV_FSP	2	ADV_FSP.2 Teljesen meghatározott külső interfészek
	ADV_HLD	2	ADV_HLD.2 Biztonságot érvényre juttató magas szintű tervezés
	ADV_IMP	1	ADV_IMP.1 A biztonsági funkciók részleges kivitelezési dokumentálása
	ADV_LLD	1	ADV_LLD.1 Leíró alacsony szintű terv
	ADV_RCR	1	ADV_RCR.1 A kölcsönös megfelelés informális szemléltetése
	ADV_SPM	1	ADV_SPM.1 Informális biztonságpolitikai modell
Útmutató dokumentumok	AGD_ADM	1	AGD_ADM.1 Adminisztrátori útmutató
	AGD_USR	1	AGD_USR.1 Felhasználói útmutató
Az életciklus támogatása	ALC_DVS	1	ALC_DVS.1 A biztonsági intézkedések azonosítása
	ALC_FLR	2	ALC_FLR.2 Hibajelentési eljárások
	ALC_LCD	1	ALC_LCD.1 A fejlesztő által meghatározott életciklus modell
	ALC_TAT	1	ALC_TAT.1 Jól meghatározott fejlesztői eszközök
Tesztelés	ATE_COV	2	ATE_COV.2 A teszt lefedettség elemzése
	ATE_DPT	1	ATE_DPT.1 A magas szintű terv tesztelése
	ATE_FUN	1	ATE_FUN.1 Funkcionális tesztelés
	ATE_IND	2	ATE_IND.2 Független tesztelés - mintán
A sebezhetőség felmérése	AVA_MSU	2	AVA_MSU.2 A vizsgálatok megerősítése
	AVA_SOF	1	AVA_SOF.1 Az értékelés tárgya biztonsági funkcióinak erősségértékelése
	AVA_VLA	2	AVA_VLA.2 Független sebezhetőség vizsgálat

5-6. táblázat – Az ALC_FLR.2-vel kibővített EAL4 értékelési garanciaszint összefoglalása

5.3.1 Konfiguráció menedzselés (ACM, Assurance: Configuration Management)

ACM_AUT.1: Részleges konfiguráció menedzselés automatizálás

Fejlesztői feladatok:

- ACM_AUT.1.1D A fejlesztőnek egy konfiguráció menedzselés rendszert kell használnia.
- ACM_AUT.1.2D A fejlesztőnek egy konfiguráció menedzselés tervet kell átadnia.

A bizonyíték elemek tartalma és bemutatása:

- ACM_AUT.1.1C A konfigurálás menedzsment rendszernek automatizált eszközöket kell biztosítania, mely csak jogosult változtatásokat enged végrehajtani az értékelés tárgya megvalósítási reprezentációiban.
- ACM_AUT.1.2C A konfigurálás menedzsment rendszernek automatizált eszközöket kell biztosítania az értékelés tárgya generálásának támogatására.
- ACM_AUT.1.3C A konfigurálás menedzsment tervnek le kell írnia a konfigurálás menedzsment rendszerben használt automatizált eszközöket.
- ACM_AUT.1.4C A konfigurálás menedzsment tervnek le kell írnia, hogy a konfigurálás menedzsment rendszerben hogyan használják az automatizált eszközöket.

Értékelői feladatelemek:

- ACM_AUT.1.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására

ACM_CAP.4: A generálás támogatása és elfogadási eljárások

Fejlesztői feladatok:

- ACM_CAP.4.1D A fejlesztőnek meg kell adnia az értékelés tárgya hivatkozást.
- ACM_CAP.4.2D A fejlesztőnek egy konfiguráció menedzselés rendszert kell használnia.
- ACM_CAP.4.3D A fejlesztőnek egy konfiguráció menedzselés dokumentációt kell átadnia.

A bizonyíték elemek tartalma és bemutatása:

- ACM_CAP.4.1C Az értékelés tárgya hivatkozásnak egyedi módon kell azonosítania az értékelés tárgya verzióit.
- ACM_CAP.4.2C Az értékelés tárgyát meg kell jelölni ezzel a hivatkozással.
- ACM_CAP.4.3C A konfiguráció menedzselés dokumentációnak tartalmaznia kell egy konfiguráció listát, egy konfiguráció menedzselés tervet és egy elfogadási tervet.
- ACM_CAP.4.4C A konfiguráció listának le kell írnia az értékelés tárgyát alkotó konfiguráció elemeket.
- ACM_CAP.4.5C A konfiguráció menedzselés dokumentációnak le kell írnia a konfiguráció elemek egyedi azonosításához használt módszert.
- ACM_CAP.4.6C A konfiguráció menedzselés rendszernek egyedi módon kell azonosítania minden konfiguráció elemet.
- ACM_CAP.4.7C A konfiguráció menedzselés tervnek le kell írnia a konfiguráció menedzselés rendszer használatát.
- ACM_CAP.4.8C A bizonyítékoknak meg kell mutatniuk, hogy a konfiguráció menedzselés rendszer a konfiguráció menedzselés tervnek megfelelően működik.

- ACM_CAP.4.9C A konfiguráció menedzselés dokumentációnak bizonyítékot kell adnia arra, hogy minden konfiguráció elemet megfelelően kezeltek és kezelnek a konfiguráció menedzselés rendszer alapján.
- ACM_CAP.4.10C A konfiguráció menedzselés rendszernek gondoskodnia kell arról, hogy csak jogosult változtatások történhessenek a konfiguráció elemekben.
- ACM_CAP.4.11C A konfiguráció menedzselés rendszernek támogatnia kell az értékelés tárgya generálását.
- ACM_CAP.4.12C Az elfogadási tervnek le kell írni az értékelés tárgya részét képező konfiguráció elemek módosítására vagy újra létrehozására vonatkozó elfogadási eljárásokat.

Értékelői feladatelemek:

- ACM_CAP.4.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására

ACM_SCP.2: A biztonsági hibákat követő konfiguráció menedzselés

Fejlesztői feladatok:

- ACM_SCP.2.1D A fejlesztőnek konfiguráció menedzselés dokumentációt kell készítenie.

A bizonyíték elemek tartalma és bemutatása:

- ACM_SCP.2.1C A konfiguráció menedzselés dokumentációnak meg kell mutatnia, hogy a konfiguráció menedzselés rendszer nyomon követi legalább a következő konfiguráció elemeket: a TOE megvalósítási reprezentációja, tervezési dokumentációk, tesztelési dokumentáció, felhasználói és adminisztrátori dokumentációk, a konfiguráció menedzselés dokumentáció, valamint a biztonsági hibák.
- ACM_SCP.2.2C A konfiguráció menedzselés dokumentációnak le kell írnia, hogyan követi nyomon a konfiguráció menedzselés rendszer a különböző konfiguráció elemeket.

Értékelői feladatelemek:

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

5.3.2 Kiszállítás és működtetés (ADO, Assurance: Delivery and Operation)

ADO_DEL.2: A módosítás kimutatása

Fejlesztői feladatok:

- ADO_DEL.2.1D A fejlesztőnek dokumentálnia kell az értékelés tárgya vagy annak részei felhasználóhoz való szállításának eljárásait.
- ADO_DEL.2.2D A fejlesztőnek használnia kell a szállítási eljárásokat.

A bizonyítékelemek tartalma és megjelenésmódja:

- ADO_DEL.2.1C A szállítási dokumentációnak le kell írnia minden olyan eljárást, amely az értékelés tárgyának a felhasználó telephelyére történő szállítása során a biztonság fenntartásához szükséges.
- ADO_DEL.2.2C A szállítási dokumentációnak le kell írnia, hogy a különböző eljárások és műszaki intézkedések hogyan biztosítják a módosítások detektálását, vagy minden más eltérést a fejlesztő mester kópiája és a felhasználó helyszínén kapott verzió között.
- ADO_DEL.2.3C A szállítási dokumentációnak le kell írnia, hogy a különböző eljárások hogyan teszik detektálhatóvá a hamisítást, még abban az esetben is, amikor a fejlesztő nem küld semmit a felhasználónak.

Értékelői tevékenységelemek:

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

ADO_IGS.1 Hardver telepítés, szoftver telepítés, a beindítás eljárásai

Fejlesztői feladatok:

- ADO_IGS.1.1D A fejlesztőnek dokumentálnia kell a biztonságos hardver és szoftver telepítéshez, valamint az indításhoz szükséges eljárásokat.

A bizonyítékelemek tartalma és megjelenésmódja:

- ADO_IGS.1.1C A dokumentációnak le kell írnia a biztonságos hardver és szoftver telepítéshez, valamint az indításhoz szükséges lépéseket.

Értékelői tevékenységelemek:

- ADO_IGS.1.1E Az értékelőnek meg kell arról győződnie, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek
- ADO_IGS.1.2E Az értékelőnek meg kell állapítania a hardver és szoftver telepítés, valamint az indítás eljárásairól, hogy azok biztonságos konfigurációt eredményeznek-e.

5.3.3 Fejlesztés (ADV, Assurance: Development)

ADV_FSP.2: Teljesen meghatározott külső interfészek

Fejlesztői feladatok:

- ADV_FSP.2.1D A fejlesztőnek funkcionális specifikációt kell átadnia.

A bizonyíték elemek tartalma és bemutatása:

- ADV_FSP.2.1C A funkcionális specifikációnak informális stílusban le kell írnia a TSF-t (az értékelés tárgya biztonsági funkcióit) és annak külső interfészeit.
- ADV_FSP.2.2C A funkcionális specifikációnak belsőleg konzisztensnek (ellentmondás-mentesnek) kell lennie.
- ADV_FSP.2.3C A funkcionális specifikációnak le kell írnia minden külső TSF interfész használatának célját és módját, teljesen részletezve valamennyi hatást, kivételt és hibaüzenetet.
- ADV_FSP.2.4C A funkcionális specifikációnak teljes mértékben reprezentálnia kell a TSF-t.
- ADV_FSP.2.5C A funkcionális specifikációnak egy indoklást kell adnia arra, hogy teljes mértékben reprezentálja a TSF-et.

Értékelői feladatelemek:

- ADV_FSP.1.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.
- ADV_FSP.1.2E Az értékelőnek meg kell állapítania, hogy a funkcionális specifikáció a TOE funkcionális biztonsági követelményeinek pontos és teljes megvalósulása-e.

ADV_HLD.2: Biztonságot érvényre juttató magas szintű tervezés

Fejlesztői feladatok:

- ADV_HLD.2.1D A fejlesztőnek magas szintű tervet kell átadnia.

A bizonyíték elemek tartalma és bemutatása:

- ADV_HLD.2.1C A magas szintű terv bemutatásának informálisnak kell lennie.
- ADV_HLD.2.2C A magas szintű tervnek belsőleg konzisztensnek kell lennie.
- ADV_HLD.2.3C A magas szintű tervnek le kell írnia a TSF struktúráját alrendszerek szerint.
- ADV_HLD.2.4C A magas szintű tervnek le kell írnia minden egyes TSF alrendszer által nyújtott biztonsági funkcionalitást.
- ADV_HLD.2.5C A magas szintű tervnek azonosítania kell a TSF által megkövetelt minden alapul szolgáló hardvert, förmvert és/vagy szoftvert, az ezekkel megvalósított kiegészítő védelmi mechanizmus által biztosított funkciók bemutatásával.
- ADV_HLD.2.6C A magas szintű tervnek azonosítania kell minden TSF alrendszer interfészt.
- ADV_HLD.2.7C A magas szintű tervnek azonosítania kell, hogy a TSF alrendszerek interfészei közül melyek láthatók kívülről.
- ADV_HLD.2.8C A magas szintű tervnek le kell írnia minden TSF alrendszer interfész használatának célját és módját, azok hatásával, kivételekkel és hibaüzenetekkel, amennyiben ez utóbbiak lényegesek.

- ADV_HLD.2.9C A magas szintű tervnek le kell írnia a TOE felosztását TSP-t érvényre juttató és egyéb alrendszerekre.

Értékelői feladatelemek:

- ADV_HLD.2.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.
- ADV_HLD.2.2E Az értékelőnek meg kell állapítania, hogy a magas szintű terv pontos és teljes megjelenítése a TOE funkcionális biztonsági követelményeinek.

ADV_IMP.1: A biztonsági funkciók részleges kivitelezési dokumentálása

Fejlesztői feladatok:

- ADV_IMP.1.1D A fejlesztőnek biztosítania kell a megvalósítási reprezentációt a TOE biztonsági funkcióinak egy kiválasztott részhalmazára.

A bizonyíték elemek tartalma és bemutatása:

- ADV_IMP.1.1C A megvalósítási reprezentációnak olyan részletességgel kell egyértelműen meghatároznia a biztonsági funkciókat, hogy ebből a biztonsági funkciók már létrehozhatóak legyenek, minden további tervezési döntés nélkül.
- ADV_IMP.1.2C A megvalósítási reprezentációnak belsőleg konzisztensnek kell lennie.

Értékelői feladatelemek:

- ADV_IMP.1.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.
- ADV_IMP.1.2E Az értékelőnek meg kell állapítania, hogy a rendelkezésére bocsátott legkevésbé absztrakt TSF reprezentáció pontos és teljes megjelenítése-e a TOE funkcionális biztonsági követelményeinek.

ADV_LLD.1: Leíró alacsony szintű terv

Fejlesztői feladatok:

- ADV_LLD.1.1D A fejlesztőnek alacsony szintű tervet kell átadnia.

A bizonyíték elemek tartalma és bemutatása:

- ADV_LLD.1.1C Az alacsony szintű terv bemutatásának informálisnak kell lennie.
- ADV_LLD.1.2C Az alacsony szintű tervnek belsőleg konzisztensnek kell lennie.
- ADV_LLD.1.3C Az alacsony szintű tervnek le kell írnia a TSF struktúráját modulok szerint.
- ADV_LLD.1.4C Az alacsony szintű tervnek le kell írnia minden modul célját.
- ADV_LLD.1.5C Az alacsony szintű tervnek meg kell határoznia a modulok közötti belső kapcsolatokat a biztosított biztonsági funkcionalitás és a más moduloktól való függés szempontjából.
- ADV_LLD.1.6C Az alacsony szintű tervnek le kell írnia, hogy a TSP-t érvényre juttató összes funkciót hogyan biztosítják.
- ADV_LLD.1.7C Az alacsony szintű tervnek azonosítania kell a TSF moduljaihoz csatlakozó valamennyi interfészt.
- ADV_LLD.1.8C Az alacsony szintű tervnek azonosítania kell, hogy a TSF moduljaihoz csatlakozó mely interfészek láthatók kívülről is.

- ADV_LLD.1.9C Az alacsony szintű tervnek le kell írnia minden TSF modulhoz kapcsolódó interfész használatának célját és módját, azok hatásával, kivételekkel, illetve hibaüzenetekkel.
- ADV_LLD.1.10C Az alacsony szintű tervnek le kell írnia a TOE felosztását TSP-t érvényre juttató és egyéb modulokra.

Értékelői feladatelemek:

- ADV_LLD.1.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.
- ADV_LLD.1.2E Az értékelőnek meg kell állapítania, hogy az alacsony szintű terv pontos és teljes megjelenítése a TOE funkcionális biztonsági követelményeinek.

ADV_RCR.1: A kölcsönös megfelelés informális szemléltetése

Fejlesztői feladatok:

- ADV_RCR.1.1D A fejlesztőnek át kell adnia a biztosított TSF reprezentációk minden egymásnak megfelelő párjának megfeleltetés-elemzését.

A bizonyíték elemek tartalma és bemutatása:

- ADV_RCR.1.1C A megfeleltetés-elemzésnek be kell mutatnia, hogy az absztraktabb TSF reprezentáció minden lényeges biztonsági funkcionalitását helyesen és teljes mértékben finomítja tovább a kevésbé absztrakt TSF reprezentáció.

Értékelői feladatelemek:

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

ADV_SPM.1: Informális biztonságpolitikai modell

Fejlesztői feladatok:

- ADV_SPM.1.1D A fejlesztőnek át kell adnia a TOE biztonsági szabályzat modelljét (TSP modell).
- ADV_SPM.1.2D A fejlesztőnek szemléltetnie kell a TSP modell és a funkcionális specifikáció közötti megfelelőséget.

A bizonyíték elemek tartalma és bemutatása:

- ADV_SPM.1.1C A TSP modellnek informálisnak kell lennie.
- ADV_SPM.1.2C A TSP modellnek le kell írnia a TSP valamennyi modellezhető szabályzatának jellemzőit és szabályait.
- ADV_SPM.1.3C A TSP modellnek tartalmaznia kell egy indoklást, mely kimutatja a modell teljességét és konzisztenciáját, a TSP valamennyi modellezhető szabályzatára nézve.
- ADV_SPM.1.4C A TSP modell és a funkcionális specifikáció közötti megfelelőség szemléltetésének meg kell mutatnia, hogy a funkcionális specifikáció valamennyi biztonsági funkciója teljes és konzisztens a TSP modellhez viszonyítva.

Értékelői feladatelemek:

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

5.3.4 Útmutató dokumentumok (AGD, Assurance: Guidance Documents)

AGD_ADM.1: Adminisztrátori útmutató

Fejlesztői feladatok:

- AGD_ADM.1.1D A fejlesztőnek a TOE adminisztrátorai számára adminisztrátori útmutatót kell készítenie és beadnia.

A bizonyíték elemek tartalma és bemutatása:

- AGD_ADM.1.1C Az adminisztrátori útmutatónak le kell írnia a TOE adminisztrátora rendelkezésére álló adminisztrátori funkciókat és interfészeket.
- AGD_ADM.1.2C Az adminisztrátori útmutatónak le kell írnia, hogy hogyan kell a TOE-t biztonságos módon adminisztrálni.
- AGD_ADM.1.3C Az adminisztrátori útmutatónak tartalmaznia kell azon funkciókkal és jogosultságokkal kapcsolatos figyelmeztetéseket, melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.
- AGD_ADM.1.4C Az adminisztrátori útmutatónak le kell írnia a felhasználói viselkedéssel kapcsolatos minden feltételezést, mely a TOE biztonságos üzemelése szempontjából lényeges.
- AGD_ADM.1.5C Az adminisztrátori útmutatónak le kell írnia minden biztonsági szempontból fontos paramétert, mely az adminisztrátor ellenőrzése alá tartozik, jelezve (ahol ez lehetséges) a biztonságos értékeket.
- AGD_ADM.1.6C Az adminisztrátori útmutatónak le kell írnia minden adminisztratív funkcióval kapcsolatban végrehajtandó, biztonsági szempontból fontos esemény típusát, ideértve a TSF ellenőrzése alá eső egyedek biztonsági tulajdonságait.
- AGD_ADM.1.7C Az adminisztrátori útmutatónak konzisztensnek kell lennie minden más, értékeléshez beadott dokumentációval.
- AGD_ADM.1.8C Az adminisztrátori útmutatónak le kell írnia minden olyan, az informatikai környezetre vonatkozó biztonsági követelményt, mely az adminisztrátor számára fontos.

Értékelői feladatelemek:

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

AGD_USR.1: Felhasználói útmutató

Fejlesztői feladatok:

- AGD_USR.1.1D A fejlesztőnek a TOE felhasználói számára felhasználói útmutatót kell készítenie és átadnia.

A bizonyíték elemek tartalma és bemutatása:

- AGD_USR.1.1C A felhasználói útmutatónak le kell írnia a TOE nem adminisztrátor felhasználói rendelkezésére álló funkciókat és interfészeket.
- AGD_USR.1.2C A felhasználói útmutatónak le kell írnia, hogy a TOE által a felhasználók számára hozzáférhető biztonsági funkciókat hogyan kell biztonságosan használni.
- AGD_USR.1.3C A felhasználói útmutatónak tartalmaznia kell azon felhasználók által hozzáférhető funkciókkal és jogosultságokkal kapcsolatos figyelmeztetéseket, melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.
- AGD_USR.1.4C A felhasználói útmutatónak egyértelműen be kell mutatnia minden felhasználói feladatot, mely a TOE biztonságos üzemeltetéséhez szükséges, ideértve azokat, melyek a TOE biztonsági környezetére vonatkozó leírásban található feltételezésekhez kapcsolódnak és a felhasználói viselkedést írják le.
- AGD_USR.1.5C A felhasználói útmutatónak konzisztensnek kell lennie minden más, értékeléshez beadott dokumentációval.
- AGD_USR.1.6C A felhasználói útmutatónak le kell írnia minden olyan, az informatikai környezetre vonatkozó biztonsági követelményt, mely a felhasználó számára fontos.

Értékelői feladatelemek:

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

5.3.5 Életciklus támogatás (ALC, Assurance: Life Cycle Support)

ALC_DVS.1: A biztonsági intézkedések azonosítása

Fejlesztői feladatok:

- ALC_DVS.1.1D A fejlesztőnek a fejlesztés biztonságáról dokumentációt kell készítenie.

A bizonyíték elemek tartalma és bemutatása:

- ALC_DVS.1.1C A fejlesztés biztonságáról szóló dokumentációnak le kell írnia minden olyan fizikai, eljárásbeli, személyi és egyéb biztonsági intézkedést, mely a TOE bizalmasságának és sértetlenségének a védelméhez szükséges, annak tervezési, megvalósítási és fejlesztési környezetében.
- ALC_DVS.1.2C A fejlesztési biztonságról szóló dokumentációnak bizonyítékot kell szolgáltatnia arról, hogy ezeket az intézkedéseket betartják a TOE fejlesztése és támogatása során.

Értékelői feladatelemek:

- ALC_DVS.1.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.
- ALC_DVS.1.2E Az értékelőnek meg kell győződnie arról, hogy a biztonsági intézkedéseket betartják.

ALC_LCD.1: A fejlesztő által meghatározott életciklus modell

Fejlesztői feladatok:

- ALC_LCD.1.1D A fejlesztőnek egy a TOE fejlesztéséhez és karbantartáshoz használt életciklus modellt kell felállítania.
- ALC_LCD.1.2D A fejlesztőnek dokumentálnia kell az életciklus modellt.

A bizonyíték elemek tartalma és bemutatása:

- ALC_LCD.1.1C Az életciklus modell dokumentációnak le kell írnia a TOE fejlesztéséhez és karbantartásához használt modellt.
- ALC_LCD.1.2C Az életciklus modellnek biztosítania kell a TOE fejlesztéséhez és karbantartásához szükséges ellenőrzést.

Értékelői feladatelemek:

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

ALC_TAT.1:Jól meghatározott fejlesztő eszközök

Fejlesztői feladatok:

- ALC_TAT.1.1D A fejlesztőnek azonosítania kell a TOE-hez használt fejlesztő eszközöket.
- ALC_TAT.1.2D A fejlesztőnek dokumentálnia kell a fejlesztő eszközök kiválasztott megvalósítás-függő opcióit.

A bizonyíték elemek tartalma és bemutatása:

- ALC_TAT.1.1C A megvalósításhoz használt fejlesztő eszközöknek jól meghatározottaknak kell lenniük.
- ALC_TAT.1.2C A fejlesztő eszközök dokumentációjának egyértelműen meg kell határoznia az implementáció során használt valamennyi utasítás jelentését.
- ALC_TAT.1.3C A fejlesztő eszközök dokumentációjának egyértelműen meg kell határoznia valamennyi megvalósítás-függő opció jelentését.

Értékelői feladatelemek:

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

ALC_FLR.2 A hibajavítás értékelése

Fejlesztői feladatok:

- ALC_FLR.2.1D A fejlesztőnek biztosítania kell a hibajavítási eljárásait tartalmazó dokumentációt.
- ALC_FLR.2.2D A fejlesztőnek eljárásokat kell kidolgoznia a biztonsági hibák jelentéseinek, valamint a hibajavítási kérelmek elfogadására és feldolgozására.
- ALC_FLR.2.3D A fejlesztőnek hibajavítási útmutatót kell biztosítania a TOE felhasználói számára.

A bizonyíték elemek tartalma és bemutatása:

- ALC_FLR.2.1C A hibajavítási eljárások dokumentációjának le kell írnia azokat az eljárásokat, melyek a TOE minden kibocsátott verziójában felfedett és jelentett összes biztonsági hiba nyomon követését hivatottak biztosítani.
- ALC_FLR.2.2C A hibajavítási eljárásoknak meg kell követelniük, hogy minden egyes biztonsági hibához leírják a hiba jellegét és következményét, valamint a hiba kijavításához vezető megoldás-keresési folyamat állapotát.
- ALC_FLR.2.3C A hibajavítási eljárásoknak meg kell követelniük, hogy minden biztonsági hibához azonosítva legyenek a javítási tevékenységek.
- ALC_FLR.2.4C A hibajavítási eljárások dokumentációjának le kell írnia azokat a módszereket, amelyekkel a hibákról szóló információk, a javítások, valamint a TOE felhasználók számára készített útmutatók biztosításához használnak.
- ALC_FLR.2.5C A hibajavítási eljárások dokumentációjának le kell írnia egy olyan eszközt, mely segítségével a fejlesztő megkapja a TOE felhasználóktól a TOE-ben feltételezett biztonsági hibákkal kapcsolatos jelentéseket, illetve az ezekre vonatkozó érdeklődést.
- ALC_FLR.2.6C A jelentett biztonsági hibák feldolgozására vonatkozó eljárásoknak biztosítaniuk kell, hogy bármely jelentett hibát kijavítanak és a javításokat továbbítják a TOE felhasználóknak.
- ALC_FLR.2.7C A jelentett biztonsági hibák feldolgozási eljárásainak óvintézkedéseket kell biztosítaniuk arra, hogy egy javítás sem vezet be semmilyen újabb hibát.
- ALC_FLR.2.8C A hibajavítási útmutatónak le kell írnia egy olyan eszközt, melynek segítségével a TOE felhasználók jelenthetik a fejlesztőnek a TOE feltételezett hibáit.

Értékelői feladatelemek:

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

5.3.6 Tesztek (ATE, Assurance: Tests)

ATE_COV.2: A teszt lefedettség elemzése

Fejlesztői feladatok:

- ATE_COV.2.1D A fejlesztőnek a teszt lefedettségére vonatkozó elemzést kell szolgáltatnia.

A bizonyíték elemek tartalma és bemutatása:

- ATE_COV.2.1C A teszt lefedettség elemzése mutassa be a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikációban leírt TOE biztonsági funkciók közötti megfeleltetést.
- ATE_COV.2.2C A teszt lefedettség elemzésének be kell mutatnia, hogy a funkcionális specifikációban leírt TOE biztonsági funkciók és a tesztelési dokumentációban azonosított tesztek közötti megfeleltetés teljes.

Értékelői feladatelemek:

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

ATE_DPT.1: A magas szintű terv tesztelése

Fejlesztői feladatok:

- ATE_DPT.1.1D A fejlesztőnek gondoskodnia kell a tesztelés mélységének elemzéséről.

A bizonyítékok tartalma és bemutatása:

- ATE_DPT.1.1C A tesztelés mélység elemzése mutassa be, hogy a tesztelési dokumentációban azonosított tesztek elegendőek a biztonsági funkciók magas szintű tervnek megfelelő működésének a demonstrálásához.

Értékelői feladatelemek:

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

ATE_FUN.1: Funkcionális tesztelés

Fejlesztői feladatok:

- ATE_FUN.1.1D A fejlesztőnek le kell tesztelnie a TOE biztonsági funkcióit, és dokumentálnia kell az eredményeket.
- ATE_FUN.1.2D A fejlesztőnek el kell készítenie, és át kell adnia a tesztelési dokumentációt.

A bizonyítékok tartalma és bemutatása:

- ATE_FUN.1.1C A tesztelési dokumentációnak tartalmaznia kell a tesztelési terveket, a teszt eljárások leírását, a várt teszteredményeket és a tényleges tesztelési eredményeket.
- ATE_FUN.1.2C A tesztelési terveknek azonosítaniuk kell a tesztelendő biztonsági funkciókat, és le kell írniuk a végrehajtandó tesztek célját.

- ATE_FUN.1.3C A teszt eljárások leírásának azonosítania kell a végrehajtandó teszteket, és le kell írnia a tesztelési forgatókönyvet minden biztonsági funkcióra. A forgatókönyveknek tartalmazniuk kell minden, a tesztek sorrendiségére vonatkozó függőséget.
- ATE_FUN.1.4C A várt teszteredményeknek meg kell mutatniuk a tesztek sikeres végrehajtásából keletkező várható kimenteket.
- ATE_FUN.1.5C A fejlesztő által elvégzett tesztelés eredményeinek be kell mutatniuk, hogy minden tesztelt biztonsági funkció a specifikált módon működött.

Értékelői feladatelemek:

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

ATE_IND.2: Független tesztelés - mintavételezés

Fejlesztői feladatok:

- ATE_IND.2.1D A fejlesztőnek át kell adnia a TOE-t tesztelésre.

A bizonyítékok tartalma és bemutatása:

- ATE_IND.2.1C A TOE-nek tesztelésre alkalmas állapotban kell lennie.
- ATE_IND.2.2C A fejlesztőnek biztosítania kell a TSF fejlesztői funkcionális tesztelése során használt erőforrás-készlettel ekvivalens eszközkészletet.

Értékelői feladatelemek:

- ATE_IND.2.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.
- ATE_IND.2.2E Az értékelőnek tesztelnie kell a TSF megfelelő részeit annak megállapításához, hogy a TOE a specifikáltnak megfelelően működik-e.
- ATE_IND.2.3E Az értékelőnek végre kell hajtania a tesztelési dokumentációban szereplő tesztek valamely részhalmazát (mintáját) a fejlesztői teszt eredmények ellenőrzése érdekében.

5.3.7 A sebezhetőség felmérése (AVA, Assurance: Vulnerability Assessment)

AVA_MSU.2: A vizsgálatok megerősítése

Fejlesztői feladatok:

- AVA_MSU.2.1D A fejlesztőnek el kell készítenie az útmutató dokumentációkat.
- AVA_MSU.2.2D A fejlesztőnek egy elemzést kell dokumentálnia az útmutató dokumentációkról.

A bizonyíték elemek tartalma és bemutatása:

- AVA_MSU.2.1C Az útmutatónak azonosítani kell a TOE összes lehetséges üzemmódját (beleértve a meghibásodás vagy üzemhiba utáni műveleteket is), és azok biztonságos üzemeltetésre gyakorolt kihatásait és következményeit.
- AVA_MSU.2.2C Az útmutatónak teljesnek, egyértelműnek, következetesnek és megalapozottnak kell lennie.
- AVA_MSU.2.3C Az útmutatónak fel kell sorolnia minden feltételezést a leendő üzemi környezetről.
- AVA_MSU.2.4C Az útmutatónak számba kell vennie a külső biztonsági intézkedésekkel kapcsolatos minden követelményt (beleértve a külső eljárásbeli, fizikai és személyi intézkedéseket is).
- AVA_MSU.2.5C A fejlesztői elemzésnek ki kell mutatnia az útmutatók teljességét.

Értékelői feladatelemek:

- AVA_MSU.2.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.
- AVA_MSU.2.2E Az értékelőnek meg kell ismételnie minden konfigurációs és telepítési eljárást, annak megállapítása érdekében, hogy a TOE kizárólag az átadott útmutató dokumentáció alapján biztonságosan konfigurálható és használható.
- AVA_MSU.2.3E Az értékelőnek meg kell határoznia, hogy az útmutató dokumentáció használatával észrevehető-e minden nem biztonságos állapot.
- AVA_MSU.2.4E Az értékelőnek meg kell erősítenie, hogy a fejlesztői elemzés kimutatja, hogy az útmutató a TOE valamennyi működési módjában útmutatást ad a biztonságos működtetésre.

AVA_SOF.1: Az értékelés tárgya biztonsági funkcióinak erősségértékelése

Fejlesztői feladatok:

- AVA_SOF.1.1D A fejlesztőnek a biztonsági előirányzatban definiált minden funkcióerősségi követelménnyel rendelkező mechanizmusra el kell végeznie egy biztonsági funkcióerősség elemzést.

A bizonyíték elemek tartalma és bemutatása:

- AVA_SOF.1.1C Minden TOE biztonsági funkcióerősségi követelménnyel rendelkező mechanizmus esetén az elemzésnek meg kell mutatnia, hogy a funkció erőssége azonos vagy magasabb szintű annál, amely a védelmi profilban / biztonsági előirányzatban minimális erősségi szintként szerepel.

- AVA_SOF.1.2C Minden TOE biztonsági funkcióerősségi követelménnyel rendelkező mechanizmus esetén az elemzésnek meg kell mutatnia, hogy a funkció erőssége azonos vagy magasabb szintű, mint a védelmi profilban / biztonsági előirányzatban megadott minimális erősségi mérték.

Értékelői feladatelemek:

- AVA_SOF.1.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.
- AVA_SOF.1.2E Az értékelőnek meg kell győződni arról, hogy az erősségi követelmények helyesek.

AVA_VLA.2: Független sebezhetőség vizsgálat

Fejlesztői feladatok:

- AVA_VLA.2.1D A fejlesztőnek végre kell hajtania és dokumentálnia kell a TOE útmutatók elemzését, olyan módszerek után kutatva, melyekkel egy felhasználó megsértheti a TSP-t.
- AVA_VLA.2.2D A fejlesztőnek dokumentálnia kell az azonosított sebezhetőségek kiküszöbölését.

A bizonyíték elemek tartalma és bemutatása:

- AVA_VLA.2.1C A dokumentációnak meg kell mutatnia minden azonosított sebezhetőség esetén, hogy azt a TOE célkörnyezetében nem lehet kihasználni.
- AVA_VLA.2.2C A dokumentációnak igazolnia kell, hogy a TOE az azonosított sebezhetőségekre ellenáll a nyilvánvaló áthatolási támadásoknak.

Értékelői feladatelemek:

- AVA_VLA.2.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.
- AVA_VLA.2.2E Az értékelőnek a fejlesztői sebezhetőségi elemzés alapján le kell folytatnia a áthatolás tesztelést, annak biztosítása érdekében, hogy az azonosított sebezhetőségeket valóban kivédték.
- AVA_VLA.2.3E Az értékelőnek végre kell hajtania a független sebezhetőségi elemzést.
- AVA_VLA.2.4E Az értékelőnek független áthatolás tesztelést kell elvégeznie a független sebezhetőségi elemzés alapján, a célkörnyezetben feltételezhető további azonosított sebezhetőségek kihasználhatóságának meghatározása céljából.
- AVA_VLA.2.5E Az értékelőnek meg kell határoznia, hogy a TOE ellenáll-e egy alacsony támadási képességgel bíró támadó által végrehajtott áthatolási támadásnak.

6. TOE összefoglaló előírás

A TOE összefoglaló előírás az InfoCA rendszer biztonsági követelményeit teljesítő biztonsági funkciókat tartalmazza. Leírja az InfoCA rendszer összes biztonsági funkcióját és garanciális intézkedését, amelyek az InfoCA rendszer biztonsági követelményeinek a kielégítéséhez járulnak hozzá.

6.1 A TOE biztonsági funkciói

A biztonsági követelmények teljesítése érdekében az InfoCA rendszer az alábbi biztonsági funkciókat valósítja meg.

- BF1: Bizalmi munkakörök kezelése
- BF2: Azonosítás és hitelesítés
- BF3: Hozzáférés ellenőrzés
- BF4: Kulcskezelés
- BF5: Biztonsági naplózás
- BF6: A szolgáltatások által létrehozott és fogadott üzenetek védelme
- BF7: Tanúsítvány előállítás
- BF8: Tanúsítvány visszavonás
- BF9: Visszavonás állapot (CRL, OCSP)
- BF10: Időbélyegzés

Az alábbiak részletezik az egyes biztonsági funkciókat, meghatározva azt is, hogy az egyes biztonsági funkciók mely funkcionális biztonsági követelmények (SFR) kielégítéséhez járulnak hozzá, illetve milyen (informatikai vagy nem informatikai) környezeti támogatást (ezen belül mely IT környezetre vonatkozó SFR-ek külső kielégítését) várnak el.

6.1.1 BF1: Bizalmi munkakörök kezelése (jogosultság kezelés)

Ennek a biztonsági funkciónak az a célja, hogy a különböző jogosultságokat egységesen és biztonságosan kezelje, egyúttal az utólagos felelősségre vonhatóságot is biztosítsa.

Az InfoCA rendszer és környezete együttesen az alábbi, különböző jogokkal bíró munkaköröket különbözteti meg és kezeli:

- rendszer biztonsági tisztviselő (SSO, System Security Officer),
- biztonsági tisztviselő (SO, Security Officer),
- regisztrációs tisztviselő (RO, Registration Officer),
- rendszeradminisztrátor,
- rendszerüzemeltető,
- rendszervizsgáló

6.1.1.1 Az InfoCA rendszer jogosultság kezelése

Az InfoCA rendszer az alábbi, különböző jogokkal bíró munkaköröket különbözteti meg:

- **Rendszer biztonsági tisztviselő**: Az SSO egyetlen feladata a rendszerben a biztonsági tisztviselők (SO-k) fiókjának engedélyezése és törlése. /Az SO fiókok létrehozásához, módosításához és törléséhez két különböző SSO aláírás kell a megfelelő konfigurációs fájlra. Az SSO kulcsok ellenőrzéséhez szükséges tanúsítványokat az InfoCA rendszer program bináris változata titkosítva tartalmazza. Az InfoCA rendszer három SSO tanúsítványt tartalmaz, ezek közül bármely kettő együtt jogosult az SSO feladatok ellátására./
- **Biztonsági tisztviselő:** Az SO-k kezelhetik a CA paramétereit és profiljait, ezáltal ők vezérlik a CA automatikus működését. Az SO-k másik jogosulsága a regisztrációs tisztviselők (RO-k) engedélyezése és törlése. /A konfigurációs állományok megadásához, illetve az RO fiókok létrehozásához, módosításához és törléséhez két különböző SO aláírása szükséges a megfelelő fájlokra./ A fentieken kívül az SO-k jogosultak új LDAP fák felépítésére az adatbázisból.
- **Regisztrációs tisztviselő:** A végfelhasználói tanúsítványokkal kapcsolatos műveletek végrehajtására feljogosított személyek. Jogosultságuktól függően az alábbi kérelmek kiadásáért (összeállításáért, aláírásáért és CA-hoz továbbításáért) felelősek
  - Tanúsítvány kérelem elkészítése (Issue),
  - Visszavonási kérelem beadása (Revocation),
  - Felfüggesztési kérelem beadása (Hold),
  - Felfüggesztett tanúsítvány újra aktíválása (Activate),
  - Magánkulcs (és tanúsítvány) visszaállítás kérelem beadása (Key Recovery),
  - Magánkulcshoz tartozó PIN kódok újranyomtatása (PIN reprint),
  - Külső fájlból beolvasott kérések tartalmának módosítása (May modify setting).

  /Az RO-k tehát különböző típusú kéréseket küldhetnek a CA-nak. Az RO-k által küldött kérések mindig digitális aláírással vannak ellátva./

Az InfoCA rendszer képes a felhasználókat összekapcsolni a fenti munkakörökkel.

Ez a biztonsági funkció a következő SFR-ek kielégítésére irányul: **FMT_SMF.1 (iteráció 2), FMT_SMR.2 (iteráció 2), FMT_MOF.1 (iteráció 3), FMT_MSA.1 (iteráció 2), FMT_MSA.1 (iteráció 3), FMT_MSA.2 (iteráció 2), FMT_MSA.3 (iteráció 2).**

6.1.1.2 A környezet támogatása

A környezetnek jelentős támogatást kell adnia a bizalmi munkakörök kezeléséhez.

Az alábbi munkaköröket az IT környezet (operációs rendszer, illetve elkülönült Syslog szerver) különbözteti meg:

- **rendszeradminisztrátor**: Az InfoCA rendszer, valamint a syslog szervert futtató operációs rendszer rendszergazdája, aki jogosult az InfoCA rendszer telepítésére és alap konfigurálására, az InfoCA rendszer környezetében megbízható szerepkört betöltő felhasználók (rendszerüzemeltetők, rendszervizsgálók) fiókjának kezelésére.
- **rendszerüzemeltető**: Az InfoCA rendszer mindennapos működéséért felelős személy, aki az InfoCA rendszer elindítására és leállítására, valamint kézi mentésére és helyreállítására is fel van hatalmazva.
- **rendszervizsgáló:** Az InfoCA rendszer naplóinak (syslog szerver) karbantartására (olvasására, keresések végrehajtására), valamint az archívumok megtekintésére feljogosított személy.

Az IT környezet a fentiekkel kielégíti a következő SFR-eket: **FMT_SMF.1 (iteráció 1)**, **FMT_MOF.1 (iteráció 1)**, **FMT_MOF.1 (iteráció 2), FMT_MTD.1 (iteráció 1)**, **FMT_MTD.1 (iteráció 2)**, **FMT_MSA.1 (iteráció 1), FMT_MSA.2 (iteráció 1), FMT_MSA.3 (iteráció 1)**, valamint támogatja a következő SFR-t: **FMT_SMR.2 (iteráció 1)**.

Eljárásrendi intézkedésekkel kell biztosítani az alábbiakat:

- egy felhasználó nem tölthet be egyszerre rendszeradminisztrátor és rendszervizsgáló szerepkört,
- egy felhasználó nem tölthet be egyszerre rendszeradminisztrátor és (az InfoCA rendszer által kezelt) tisztviselői (SSO, SO vagy RO) szerepkört,
- egy felhasználó nem tölthet be egyszerre rendszervizsgáló és (az InfoCA rendszer által kezelt) tisztviselői (SSO, SO vagy RO) szerepkört.

A nem-IT környezet a fentiekkel támogatja a következő SFR-t: **FMT_SMR.2 (iteráció 1)**.

6.1.2 BF2: Azonosítás és hitelesítés

Ennek a biztonsági funkciónak a célja a jogosult felhasználók egyértelmű azonosítása, valamint a biztonsági jellemzők (pl. munkakörök, jogosultságok) felhasználókkal való pontos összekapcsolásának a biztosítása.

Az InfoCA rendszer és környezete együttesen valósítja meg az InfoCA rendszer működéséhez szükséges főbb elemeket működtető felhasználók azonosítását és hitelesítést, amiről a 6-1. táblázat ad áttekintést:

Az InfoCA rendszer elemei	Az adott elem felhasználói (szerepkörök szerint)	A felhasználói azonosítást és hitelesítést végző rendszer/elem
InfoCA .exe	rendszerüzemeltető	környezet (operációs rendszer)
Setup_InfoCA.exe	rendszeradminisztrátor	környezet (operációs rendszer)
InfoCAKeySetup.exe	rendszeradminisztrátor	környezet (operációs rendszer)
InfoCASetup .exe	**SSO, SO**	**InfoCA rendszer**
InfoRA.exe	**SO, RO**	**InfoCA rendszer**
Setup_InfoRA.exe	rendszeradminisztrátor	környezet (operációs rendszer)
Syslog szerver	rendszervizsgáló	környezet (operációs rendszer)

6-1. táblázat – A felhasználók azonosítása és hitelesítése terén megvalósuló munkamegosztás az InfoCA rendszer és környezete között

6.1.2.1 Az InfoCA rendszer felhasználó azonosítása és hitelesítése

Az InfoCA rendszer (pontosabban az InfoCA rendszer alábbi elemei: InfoCASetup.exe, InfoRA.exe) minden felhasználójától (SSO, SO és RO) megköveteli, hogy azonosítsa magát, és az azonosság sikeres hitelesítésének kell megelőznie az adott felhasználó vagy a felhasználó feltételezett szerepköre nevében történő bármely további művelet végrehajtásának az engedélyezését.

Az InfoCA rendszer valamennyi bizalmi munkakört betöltő felhasználója (SSO, SO, RO) rendelkezik egy aláíró kulcspárral. Az SO és RO kulcspárok nyilvános kulcs része egy nyilvános kulcsú tanúsítványba foglalva az operációs rendszer tanúsítványtárában és a biztonsági beállításokat tartalmazó InfoCA.so és InfoCA.ro fájlokban helyezkedik el, míg a három SSO nyilvános kulcsát a programkód tartalmazza (miután a InfoCAKeySetup.exe elhelyezte ezeket). A kulcspárok magánkulcs részét tulajdonosa egy intelligens kártyán tárolja, s egy PIN aktivizáló kóddal aktivizálhatja azt.

A felhasználó azonosítása a képernyőn megjelenített tanúsítványok közül a megfelelő kiválasztásával történik, a hitelesítés pedig a tanúsítványhoz tartozó magánkulcs aktivizálásával (a tároló intelligens kártya behelyezésével és a PIN kód megadásával), egy véletlen sorozat digitális aláírásával valósítható meg. A digitális aláírás sikeres ellenőrzése igazolja, hogy valóban a kiválasztott tanúsítvány alanya (a megfelelő magánkulcs birtokosa) az adott felhasználó.

Sikeres hitelesítés esetén az InfoCA rendszer a hitelesített felhasználó biztonsági tulajdonságait (szerepkör, s az ebből adódó jogosultságok) összekapcsolja az adott felhasználó nevében tevékenykedő szubjektumokkal.

Sikertelen hitelesítés esetén az InfoCA rendszer adott eleme (InfoCASetup.exe, InfoRA.exe) leáll.

Az InfoCA rendszerben minden felhasználó számára kötelező az újrahitelesítés kijelentkezés után, illetve új szerepkörben való ismételt bejelentkezés esetén.

Ez a biztonsági alfunkció a következő SFR-ek kielégítésére irányul: **FIA_ATD.1 (iteráció 2), FIA_AFL.1 (iteráció 2), FIA_UID.1 (iteráció 2), FIA_UAU.1 (iteráció 2), FIA_USB.1 (iteráció 2).**

6.1.2.2 A környezet támogatása

Az InfoCA rendszer környezete minden felhasználójától (rendszeradminisztrátor, rendszerüzemeltető, rendszervizsgáló) megköveteli, hogy azonosítsa magát, és az azonosság sikeres hitelesítésének kell megelőznie az adott felhasználó vagy a felhasználó feltételezett munkaköre nevében történő bármely további művelet végrehajtásának az engedélyezését.

Az azonosítás és hitelesítés a felhasználói név és az ehhez tartozó jelszó bekérésével és ellenőrzésével, vagy az operációs rendszer által támogatott intelligens kártyával valósul meg.

Sikeres hitelesítés esetén az IT környezet (operációs rendszer) a hitelesített felhasználó biztonsági tulajdonságait (szerepkör, s az ebből adódó jogosultságok) összekapcsolja az adott felhasználó nevében tevékenykedő szubjektumokkal.

Amennyiben a rendszeradminisztrátor által konfigurálható „hitelesítési kísérletek maximális száma” darab sikertelen hitelesítési kísérlet történik az érintett felhasználói azonosító legutolsó sikeres hitelesítése óta, a környezet (operációs rendszer) az érintett rendszerüzemeltető, rendszervizsgáló fiókját blokkolja, illetve az érintett rendszeradminisztrátort 1 perc várakoztatás után ismételt azonosításra/hitelesítésre szólítja fel.

Az InfoCA rendszer környezetében minden felhasználó számára kötelező az újrahitelesítés kijelentkezés után, illetve új szerepkörben való ismételt bejelentkezés esetén.

Ez a biztonsági alfunkció a következő SFR-ek kielégítésére irányul: **FIA_ATD.1 (iteráció 1), FIA_AFL.1 (iteráció 1), FIA_UID.1 (iteráció 1), FIA_UAU.1 (iteráció 1), FIA_USB.1 (iteráció 1).**

6.1.3 BF3: Hozzáférés ellenőrzés

Ennek a biztonsági funkciónak a célja a védendő értékekhez való hozzáférések ellenőrzése, illetve korlátozása.

Mind az InfoCA rendszer, mind annak környezete egy hasonló és igen szígorú hozzáférés ellenőrzési szabályt juttat érvényre, melyet az 5.1.3.1 és 5.2.3.1 pontok ismertetnek.

Az ellenőrzési szabály lényege a következő:

- a felhasználók számára a következők alapján biztosított: az objektumokhoz (adatok/fájlok) való hozzáférés: azonosító, szerepkör, az igényelt hozzáférés típusa, a hozzáférési kérelem tartalma, és egy magánkulcs birtoklása,
- a felhasználók azonosítása magában foglalja az alábbiakat: különböző hozzáférési jogosultságokkal rendelkező személyek, különböző hozzáférési jogosultságokkal rendelkező szerepkörök, egy vagy több különböző hozzáférési jogosultságokkal rendelkező szerepkörrel felruházott személyek,
- hozzáférés típusok: olvasás,írás, végrehajtás.

Mind az InfoCA rendszer, mind annak környezete azt is biztosítja, hogy a fenti hozzáférés ellenőrzési szabályt érvényre juttató funkciók valóban meghívódnak, és sikeresen befejeződnek, mielőtt az engedélyezendő műveletek végrehajtása lehetővé válik.

6.1.3.1 Az InfoCA rendszer hozzáférés ellenőrzése

Az InfoCA rendszer a rendszer-, illetve felhasználói objektumokhoz való minden hozzáférést ellenőriz.

Az azonosított és hitelesített felhasználóknak az általuk betöltött szerepkör alapján kizárólag a 6-2. táblázatban szereplő hozzáféréseket engedélyezi.

A jogosultság ellenőrzését mindig a CA (InfoCA.exe elem) végzi két lépésben kerül sor:

- első lépés a fiókok, konfigurációs állományok, profilok, regisztrációs kérelmek aláírásának az ellenőrzése,
- második lépés (érvényes aláírás esetén) az aláíró jogosultságának elenőrzése.

A CA (InfoCA.exe elem) egyaránt visszautasítja az érvényes aláírás nélküli, illetve a jogosulatlanul aláírt állományokat (fiókok, konfigurációs állományok, profilok, regisztrációs kérelmek).

Az RO-k által a különböző kérések elkészítése és kiadása előtti ellenőrzések nem az InfoCA rendszer, hanem annak környezetének a hatáskörébe tartoznak.

Ez a biztonsági funkció a következő SFR-ek kielégítésére irányul: **FDP_ACC.1 (iteráció 2), FDP_ACF.1 (iteráció 2), FPT_RVM.1 (iteráció 2)**

Munkakör	Engedélyezett tevékenység	Az InfoCA rendszer érintett eleme
Rendszer biztonsági tisztviselő (SSO)	SO fiók (account) létrehozása, módosítása, törlése /a három SSO-ból kettőnek az aláírása kell/	InfoCA InfoCA Setup
Biztonsági tisztviselő (SO):	RO fiók létrehozása, módosítása, törlése /két különböző SO aláírása kell/ A CA paraméterek és profilok menedzselése (a konfigurációs állományok megadása) /két különböző SO aláírása kell/	InfoCA InfoCA Setup
Biztonsági tisztviselő (SO):	LDAP fa újraépítése adatbázisból	Info RA
Regisztrációs tisztviselő (RO)	Tanúsítvány kérelem elkészítése (Issue), Visszavonási kérelem beadása (Revocation), Felfüggesztési kérelem beadása (Hold), Felfüggesztett tanúsítvány újra aktiválása (Activate), Magánkulcs (és tanúsítvány) visszaállítás kérelem beadása (Key Recovery), Magánkulcshoz tartozó PIN kódok újranyomtatása (PIN reprint), Külső fájlból beolvasott kérések tartalmának módosítása egy tanúsítványprofilon belül (May modify setting). /Minden RO fiók létrehozásakor, vagy annak módosításakor az SO-k külön engedélyezhetik az alábbi jogosultságokat, minden tanúsítványprofilra külön-külön: Issue, Revocation, Hold, Activate, Key Recovery, PIN reprint. Minden tanúsítványprofil létrehozásakor vagy annak módosításakor az SO-k külön-külön engedélyezhetik az alábbi jogosultságot: May modify setting./	Info RA.

6-2. táblázat: Az InfoCA rendszer szerepkör alapú hozzáfésér ellenőrzése

6.1.3.2 A környezet támogatása

Az IT környezet az alábbiak biztosításával támogatja a hozzáférés ellenőrzést:

- Az operációs rendszer egy olyan biztonsági tartományt biztosít az InfoCA rendszer számára, ami megvédi azt a nem megbízható egyedek általi beavatkozástól és hamisítástól (futás közben).
- Az RO-k által a különböző kérések elkészítése és kiadása előtt a kérés kiadhatóságának ellenőrzése (pl. hogy egy alanytól beérkező visszavonási kérés jogosult kérés-e).

Az IT környezet a fentiekkel kielégíti a következő SFR-eket: **FPT_SEP.1, FDP_ACC.1 (iteráció 1), FDP_ACF.1 (iteráció 1), FPT_RVM.1 (iteráció 1)**

6.1.4 BF4: Kulcskezelés

Az InfoCA rendszerben a kulcsok az alábbi kategóriákba sorolhatók:

- **tanúsítvány és CRL aláíró kulcsok** - a tanúsítvány előállítás és visszavonás szolgáltatás kulcspárja, amellyel a különböző tanúsítványokat és visszavonási listákat írja alá az InfoCA rendszer.
- **infrastrukturális kulcsok** – az InfoCA rendszer által az alábbi folyamatokhoz használt kulcs: naplórekordok aláírása,
- **rendszervezérlési kulcsok** – az InfoCA rendszer bizalmas munkakört betöltő felhasználói által használt kulcsok, melyek hitelesítési-, aláírási- vagy bizalmassági szolgáltatásokat biztosítanak.
- **végfelhasználói kulcsok** – az InfoCA rendszer által (a HSM-ben vagy az RA-hoz csatlakozó intelligens kártyán) az ügyfelek számára előállított kulcspárok.

Az InfoCA rendszerben az IT környezet részét képező kriptográfiai hardver eszközök végzik a kriptográfiai szempontból biztonságkritikus funkciók döntő többségét (lásd 6.1.4.2). Maga az InfoCA rendszer a HSM modul aktivizálásával lát el bizonyos kulcskezelési feladatokat (lásd 61.4.1).

6.1.4.1 Az InfoCA rendszer kulcskezelése

Ennek az összetett biztonsági funkciónak a célja az InfoCA rendszer által kezelt különböző funkciókat betöltő magán- titkos és nyilvános kulcsok biztonságos menedzselése.

Az alábbi biztonsági alfunkciókból áll:

- kulcsok generálása és törlése,
- titkosító magánkulcsok exportálása
- felhasználói titkos kulcsok kezelése
- titkosító magánkulcsok letétbe helyezése, tárolása és visszaállítása,
- a nyilvános kulcsok védelme.

<u>Kulcsok generálása és törlése</u>

Az InfoCA rendszer nem generál és nem töröl titkos vagy magánkulcsot (a kulcsgenerálás és törlés a környezet részét képező HSM-ben, illetve a megbízható munkaköröket betöltő felhasználók intelligens kártyáiban történik).

<u>Titkosító magánkulcsok exportálása</u>

Az ügyfelek számára generált titkosító magánkulcsok kezelése az alábbi feladatokat jelenti:

- a titkosító magánkulcsok generálása (ez a környezet részét képező kriptográfiai hardver eszközben (HSM) történik),
- a titkosító magánkulcsok exportálása a HSM-ből (ezt az InfoCA rendszer végzi). Ez két céllal is történik: az ügyfelekhez való továbbítás, illetve az InfoCA adatbázisban való tárolás érdekében. A magánkulcsok titkosítva kerülnek exportálásra.
- a titkosító magánkulcsok védett tárolása adatbázisban (ezt is az InfoCA rendszer végzi).

Ez a biztonsági alfunkció a következő SFR-ek kielégítésére irányul: **FDP_ETC_CIMC.5, FDP_ACF_CIMC.2.**

Felhasználói titkos kulcsok kezelése

Felhasználói titkos kulcsok (letétbe helyezett magánkulcsok visszaállításához szükséges jelszavak) (HSM által) titkosítva kerülnek letárolásra.

Ez a biztonsági alfunkció a következő SFR kielégítésére irányul: **FDP_ACF_CIMC.3**.

A nyilvános kulcsok védelme

Az InfoCA által adatbázisban tárolt végfelhasználói nyilvános kulcsok tanúsítványba foglalva, (az InfoCA szolgáltató kulcsával aláírt módon) digitális aláírással védve vannak a jogosulatlan módosítással szemben.

Ez a biztonsági alfunkció a következő SFR kielégítésére irányul: **FDP_SDI_CIMC.3**

6.1.4.2 A környezet támogatása

Az IT környezet részét képező kriptográfiai hardver eszközök végzik a kriptográfiai szempontból biztonságkritikus funkciók döntő többségét:

- a HSM-ben, illetve a megbízható munkaköröket betöltő felhasználók intelligens kártyáiban történik minden titkos és magánkulcs generálása /**FCS_CKM.1**/,
- A HSM tárolja és védi a tanúsítvány aláíró kulcsot /**FMT_MTD_CIMC.4/**
- a HSM, illetve a megbízható munkaköröket betöltő felhasználók intelligens kártyáik végzik a titkos és magánkulcsok megsemmisítését /**FCS_CKM.4, FCS_CKM_CIMC.5**/,
- a HSM, illetve a megbízható munkaköröket betöltő felhasználók intelligens kártyáik hajtják végre a kriptográfiai műveletek többségét, köztük valamennyi magánkulcs aktivizálással járó műveletet /**FCS_COP.1**/,
- a HSM-ben tárolt tanúsítvány aláíró magánkulcs exportálása (titokmegosztással) és helyreállítása /**FMT_MTD_CIMC.7**/.

6.1.5 BF5: Biztonsági naplózás

Ennek az összetett biztonsági funkciónak a célja a teljes körű ellenőrzés lehetőségének a megteremtése, az összes biztonsági szempontból fontos tevékenység egyértelmű nyomon követhetőségének a biztosításával.

A biztonsági naplózás tekintetében az InfoCA rendszer csak a legalapvetőbb funkciókat valósítja meg: naplóeseményeket generál megfelelő adatokkal, az eseményeket össszeköti a kiváltásukban közreműködő felhasználókkal, valamint digitálisan aláírja a naplóeseményeket.

A naplóesemények az InfoCA rendszerből generálásukat és aláírásukat követően azonnal kikerülnek, egy Syslog szerverre továbbítódnak. Ezt követően az InfoCA rendszer környezetének (Syslog szerver operációs rendszere, különböző alkalmazások és eljárásrendek) a feladata a naplórekordok megvédése, áttekintése és kiértékelése.

6.1.5.1 Az InfoCA rendszer biztonsági naplózása

Az alábbi biztonsági alfunkciókból áll:

- BF5.1: Napló adatok generálása megfelelő adatokkal
- BF5.2 A naplóbejegyzések sértetlenségének garantálása

Napló adatok generálása megfelelő adatokkal

Az InfoCA rendszer naplózza mindazokat az eseményeket, amelyek az 5-5. táblázatban szerepelnek. Ezek lefedik a jelen biztonsági előirányzat valamennyi funkcionális követelményére a CC által alap szinten elvárt naplózandó eseményeket, egyúttal átfogják a hitelesítés-szolgáltatás nyújtásának teljes folyamatát, és lehetővé teszik minden olyan esemény rekonstruálását, melyre a hitelesítés-szolgáltatással kapcsolatos valós helyzetek megítéléséhez szükség lehet.

Az InfoCA rendszer naplózási funkciója elindul és leáll minden esetben, amikor az InfoCA rendszer elindul és leáll, egyúttal ez utóbbi két esemény is naplózásra kerül.

Az InfoCA rendszer az általa létrehozott naplóbejegyzéseket egy syslog szervernek küldi el. (A konfigurálás során kötelező egy helyes naplószerver megadása, enélkül a rendszer nem indul el.)

Minden naplóbejegyzésbe bekerülnek az alábbi információk:

- az esemény dátuma,
- az esemény időpontja,
- az esemény típusa,
- szubjektum azonosító (amennyiben ez jellemző),
- az esemény kimenetele (siker vagy sikertelenség).

Minden olyan naplóesemény, melynek kiváltásában felhasználó működött közre, egyértelműen össze van kapcsolva ennek a felhasználónak az InfoCA rendszerben használt azonosítójával (szubjektum azonosító), így a felhasználók cselekedeteikért utólag felelősségre vonhatók.

A naplóba nem kerülnek nyílt formában magán, vagy titkos kulcsok, illetve olyan egyéb biztonsági paraméterek, melyek illetéktelen megismerése biztonsági szempontból kritikus lenne.

Ez a biztonsági alfunkció a következő SFR-ek kielégítésére irányul: **FAU_GEN.1, FAU_GEN.2.**

A naplóbejegyzések sértetlenségének garantálása

Az InfoCA rendszer a napló adatok sértetlenségének garantálása érdekében, valamint a sértetlenség ellenőrzésére az alábbiakat biztosítja:

- Az InfoCA rendszer a naplóbejegyzések sértetlenségét egy folyamatos, adatbázisban is letárolt lenyomat értékkel biztosítja.
- Minden naplóeseményre egy digitális aláírás készül (egy infrastrukturális kulccsal, melyet a HSM modul aktivizál), s az aláírandó adatok közé bekerül a korábbi naplóbejegyzésekre számolt lenyomat érték is.

Ez a biztonsági alfunkció a következő SFR-ek kielégítésére irányul: **FPT_CIMC_TSP.1.**

6.1.5.2 A környezet támogatása

Az InfoCA rendszer környezetének igen komoly támogatást kell biztosítania a biztonsági naplózás funkcióhoz.

Az InfoCA rendszer (informatikai) környezetének az alábbiakat kell biztosítania:

- meg kell megvédenie a Syslog szerveren tárolt naplórekordokat a jogosulatlan törléssel szemben, s észlelnie kell a naplóállományok esetleges megváltoztatását (**FAU_STG.1**),
- garantálnia kell, hogy naplóbejegyzések feldolgozásuk előtt ne veszhessenek el /megfelelő tárhely biztosításával, valamint a rendelkezésre álló tárhely betelése esetén a legrégebben tárolt naplórekordok felülírásával/ (**FAU_STG.4**),
- biztosítania kell a rendszervizsgálók számára azt a lehetőséget, hogy a naplóbejegyzésekből minden információt értelmezhető formában kiolvassanak (**FAU_SAR.1**),
- lehetőséget kell biztosítania a naplóbejegyzésben történő keresések végrehajtására az események típusa, valamint az esemény kiváltásáért felelős felhasználó szerint (**FAU_SAR.3**),
- független időforrással (rendszeridő) biztosítania kell a naplórekordokba kerülő időpont megbízhatóságát (**FPT_STM.1**),
- képesnek kell lennie különböző szabályok alkalmazására a naplóesemények figyelemmel kísérése során, s ezen szabályok alapján a biztonsági szabályzat potenciális megsértésének jelzésére (**FAU_SAA.1** és **FAU_ARP.1**)

6.1.6 BF6: A szolgáltatások által létrehozott és fogadott üzenetek védelme

Ennek a biztonsági funkciónak a célja az InfoCA rendszernek küldött adatok, valamint az innen kikerülő adatok sértetlenségének, hitelességének és (szükség esetén) bizalmasságának a biztosítása.

Az InfoCA rendszer biztonságot növelő különlegessége, hogy a biztonsági szempontból kritikus CA alrendszernek ügyfelekkel nincs közvetlenül kommunikációs kapcsolata:

- az ügyfelektől származó kérések helyességét és jogosultságát az InfoCA rendszer környezete végzi el, s a helyes és jogosult kéréseket az RO-k továbbítják az RA-ból a CA-nak,
- a CA-hoz beérkező kérésekre születő egyik lehetséges választípus (kibocsátott tanúsítvány, generált kulcspár, kinyomtatott PIN boríték, visszaállított titkosított magánkulcs) az RA közvetítésével, de szintén az InfoCA rendszer környezete által megvalósítva jut el az ügyfelekhez,
- a CA-hoz beérkező kérésekre születő másik választípus a kibocsátott visszavonási lista, melyet a CA LDAP-okba publikál, az ügyfelek azokat onnan érhetik el.

A fentiekből következően a szolgáltatások által létrehozott és fogadott üzenetek védelme az InfoCA rendszer hatókörén kívül esik. Nem így az InfoCA rendszer két alrendszere (RA és CA) közötti belső kommunikáció.

6.1.6.1 Az InfoCA rendszer által megvalósított védelem

Az InfoCA rendszer biztosítja a két alrendszere (RA és CA) között cserélt információk sértetlenségét és hitelességét:

- A CA minden általa fogadott biztonság-kritikus információt (pl. regisztrációs tisztviselő tanúsítványkérelmét, biztonsági tisztviselők által megadott vagy módosított konfigurációs állományokat) csak az erre külön feljogosított, bizalmi munkakört betöltő személyektől (RO-k, illetve SO-k) fogad el, azt is csak akkor, ha az információ érvényes digitális aláírással lett ellátva.
- A CA az általa készített tanúsítványokat és visszavonási listákat digitálisan aláírja, ezzel biztosítva az eredet bizonyíthatóságát. Szintén digitális aláírás bizonyítja a CA-ból az RA alrendszerbe átkerülő konfigurációs állományok sértetlenségét és hitelességét.

Ez a biztonsági alfunkció a következő SFR kielégítésére irányul: **FDP_ITT.1 (iteráció 4)** és **FPT_ITT.1 (iteráció 4)**.

6.1.6.2 A környezet támogatása

A biztonsági funkció környezeti támogatása az alábbiakat jelenti:

- az ügyfelek és a HSZ közötti üzenetek sértetlenségének, hitelességének és bizalmasságának a védelme,
- az RA és CA között cserélt információk bizalmasságának védelme (pl. VPN alkalmazásával).

Ez a biztonsági alfunkció a következő SFR kielégítésére irányul: **FDP_ITT.1 (iteráció 1, 2, 3)** és **FPT_ITT.1 (iteráció 1, 2, 3)**.

6.1.7 BF7: Tanúsítvány előállítás

6.1.7.1 Az InfoCA rendszer tanúsítvány előállítása

Ennek a biztonsági funkciónak a célja annak biztosítása, hogy az InfoCA rendszer alap szolgáltatásai közé tartozó tanúsítvány előállítási (köztük a kezdeti, megújítási, felülhitelesítési) kérelmek biztonságos módon hajtódjanak végre.

A végfelhasználóktól beérkező tanúsítvány kérelemben megadott adatok körének és érvényességének ellenőrzését az InfoCA rendszeren kívül végzik.

Az InfoCA rendszer ugyanakkor a regisztrációs tisztviselő számára biztosít egy mechanizmust, mely lehetővé teszi egy tanúsítvány kérelem jóváhagyását, illetve elutasítását (a kérelemben megadott adatok ellenőrzésének eredménye alapján).

A jóváhagyott (az RA-ban összeállított) tanúsítvány kérelmet a regisztrációs tisztviselő digitálisan aláírja, így kerül automatikus feldolgozásra a CA-hoz.

Az InfoCA rendszer (CA alrendszere) tanúsítvány aláírására használt magánkulcsát kizárólag a tanúsítványok és a megfelelő visszavonás állapot adatok aláírására használja fel. Az InfoCA rendszer (CA) azt is biztosítja, hogy csak érvényes (tehát nem lejárt, és nem is visszavont) tanúsítványhoz tartozó magánkulccsal ír alá tanúsítványt és CRL-t.

A tanúsítvány előállítás tanúsítvány profilokon alapul, s az InfoCA rendszer biztosítja, hogy a kiadott tanúsítványok megfelelnek valamelyik profilnak.

A CA tetszőleges számú különböző tanúsítvány profil alapján képes tanúsítványok kibocsátására. Az egyes profilok módosíthatóak és törölhetőek is a rendszerből.

Az InfoCA rendszer által kibocsátott tanúsítványokra teljesülnek az alábbiak:

- a tanúsítványok formátuma megfelel a nyilvános kulcs tanúsítványra vonatkozó X.509 szabványnak,
- a tanúsítványok megfelelnek az aktuálisan meghatározott tanúsítvány profilnak,
- a tanúsítványokban a version mező a 2 egész számot tartalmazza,
- a tanúsítványokban a serialNumber egyedi, a kibocsátó hitelesítés-szolgáltatóra vonatkozóan.
- A validity mezőben meghatározott notBefore érték nem előzheti meg az aktuális időpontot, míg a meghatározott notAfter érték nem előzheti meg a notBefore-ban megadott értéket.
- Ha az issuer mező egy null Name értéket tartalmaz (pl. nullák sorozatából álló megkülönböztetett neveket), akkor a tanúsítvány tartalmaz egy kritikus issuerAltName kiterjesztést.
- Ha a subject mező egy null Name értéket tartalmaz (pl. nullák sorozatából álló megkülönböztetett neveket), akkor a tanúsítványnak tartalmaznia kell egy kritikus subjectAltName kiterjesztést.
- A signature mező és a subjectPublicKeyInfo mezőben szereplő algorithm mindig egy SHA lenyomat alapú RSA aláíró algoritmus OID-jét tartalmazza.

A profilok meghatározásához első lépésként az alábbi általános profil adatokat kell megadni:

- Name (a profil kötelezően egyedi neve)

- CRL distribution (a CRL distribution point tanúsítvány mezők megadása)
- PIN mail templates (amennyiben a CA generál kulcspárt az adott kéréshez, mely sablonok alapján nyomtasson a CA PIN borítékot automatikusan)
- Not before (ezen paraméter bekapcsolt állapotában a CA ellenőrzi, hogy a kiadandó tanúsítvány érvényességi ideje nem lehet korábbi az itt megadott értéknél)
- Not after (ezen paraméter bekapcsolt állapotában a CA ellenőrzi, hogy a kiadandó tanúsítvány érvényességi ideje nem lehet későbbi az itt megadott értéknél)
- Minimal validity (ezen paraméter bekapcsolt állapotában a CA ellenőrzi, hogy a kiadandó tanúsítvány érvényességi ideje nem lehet rövidebb az itt megadott értéknél)
- Maximal validity (ezen paraméter bekapcsolt állapotában a CA ellenőrzi, hogy a kiadandó tanúsítvány érvényességi ideje nem lehet hosszabb az itt megadott értéknél)
- Default key length (a profil alapján kiadható tanúsítványok esetén alkalmazandó alapértelmezett kulcshossz)
- Allowed key length (a profil alapján kiadható tanúsítványok esetén engedélyezett minimális és maximális kulcshossz)
- Key recovery (A CA oldalon generált kulcsok esetén alkalmazandó későbbi visszaállíthatóságra vonatkozó szabály. Yes esetén a kulcs visszaállítható később, No esetén semmiképpen. Amennyiben az RO „may modify setting" jogosultsággal rendelkezik, a kérés összeállításakor felülbírálhatja ezt a beállítást.)
- Public key source (A nyilvános kulcsok származási helyét adja meg e paraméter. Ez lehet hardver (CA generált), szoftver (CA generált) illetve Client (RA oldalon generált). Amennyiben az RO „may modify setting" jogosultsággal rendelkezik, a kérés összeállításakor felülbírálhatja ezt a beállítást.)
- Basic constraints (a Basic constraints tanúsítvány mező paraméterei)
- Key identifier (a Subject és az Authority Key identifier mezők paraméterei)
- Quelified Certificate Policy (a minősített tanúsítványokra vonatkozó paraméterek)

A fenti általános profil adatokon túl megadhatók még az alábbi paraméterek is:

- Info Access (A profil tartalmazhatja a tanúsítványba bekerülő Authority Info Access és Subject Info Access mezők paramétereit is. Mindkét esetben OCSP, CA és Timestamp hozzáférési információkat lehet megadni. Mindháromnál URL-t lehet megadni, de nem kötelező egyik mező kitöltése sem.)
- Key Usage (külön megadhatóak a profilban a Key Usage, Extended Key Usage mezők, de emellett lehetőség van saját egyedi OID-del megadott kulcs használati értékek definiálására is.)
    - Key Usage lehetséges értékei: digitalSignature, nonRepudiation, keyCertSign, encipherOnly, decipherOnly, dataEncipherment, keyAgreement, keyEncipherment, cRLSign (az is megadható, hogy a mező kritikus legyen-e)
    - Extended Key Usage lehetséges értékei: timeStamping, serverAuth, clientAuth, codeSigning, emailProtection, OCSPSigning, smartcardLogon, IPSecEndSystem, IPSecTunnel, IPSecUser, IPSecKe,

MicrosoftSGC, NestcapeSGC (az is megadható, hogy a mező kritikus legyen-e)
    - Custom Key Usage lehetséges értékei: tetszőleges OID megadható
- Alternative Names (Az Alternative Names beállítások alatt a Subject és az Issuer Alternative Names mezők egyaránt megadhatóak. Lehetséges felépítésük és értékeik egymással azonosak.)
    - Alternative Names lehetséges értékei: Email, URI, DNS, RID, IP, Directory Name, X.400 Name, Other name, EDI party name
- Certificate Policy (Minden profilhoz egy tanúsítvány policy megadása is lehetséges. A policy több különböző policy qualifier-t is tartalmazhat. Ezeknek két típusa van: text és uri.)
    - A Certificate Policy mezői, s ezek lehetséges értékei:
        - Options (a mező kritikus legyen vagy sem)
        - Policy Identifier (a policy-t azonosító egyedi OID)
        - Policy qualifiers/text (Text, Organization és Notice number mezők)
        - Policy qualifiers/uri (Uri mező)
- LDAP szerverek (minden tanúsítvány profil egyedileg is tartalmazhat tetszőleges számú LDAP publikációs pontot is, ahová a CA setupban definiált globális LDAP mellett a tanúsítványok publikálásra kerülnek.)
- Custom Extensions (A CA a jövőben megjelenő vagy egyedi tanúsítvány mezők kezeléséhez támogatja a saját mezők definiálását. A profilok tetszőleges számú és tartalmú ilyen mezőt tartalmazhatnak, ezek érvényességére és helyességére az InfoCA Setup és az InfoCA nem tud ellenőrzéseket végezni, csak szintaktikai jellegűeket.
    - A Custom Extensions mezői, s ezek lehetséges értékei:
        - Id (a saját mezőt azonosító egyedi OID)
        - Name (a saját mező neve, mely nem jelenik meg a tanúsítványban, csak adminisztrációs célja van)
        - Long Name (a saját mező leírása, mely nem jelenik meg a tanúsítványban, csak adminisztrációs célja van)
        - Value (a mező bináris tartalma az alábbi formátumnak megfelelően: „DER:01:02:03”, azaz a kezdete minden esetben „DER:”, majd ezt követően az egyes byte-ok értékei következnek „:” jellel elválasztva egymástól)

Ez a biztonsági funkció a következő SFR-ek kielégítésére irányul: **FDP_CIMC_CER.1** és **FMT_MOF_CIMC.3.**

6.1.7.2 A környezet támogatása

A végfelhasználóktól beérkező tanúsítvány kérelemben megadott adatok körének és érvényességének ellenőrzését az InfoCA rendszeren kívül végzik. Ennek során (amennyiben a magánkulcs digitális aláírás létrehozására is alkalmazható, és a kulcspárt nem az InfoCA rendszer állította elő) azt is ellenőrizni kell, hogy a leendő tanúsítvány alany birtokolja-e a tanúsítvány kérelemben szereplő nyilvános kulcshoz tartozó magánkulcsot.

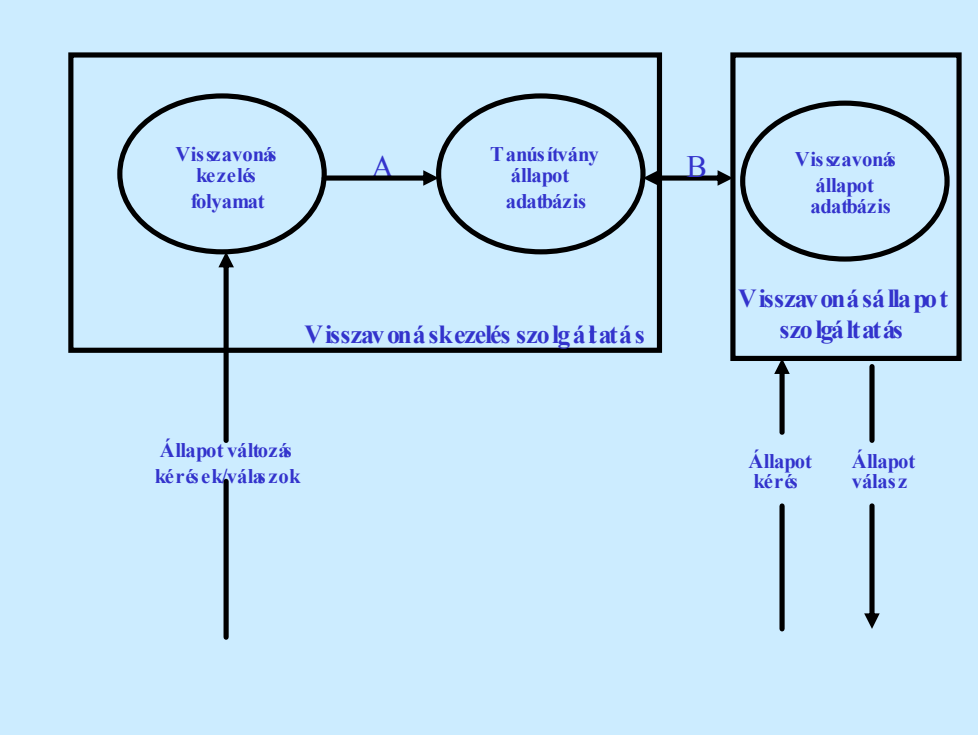
Az RO által az RA-ban összeállított és jóváhagyott (aláírt) tanúsítvány kérelmet viszont már teljes mértékben a CA dolgozza fel, ehhez nem vár el környezeti támogatást.

6.1.8 BF8: Tanúsítvány visszavonás

6.1.8.1 Az InfoCA rendszer tanúsítvány visszavonása

Ennek a biztonsági funkciónak a célja az InfoCA rendszerben kiadott tanúsítványok állapotának gondozása (tanúsítványok felfüggesztése, újra aktiválása, visszavonása), valamint a tanúsítványok állapotának CRL-ekben történő publikálása.

A „Visszavonás kezelés” és a „Visszavonás állapot” szolgáltatások tipikus együttműködési módját szemlélteti a 6-1. ábra.



6-1. ábra: A visszavonás kezelés és a visszavonás állapot szolgáltatások közötti üzenetek

A 6-1. ábrán jól látható, hogy a visszavonás kezelés szolgáltatás által kezelt (frissített) tanúsítvány állapot adatbázistól üzenetekre van szüksége a visszavonás állapot szolgáltatásnak. Ebből számos biztonsági követelmény adódik (pl. az üzenet hitelességének és sértetlenségének biztosítása és ellenőrzése).

Az InfoCA rendszerben állapot változtatást csak a regisztrációs tisztviselők kezdeményezhetik.

Az InfoCA rendszerben minden felfüggesztésre, felfüggesztés megszüntetésére (újra aktiválásra) és visszavonásra vonatkozó kérelmet a kezdeményezésre jogosult regisztrációs tisztviselő aláírásával hitelesít, melynek érvényességét a CA végrehajtás előtt ellenőriz.

Az InfoCA rendszerben egy (hitelesített és érvényesített) visszavonási, felfüggesztési és újra aktiválási kérelem az éles tanúsítvány állapot adatbázis módosításával azonnal végrehajtásra kerül.

Ha egy tanúsítványt visszavontak, azt már nem lehet újra használatba venni.

Ez a biztonsági funkció a következő SFR kielégítésére irányul: **FMT_MOF_CIMC.5**.

6.1.8.2 A környezet támogatása

A tanúsítványok visszavonását teljes mértékben az InfoCA rendszer végzi, a környezettől ehhez nem vár el támogatást.

6.1.9 BF9: Visszavonás állapot (CRL, OCSP)

6.1.9.1 Az InfoCA rendszer visszavonás állapot szolgáltatása

Ennek az összetett biztonsági funkciónak a célja a Tanúsítvány visszavonás biztonsági funkció által módosított állapotok publikálása, illetve lekérdezési lehetőségének biztosítása.

Az InfoCA rendszer kétféle visssszavonás állapot szolgáltatást támogat, az alábbi két biztonsági alfunkcióval:

- CRL visszavonás állapot publikálás,
- OCSP visszavonás állapot szolgáltatása.

CRL visszavonás állapot publikálás

Ennek a biztonsági alfunkciónak a célja a Tanúsítvány visszavonás biztonsági funkció által kezelt állapotok publikálása, szabványos visszavonási listák (CRL) formájában.

Az InfoCA rendszer egyidejűleg több független CRL profilt is képes kezelni, a visszavont tanúsítványokról a CRL profiloknak megfelelő CRL-ket generál és publikál (LDAP-ba).

Az InfoCA rendszer által kibocsátott visszavonási listákra teljesülnek az alábbiak:

- minden CRL szerkezete és tartalma megfelel az RFC 5280 előírásainak (v2),
- minden CRL tartalmát a tanúsítvány állapot adatbázis aktuális tartalma határozza meg,
- minden CRL a szolgáltatói kulccsal kerül digitális aláírásra, a digitális aláírásra használt aláíró algoritmus (rsa-sha1, rsa-sha256, rsa-sha348 vagy rsa-sha512) és kulcsméret (2048 bit) megfelel a "Biztonságos algoritmusok"-ra vonatkozó NHH elvárásoknak.
- a version mező az 1 egész értéket tartalmazza,
- ha az issuer mező egy null Name értéket tartalmaz (pl. nullák sorozatából álló megkülönböztetett neveket), akkor a CRL tartalmaz egy kritikus issuerAltName kiterjesztést,
- a signature és a signatureAlgorithm mező az rsa-sha1, rsa-sha256, rsa-sha348 és rsa-sha512 algoritmusok egyikének OID-jét tartalmazza,
- a thisUpdate mező a CRL kibocsátásának dátumát jelzi,
- a nextUpdate mezőben (ha ki van töltve) megadott idő sosem előzi meg a thisUpdate mezőben megadott időt.

Az InfoCA rendszer által publikált visszavonási listák a CRL profilok beállításától függően képesek az alábbiakra:

- a listába vagy csak végfelhasználói, vagy csak szolgáltatói tanúsítványok kerülnek be, vagy pedig mindkét fajta bekerül,
- alap CRL (egy darab, kitüntetett) vagy delta CRL (ebből több is lehet),
- automatikus CRL generálás meghatározott generálási időközönként,

- a CA minden visszavonás, felfüggesztés és újra aktiválás esetén generáljon-e CRL-t (függetlenül a generálási időköztől),
- a már lejárt tanúsítványok kikerüljenek-e a CRL-ből, és ha igen, mennyi idővel a lejárat után,
- A CRL profilok megadása során tetszőleges számú LDAP publikálási pont is megadható.

Ez a biztonsági alfunkció a következő SFR kielégítésére irányul: **FDP_CIMC_CRL.1** és **FDP_CIMC_CSE.1.**

OCSP visszavonás állapot szolgáltatása

Ennek a biztonsági alfunkciónak a célja a Tanúsítvány visszavonás biztonsági alfunkció által kezelt állapotok lekérdezhetőségének a biztosítása, szabványos OCSP kérésekre adott szabványos OCSP válaszok formájában.

Az InfoCA rendszer által támogatott OCSP szolgáltatást az alábbiak jellemzik:

Az OCSP szolgáltatás telepítéstől és konfigurálástól függő módon több üzemmódban képes futni, amelyeket a funkcionalitás és a rendelkezésére bocsájtott adatok mennyisége különböztet meg:

a) URL alapú, CRL alapján adott OCSP válasz,
b) LDAP alapú, CRL alapján adott OCSP válasz,
c) LDAP alapú, CRL és tanúsítvány keresésen alapuló válasz,
d) adatbázis alapú.

Az OCSP szolgáltatás megfelel az RFC 2560 előírásainak, az alábbiak szerint:

- az RFC 2560 szerkezeti és tartalmi elvárásainak megfelelő szabványos kérésre szabványos választ ad (v1 protokoll verziószám mellett)
- sikeres kérés feldolgozás esetén az alábbi státuszokat adja válaszként:
  - a) és b) üzemmódokban: revoked vagy unknown (vagyis az OCSP válasz csak a visszavonásra vonatkozik, az érvényességre nem)
  - c) üzemmódban: good, revoked vagy unknown (ahol a visszavonás ténye a CRL-ből dől el, az érvényesség ténye pedig abból, hogy az LDAP-ban megtalálható és érvényes-e a keresett tanúsítvány)
  - d) üzemmódban: good, revoked vagy unknown (ahol az OCSP kiszolgáló adatbázisban keresi meg a tanúsítványok érvényességi és visszavonásra vonatkozó adatait, és az alapján válaszol)
- sikertelen feldolgozás esetén az alábbi hiba választ támogatja:
  - malformedRequest (szintaktikailag vagy tartalmilag helytelen OCSP kérés esetén)
- az OCSP válaszadás felkészül az OCSP kérésben opcionálisan megjelenő alábbi elemek jelenlétére:
  - optionalSignature (ebben az esetben az opcionális aláírással a kérés sértertlenségét ellenőrzi)
- az OCSP válasz aláírását a következők jellemzik:
  - RSA aláíró algoritmus (legfeljebb 8Kbyte kulcsméret mellett)
  - konfigurálástól függően SHA-1, SHA-256, SHA-348 vagy SHA-512 hash algoritmus

    - konfigurálástól függően az OCSP válaszba foglalható az OCSP válasz aláírásához tartozó tanúsítvány
- az OCSP válaszadás támogatja az alábbi opcionális elemeket:
    - nextUpdate (amely a), b) és c) üzemmódokban megegyezik a CRL azonos paraméterével, a d) üzemmódban pedig az ocspupdate adatbázis táblában meghatározottak szerint készül)
- az OCSP válaszadás a válaszadó (ResponderID) azonosítására használható lehetőségek közül az alábbit választja:
    - byName
- az OCSP válaszadás az alábbi opcionális kiterjesztéseket támogatja:
    - Nonce
- az OCSP válaszadás egy olyan OCSP kérésre, melyben nem támogatott (nem felismert) kritikus kiterjesztés szerepel, nem ad választ és naplózza az eseményt
- az OCSP válaszadás egy olyan OCSP kérésre, melyben nem támogatott (nem felismert) nem kritikus kiterjesztés szerepel, szabályos választ ad a kiterjesztés figyelmen kívül hagyásával

Az OCSP szolgáltatás megfelel a CWA 14167-1 előírásainak, az alábbiak szerint:

- naplózásra kerül (hogy archiválhatók legyenek) az alábbi események:
    - minden OCSP kérés
    - minden OCSP válasz

Ez a biztonsági alfunkció a következő SFR kielégítésére irányul: **FDP_CIMC_CRL.1** és **FDP_CIMC_OCSP.1 és FDP_CIMC_CSE.1.**

6.1.9.2 A környezet támogatása

A visszavonás állapot biztonsági funkciót teljes egészében az InfoCA rendszer valósítja meg (a környezet támogatása nélkül).

6.1.10 BF10: Időbélyegzés

6.1.10.1 Az InfoCA rendszer időbélyegzése

Ennek az összetett biztonsági funkciónak a célja az időbélyegzés szolgáltatás megalapozása és biztosítása.

E biztonsági funkció az alábbi két biztonsági alfunkcióból áll:

- Időszinkronizálás
- Időbélyeg válaszadás

Időszinkronizálás

Ennek a biztonsági alfunkciónak a célja a pontos idő garantálása az időbélyeg válaszadás számára. A biztonsági alfunkciót megvalósító alrendszer (TimeServer modul) a rendszer belső óráját a megadott (külső) időforrásokkal szinkronba tartja. A szinkronizáció SNTP protokollon keresztül valósul meg. Amennyiben a TimeServer belső órája kiesik az időszinkronból, a szolgáltatás az időbélyeg válaszadást megvalósító alrendszer (TSS Responder modul) számára egy ennek megfelelő üzenetet ad vissza, így a szolgáltatás jelezni tudja a kérő felé, hogy az időszinkron jelenleg nem megfelelő pontosságú a kérések kiszolgálásához.

Az InfoCA rendszer informatikai környezete több független időforrást, valamint egy NTPv4 protokoll alapú ntpd programot biztosít. Az ntpd szinkronizálja a rendszeridőt, valamint meghatározza az UTC-től való eltérés maximális eltérését.

A biztonsági funkció ellenőrzi, hogy a maximális eltérés a konfigurálható határon belül van-e. Ha belül van, akkor az InfoCA rendszer ezt a rendszeridőt elfogadja, s ezt használja az időbélyegzés szolgáltatásához. Ellenkező esetben a biztonsági funkció ezt naplózza és jelzi e tényt az időbélyeg válaszadás biztonsági alfunkciónak.

Ez a biztonsági alfunkció a következő SFR kielégítésére irányul: **FPT_STM.1.**

Időbélyeg válaszadás

Ennek a biztonsági alfunkciónak a célja az RFC 3161 szabvány előírásainak megfelelő szabványos időbélyeg kérésekre szabványos időbélyeg válaszok létrehozása.

Az InfoCA rendszer az RFC 3161 szabványnak megfelelő időbélyegzést biztosít, az alábbi tulajdonságokkal:

- Az InfoCA rendszer nem ellenőrzi az időbélyeg kérések eredetét, jogosultságát (azaz a kérő esetleges azonosítását és hitelesítését az IT környezetnek kell elvégeznie)
- Az InfoCA rendszer ellenőrzi az időbélyeg kérésekben alkalmazott lenyomatkészítő algoritmust, s konfigurálástól függően csak a következőt fogadja el: SHA-1, SHA-256, SHA-348 vagy SHA-512
- Miután az InfoCA rendszer IT környezete szinkronizálja független időforrásait és meghatározza az UTC-től való eltérés maximális eltérését, az InfoCA rendszer ellenőrzi, hogy a maximális eltérés egy konfigurálható határon belül van-e. Az InfoCA rendszer biztosítja, hogy minden általa kibocsátott időbélyeg token tartalmazza az alábbiakat:
    - egyedi sorszámot
    - a használt időforrás pontosságát (ez konfigurációtól függő érték)
    - annak az időbélyegzési szabályzatnak (rendnek) az azonosítóját, amely értelmében készült.

Az InfoCA rendszer HSM-ben (biztonságos kriptográfiai modulban) generált és tárolt magánkulccsal írattatja alá az időbélyeg tokeneket (időbélyeg válaszokat). A környezet garantálja azt is, hogy az időbélyeg tokeneket aláíró magánkulcsot másra nem használják.

Az InfoCA rendszer biztosítja, hogy az időbélyeg válasz ugyanazokat az adatokat tartalmazza, mint amit a kérésben küldtek.

Az InfoCA rendszer (megfelelő konfigurációval) biztosítja, hogy a HSM biztonságos aláírást használ az időbélyeg válasz aláírására.

Az időbélyeg szolgáltatás megfelelve a CWA 14167-1 előírásainak (archiválási célból) naplóz minden időbélyeg tokent.

Ez a biztonsági funkció a következő SFR kielégítésére irányul: **FDP_CWA_TS.1** és **FMT_MOF_CWA.1**.

6.1.10.2 A környezet támogatása

Az IT környezet (a független időforrások és a szinkronizáló program biztosításával) támogatja a megbízható időpont előállítását, kielégítve ezzel a következő SFR-t: *FPT_STM.1 (iteráció 1)*

Az IT környezetnek kell ellenőriznie az időbélyeg kérések jogosultságát is (azaz a kérő esetleges azonosítását és hitelesítését).

6.2 Biztonsági funkcióerősség

Egy biztonsági előirányzatnak azonosítania kell minden olyan (valószínűségi vagy permutációs) mechanizmust, amelyet az AVA_SOF.1 garanciális követelmény szerint értékelni lehet.

Az InfoCA nem használ ilyen mechanizmust.

6.3 Garanciális intézkedések

Az alábbiakban áttekintett garanciális intézkedések eleget tesznek a kinyilvánított garanciális követelményeknek (kibővített EAL4).

6.3.1 Konfiguráció kezelés

Az InfoCA rendszer fejlesztése során keletkezett összes konfiguráció elemet figyelemmel kíséri a konfiguráció kezelés rendszer, ezáltal biztosítja az egyes elemek rendelkezésre állását a termék teljes életciklusa alatt. A lefedettség az alábbi tételekre terjed ki:

- megvalósított termék
- a termék forráskódja;
- tervezési dokumentációk;
- teszt dokumentáció és teszt szoftver;
- útmutató dokumentációk;
- fejlesztő környezetre vonatkozó dokumentációk;
- (feltárt és javított) biztonsági hibák.

Az InfoCA rendszer fejlesztése során biztosítva volt, hogy csak engedélyezett módosítások történhessenek a fejlesztés alatt álló szoftveren. Az InfoCA rendszerhez (mint termékhez, minden moduljához átfogóan) verziószámot rendelnek (2.5.buildszám), az értékelés során egyértelműen látható, hogy mely verzió értékelését végzik az értékelők.
A konfiguráció kezelési tervről készült leírás: "A konfiguráció menedzselés dokumentációja-InfoCA hitelesítés-szolgáltatás szoftver v2.5".

6.3.2 Szállítás és üzembehelyezés

A szállítással és üzembehelyezéssel kapcsolatos eljárások leírását a " Telepítési kézikönyv – InfoCA hitelesítés-szolgáltatás szoftver v2.5" című dokumentum tartalmazza.

6.3.3 Fejlesztés

A "Biztonsági szabályzat modell – InfoCA hitelesítés-szolgáltatás szoftver v2.0” című dokumentum leírja az InfoCA rendszer valamennyi modellezhető szabályzatának jellemzőit és szabályait.
A funkcionális specifikáció meghatározza az InfoCA rendszer fő biztonsági funkcióit, a külső interfészeket, ezek használatának célját és módját, teljesen részletezve valamennyi hatást, kivételt és hibaüzenetet. /”InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - Funkcionális specifikáció”/.

A magas szintű terv leírja az InfoCA rendszer fő elemeit (alrendszereit), a közöttük lévő kapcsolatokat. /”InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - Magas szintű terv”/.
Az alacsony szintű terv a InfoCA v2.5 szerkezetét modulok szerint tárgyalja, leírva minden modul célját, a modulok közötti belső kapcsolatokat, a modulokhoz csatlakozó interfészeket./" InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - Alacsony szintű terv"/

Az értékelés vizsgálta a megvalósítási reprezentáció egy részhalmazát is (a biztonság-kritikus forráskódokat).
A "Megfelelés elemzések – InfoCA hitelesítés-szolgáltatás szoftver v2.5" című dokumentum bemutatja, hogy a magasabb szintű informális leírásokban megadott biztonsági funkciókat hogyan valósítják meg az alacsonyabb szinteken, azaz hogyan felel meg egymásnak például a funkcionális specifikáció és a magas szintű terv.

6.3.4 Útmutató dokumentumok

Az InfoCA rendszer különböző felhasználóinak számára készült dokumentumok leírják az InfoCA rendszer biztonságos adminisztrálásának és felhasználásának módját /"Adminisztrátori kézikönyv –InfoCA hitelesítés-szolgáltatás szoftver v2.5", "RA kézikönyv –InfoCA hitelesítés-szolgáltatás szoftver v2.5"/.

6.3.5 Az életciklus támogatása

A tervezés és fejlesztés során az InfoCA rendszer bizalmasságának és sértetlenségének biztosításához a fejlesztői környezetre és a fejlesztők személyére vonatkozó szabályokat alkalmaztak. A fejlesztők a tervek és fejlesztés részleteit a termék teljes élete folyamán csak az arra feljogosított személyekkel beszélhetik meg, a fejlesztési telephelyen csak az arra jogosult személyek férhetnek hozzá a termékkel kapcsolatos programokhoz, dokumentációkhoz.
"A fejlesztési biztonság dokumentációja – InfoCA hitelesítés-szolgáltatás szoftver v2.0" leírja a fejlesztők által az InfoCA rendszer fejlesztése során alkalmazott szabályokat.

Az InfoCA rendszer fejlesztői környezetében a teljes fejlesztési és karbantartási folyamatot ellenőrzés alatt tartják. Az InfoCA rendszer fejlesztéséhez és karbantartáshoz felállított és használt életciklus modell leírását a " Az életciklust meghatározó dokumentáció – InfoCA hitelesítés-szolgáltatás szoftver v2.0" című anyag tartalmazza.

A "ICA v2.5 –A hibajelentési eljárások leírása - InfoCA hitelesítés-szolgáltatás szoftver v2.0" azokat az eljárásokat írja le, melyekkel a fejlesztő nyomon követi a biztonsági hibákat, azonosítja a javítás lépéseit, valamint eljuttatja a javításokkal kapcsolatos információkat a TOE felhasználói felé.
Végül a "A fejlesztő eszközök dokumentációja – InfoCA hitelesítés-szolgáltatás szoftver v2.0" című anyag meghatározza az InfoCA rendszer megvalósításához és vizsgálatához használt fejlesztő eszközöket, és ezen eszközök megvalósítástól függő tulajdonságait (opcióit).

6.3.6 Tesztelés

Az InfoCA rendszer teszteléséhez az alábbi, teszteléssel kapcsolatos dokumentumok készültek: "Tesztelési dokumentáció - InfoCA hitelesítés-szolgáltatás szoftver v2.0", " Teszt elemzések - InfoCA hitelesítés-szolgáltatás szoftver v2.5".

6.3.7 Sebezhetőségek felmérése

"Az útmutatók elemzése – InfoCA hitelesítés-szolgáltatás szoftver v2.5" című anyag azt mutatja ki, hogy a különböző útmutató dokumentumok (Telepítési kézikönyv, Adminisztrátori kézikönyv, RA kézikönyv) nem tartalmaznak félrevezető, értelmetlen és ellentmondásos útmutatásokat, valamint, hogy valamennyi üzemmódban tárgyalják a biztonságos eljárásokat.
A "Sebezhetőség elemzés – InfoCA hitelesítés-szolgáltatás szoftver v2.5" című dokumentum az InfoCA rendszer potenciális sebezhetőségeire mutatja ki, hogy az adott sebezhetőség miért nem használható ki az InfoCA rendszer működési környezetében.

7. Védelmi profil megfelelőségi nyilatkozat

A jelen biztonsági előirányzat a CIMC-PP (Certificate Issuing and Management Components Family of Protection Profiles, Version 1.0) védelmi profil számos elemét felhasználta, többek között néhány, a CIMC-PP védelmi profilban definiált, a Common Criteria 2. részében nem található funkcionális biztonsági követelményt is.
Ugyanakkor jelen biztonsági előirányzat védelmi profilnak való megfelelést nem állít (így a CIMC-PP-nek való megfelelést sem).

8. Indoklások

Ez a rész a TOE-re vonatkozó funkcionális és garanciális követelményeket indokolja, a biztonsági célokon, veszélyeken, feltételeken és biztonsági szabályzatokon alapulva.

8.1 A biztonsági célok indoklása

8.1.1 A biztonsági célok szükségessége

Az alábbi táblázatok kimutatják, hogy minden biztonsági célra szükség van: minden biztonsági cél legalább egy veszélyt, biztonsági szabályzatot vagy feltételezést lefed, egyúttal minden veszély, biztonsági szabályzat és feltételezés legalább egy biztonsági céllal le van fedve.

8-1. táblázat: A TOE-ra vonatkozó biztonsági célok és a veszélyek közötti kapcsolat

IT biztonsági cél	Veszély
O.Certificates	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions

8-2. táblázat: A környezetre vonatkozó biztonsági célok és a veszélyek közötti kapcsolat

Biztonsági cél	Veszély
OE.Administrators, Operators, Officers and Auditors guidance documentation	T.Disclosure of private and secret keys T.Administrators, Operators, Officers and Auditors commit errors or hostile actions T.Social engineering
OE.Competent Administrators, Operators, Officers and Auditors	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
OE.Cryptographic functions	T.Disclosure of private and secret keys T.Modification of private/secret keys
OE.CPS	T.Administrative errors of omission
OE.Installation	T.Critical system component fails
OE.Lifecycle security	T.Critical system component fails T.Malicious code exploitation
OE.Notify Authorities of Security Issues	T.Hacker gains access
OE.Periodically check integrity	T.Malicious code exploitation
OE.Physical Protection	T.Hacker physical access
OE.Preservation/trusted recovery of secure state	T.Critical system component fails
OE.Repair identified security flaws	T.Flawed code T.Critical system component fails
OE.Social Engineering Training	T.Social engineering
OE.Sufficient backup storage and effective restoration	T.Critical system component fails T.User error makes data inaccessible
OE.Validation of security function	T.Malicious code exploitation T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
OE.Trusted Path	T.Hacker gains access T.Message content modification

8-3. táblázat: A környezetre és a TOE-ra egyaránt vonatkozó biztonsági célok és a veszélyek közötti kapcsolat

Biztonsági cél	Veszély
O(E).Configuration Management	T.Critical system component fails T.Malicious code exploitation
O(E).Data import/export	T.Message content modification
O(E).Detect modifications of firmware, software, and backup data	T.User error makes data inaccessible T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O(E).Individual accountability and audit records	T.Administrative errors of omission T.Hacker gains access T.Administrators, Operators, Officers and Auditors commit errors or hostile actions T.User abuses authorization to collect and/or send data
O(E).Integrity protection of user data and software	T.Modification of private/secret keys T.Malicious code exploitation
O(E).Limitation of administrative access	T.Disclosure of private and secret keys T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O(E).Maintain user attributes	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O(E).Manage behavior of security functions	T.Critical system component fails T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O(E).Object and data recovery free from malicious code	T.Modification of private/secret keys T.Malicious code exploitation
O(E).Procedures for preventing malicious code	T.Malicious code exploitation T.Social engineering
O(E).Protect stored audit records	T.Modification of private/secret keys T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O(E).Protect user and TSF data during internal transfer	T.Message content modification T.Disclosure of private and secret keys
O(E).React to detected attacks	T.Hacker gains access
O(E).Require inspection for downloads	T.Malicious code exploitation
O(E).Respond to possible loss of stored audit records	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O(E).Restrict actions before authentication	T.Hacker gains access T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O(E).Security-relevant configuration management	T.Administrative errors of omission
O(E).Security roles	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O(E).Time stamps	T.Critical system component fails T.Administrators, Operators, Officers and Auditors commit errors or hostile actions

8-4. táblázat: A biztonsági szabályzatok és a biztonsági célok közötti kapcsolat

Biztonsági szabályzat	Biztonsági cél
P.Authorized use of information	OE.Auditors Review Audit Logs O(E).Maintain user attributes O(E).Restrict actions before authentication O(E).Security roles O(E).User authorization management
P.Cryptography	OE.Cryptographic functions
P.Archiving	OE.Archiving
P.TimeStampToken	O.TimeStampToken

8-5. táblázat: A feltételek és a biztonsági célok közötti kapcsolat

Feltételek	IT biztonsági cél
A.Auditors Review Audit Logs	OE.Auditors Review Audit Logs
A.Authentication Data Management	OE.Authentication Data Management
A.Communication Protection	OE.Communication Protection
A.Competent Administrators, Operators, Officers and Auditors	OE.Competent Administrators, Operators, Officers and Auditors OE.Installation O(E).Security-relevant configuration management O(E).User authorization management O(E).Configuration Management
A.Cooperative Users	OE.Cooperative Users
A.CPS	OE.CPS O(E).Security-relevant configuration management O(E).User authorization management O(E).Configuration Management
A.Disposal of Authentication Data	OE.Disposal of Authentication Data
A.Malicious Code Not Signed	O(E).Procedures for preventing malicious code O(E).Require inspection for downloads OE.Malicious Code Not Signed
A.Notify Authorities of Security Issues	OE.Notify Authorities of Security Issues
A.Operating System	OE.Operating System
A.Physical Protection	OE.Physical Protection
A.Social Engineering Training	OE.Social Engineering Training

8.1.2 A biztonsági célok elégségessége

Az alábbiakban kimutatjuk az alábbiakat:

- az azonosított biztonsági célok hatékony ellenintézkedéseket valósítanak meg a veszélyekkel szemben (8.1.2.1),
- az azonosított biztonsági célok teljesen lefedik (érvényre juttatják) valamennyi biztonsági szabályzatot (8.1.2.2),
- az azonosított biztonsági célok betartják az összes feltételezést (8.1.2.3).

8.1.2.1 A biztonsági célok elégségessége a veszélyek kivédésére

Jogosult felhasználók

T.Administrative errors of omission azokat a hibákat fogalmazza meg, amelyek közvetlenül kompromittálják a szervezet biztonsági céljait, vagy módosítják a rendszer által érvényre juttatott műszaki biztonsági szabályzatokat. Ezt a veszélyt az alábbiak védik ki:

OE.CPS biztosítja, hogy minden rendszeradminisztrátor, rendszerüzemeltető, tisztviselő és rendszervizsgáló jól ismerje azt a hitelesítési rendet (CP) és szolgáltatási szabályzatot (CPS), mely alatt a TOE-t működtetik. Ezáltal a rendszer feljogosított (privilegizált) felhasználói tisztában vannak felelősségükkel, s ez csökkenti annak valószínűségét, hogy hibásan hajtanak végre egy biztonsági szempontból kritikus funkciót.

O(E).Individual accountability and audit records biztosítja az egyéni felelősségre vonhatóságot, a naplózott események *(biztonsági szempontból releváns részének)* vonatkozásában. *(Az anoním módon igénybe vehető szolgáltatásokon kívül)* minden felhasználó egyedileg azonosított, s így a naplóesemények visszavezethetők egy felhasználóhoz. A naplóesemények egy erre feljogosított személynek információt szolgáltatnak a felhasználók múltbeli viselkedésére nézve. A naplóesemények rögzítése visszatartja a rendszer feljogosított (privilegizált) felhasználóit attól, hogy elmulasszanak végrehajtani egy biztonsági szempontból kritikus funkciót, hiszen ezért utólag felelősségre vonhatók lesznek.

O(E).Security-relevant configuration management garantálja, hogy a rendszer biztonsági szabályzatok adatait és érvényre juttató funkcióit, valamint a biztonság-kritikus konfigurációs adatokat kezelik és frissítik. Ez biztosítja, hogy ezek konzisztensek lesznek a szervezeti biztonsági szabályzatokkal, s minden változtatás megfelelően nyomon követhető és megvalósítható legyen.

T.Administrators, Operators, Officers and Auditors commit errors or hostile actions az alábbiakra irányul:

- a privilegizált felhasználók által elkövetett olyan véletlen hibák, amelyek közvetlenül kompromittálják a szervezet biztonsági céljait, vagy megváltoztatják a rendszer által érvényre juttatandó biztonsági szabályzatot, vagy
- a rendszer konfigurációjának rosszindulatú módosítása a privilegizált felhasználók által, amely lehetővé teszi a biztonság megsértését.

Ezt a veszélyt az alábbiak védik ki:

OE.Competent Administrators, Operators, Officers and Auditors biztosítja, hogy a privilegizált felhasználók képesek a TOE megfelelő kezelésére. Ez csökkenti annak valószínűségét, hogy hibát követnek el.

OE.Administrators, Operators, Officers and Auditors guidance documentation meggátolja a privilegizált felhasználók hibáit, megfelelő dokumentáció biztosításával.

O.Certificates biztosítja, hogy a tanúsítványok, tanúsítvány visszavonási listák és tanúsítvány állapot információk érvényesek. A tisztviselők által szolgáltatott, tanúsítványokba foglalandó információk érvényesítése segíti annak megakadályozását, hogy a tanúsítványokba helytelen információ kerüljön.

O(E).Detect modifications of firmware, software, and backup data biztosítja, hogy a mentett összetevők esetleges módosulása észlelhető.

O(E).Individual accountability and audit records biztosítja az egyéni felelősségre vonhatóságot, a naplózott események *(biztonsági szempontból releváns részének)* vonatkozásában. *(Az anoním módon igénybe vehető szolgáltatásokon kívül)* minden felhasználó egyedileg azonosított, s így a naplóesemények visszavezethetők egy felhasználóhoz. A naplóesemények egy erre feljogosított személynek információt szolgáltatnak a felhasználók múltbeli viselkedésére. A naplóesemények visszatartják a rendszer feljogosított (privilegizált) felhasználóit attól, hogy hibásan hajtanak végre egy biztonsági szempontból kritikus funkciót, hiszen ezért utólag felelősségre vonhatók lesznek.

O(E).Limitation of administrative access az adminisztratív funkciókat úgy tervezték, hogy a privilegizált felhasználók automatikusan ne rendelkezzenek hozzáféréssel a felhasználói objektumokhoz, a szükséges kivételeken kívül. A privilegizált felhasználók által végrehajtható műveletek korlátozása egyben csökkenti az okozható károkat is.

O(E).Maintain user attributes kezeli az egyéni felhasználókkal kapcsolatos (az adott felhasználó azonosítójához rendelt) biztonsági tulajdonság együttest (amely tartalmazhat szerepkörhöz tartozást, hozzáférési privilégiumokat stb.). Ez megakadályozza, hogy a felhasználók olyan műveletet hajtsanak végre, melyekre nincs jogosultságuk.

O(E).Manage behavior of security functions menedzsment funkciókat biztosít a biztonsági mechanizmusok konfigurálására. Ez garantálja, hogy a rosszindulatú felhasználók ellen védelmet biztosító biztonsági mechanizmusokat helyesen konfigurálják.

O(E).Protect stored audit records biztosítja, hogy a naplórekordokat védik a jogosulatlan hozzáféréssel, módosítással vagy törléssel szemben a felhasználói tevékenységekért való felelősségre vonhatóság érdekében.

O(E).Respond to possible loss of stored audit records biztosítja, hogy amennyiben a napló eseménysor tároló területe megtelt vagy majdnem megtelt, csak a rendszervizsgáló által végrehajtott (naplózandó) eseményekre kerülhessen sor. Ez garantálja, hogy az egyéb felhasználók nem hajthatnak olyan műveletet végre, melynek nincs biztosítva a naplózása, s ezen keresztül a nyomon követhetősége.

O(E).Restrict actions before authentication biztosítja, hogy csak korlátozott körű tevékenységek hajthatók végre a felhasználók hitelesítése előtt.

O(E).Security roles biztosítja, hogy biztonsági szerepköröket határoznak meg, s a felhasználókat egy vagy több ilyen szerepkörhöz rendelik. Ez megakadályozza, hogy a felhasználók olyan műveletet hajtsanak végre, melyekre nincs jogosultságuk.

O(E).Time stamps pontos időpontot biztosít az események sorrendjének ellenőrizhetőségéhez. Ez a napló átvizsgálása során lehetővé teszi az események egymásutániságának rekonstruálását.

OE.Validation of security function biztosítja, hogy a biztonság-kritikus szoftver, hardver és förmver elemek helyesen működnek (olyan funkciókon és eljárásokon

keresztül, melyek az alapul szolgáló gép tesztelésére, integritás ellenőrzésekre irányulnak).

T.User abuses authorization to collect and/or send data arra az esetre vonatkozik, amikor egy felhasználó visszaélve jogosultságaival fájlokat vizsgál át abból a célból, hogy összegyűjtsön és/vagy jogosulatlan fogadónak elküldjön érzékeny vagy biztonság-kritikus adatokat. Ezt a veszélyt az alábbiak védik ki:

> **O(E).Individual accountability and audit records** biztosítja az egyéni felelősségre vonhatóságot, a naplózott események *(biztonsági szempontból releváns részének)* vonatkozásában. *(Az anoním módon igénybe vehető szolgáltatásokon kívül)* minden felhasználó egyedileg azonosított, s így a naplóesemények visszavezethetők egy felhasználóhoz. A naplóesemények egy erre feljogosított személynek információt szolgáltatnak a felhasználók múltbeli viselkedésére. A naplóesemények visszatartják a felhasználókat attól, hogy jogosultságaikkal visszaélve adatokat gyűjtsenek és/vagy küldjenek, hiszen ezért utólag felelősségre vonhatók lesznek.

T.User error makes data inaccessible arra irányul, amikor egy felhasználó véletlenül felhasználói adatokat töröl. Következményként a felhasználói adatok hozzáférhetetlenné válnak. Példák erre az alábbiak:

- egy felhasználó véletlenül adatot töröl, rossz billentyű gomb leütéssel, vagy az enter gomb automatikus válaszként történő leütésével,
- egy felhasználó nem érti meg a számára felkínált választás következményeit, s véletlenül olyan választ ad, mely felhasználói adat törléséhez vezet,
- egy felhasználó félreértve egy rendszer parancsot, kiadásával véletlenül felhasználói adatot töröl.

Ezt a veszélyt az alábbiak védik ki:

> **OE.Sufficient backup storage and effective restoration** elegendő mentés tárolást és hatékony visszaállítást biztosít a rendszer újra felépíthetőségére, szükség esetén. Ez biztosítja, hogy a felhasználói adatok elérhetők a mentésből, amennyiben az aktuális példányt véletlenül törölték.
>
> **O(E).Detect modifications of firmware, software, and backup data** biztosítja, hogy amennyiben a mentett összetevőket módosították, ez észlelhető. Ha a mentett összetevők módosítása nem észlelhető, a mentési példány nem tekinthető a felhasználói adatok megbízható visszaállítási forrásának.

<u>Rendszer</u>

T.Critical system component fails egy vagy több rendszer komponens hibájára irányul, mely a rendszer kritikus fontosságú funkcionalitásának elvesztését eredményezi. Ez a veszély akkor lényeges, ha hardver és/vagy szoftver tökéletlenségből adódóan rendszer komponensek hibásodhatnak meg, s a rendszer funkcionális rendelkezésre állása fontos (mint jelen esetben). Ezt a veszélyt az alábbiak védik ki:

> **O(E).Configuration Management** biztosítja, hogy egy konfiguráció kezelési terv kerül megvalósításra. Ez magába foglalja a konfiguráció azonosítását és a változások ellenőrzését, valamint garantálja, hogy helytelen konfigurálás miatt nem következik be kritikus rendszer komponens hiba.
>
> **OE.Installation** biztosítja, hogy a TOE-t olyan módon szállítják, telepítik, kezelik és üzemeltetik, amely megőrzi az informatikai biztonságot. Ez garantálja, hogy helytelen telepítés miatt nem következik be kritikus rendszer komponens hiba.

O(E).Manage behavior of security functions menedzsment funkciókat biztosít a biztonsági mechanizmusok konfigurálására. Ez garantálja, hogy a biztonsági mechanizmusok helytelen konfigurálása miatt nem következik be kritikus rendszer komponens hiba.

OE.Preservation/trusted recovery of secure state biztosítja, hogy a rendszer egy biztonságos állapotban marad, még akkor is, ha működése során hiba lépett fel, s ezért a rendszert helyre kellett állítani. Ez a cél azért lényeges, mert ha a rendszerhibák nem biztonságos állapotot eredményeznének, akkor a működésre helyreállított (vagy a hiba ellenére tovább működő) rendszer megsérthetné a biztonságot.

OE.Sufficient backup storage and effective restoration elegendő mentés tárolást és hatékony visszaállítást biztosít a rendszer újra felépíthetőségére, szükség esetén. Ez biztosítja, hogy az adatok elérhetők a mentésből, amennyiben az aktuális példány elveszett egy rendszer komponens hibája miatt.

O(E).Time stamps pontos időpontot biztosít az események sorrendjének ellenőrizhetőségéhez. Amennyiben a rendszert helyre kell állítani, szükség lehet különböző tranzakciók sorrendjének a meghatározására, hogy a rendszert a hiba bekövetkezésekor érvényes állapottal konzisztens állapotba lehessen visszaállítani.

OE.Lifecycle security a fejlesztési fázisban használt olyan eszközöket és technikákat biztosít, melyek csökkentik a hardver vagy szoftver hibák valószínűségét. Ez a biztonsági cél a működtetés során észlelt olyan hibák kijavítására is irányul, melyek kritikus rendszer komponensek meghibásodásához vezethetnek.

OE.Repair identified security flaws biztosítja, hogy a gyártó kijavítja a felhasználók által azonosított biztonsági hibákat. Az ilyen hibák (ha nem javítanák ki ezeket) kritikus rendszer komponensek meghibásodásához vezethetnek.

T.Flawed code a fejlesztő által a kódolás során elkövetett hibákra irányul. A véletlen hibákra példa a technikai részletek hiánya, vagy a rossz tervezés. Ezt a veszélyt az alábbiak védik ki:

OE.Repair identified security flaws biztosítja, hogy a feltárt biztonsági hibákat kijavítják.

T.Malicious code exploitation arra a fenyegetésre irányul, amikor egy jogosult felhasználó, informatikai rendszer vagy támadó olyan rosszindulatú kódot tölt le és hajt végre, amely rendellenes eljárásokat okoz, s ezzel megsérti a rendszer értékeinek sértetlenségét, rendelkezésre állását vagy bizalmasságát. A rosszindulatú kód végrehajtását egy ezt kiváltó esemény idézi elő. Ezt a veszélyt az alábbiak védik ki:

O(E).Configuration Management biztosítja, hogy egy konfiguráció kezelési terv kerül megvalósításra. Ez a terv magába foglalja a konfiguráció azonosítását és a változások ellenőrzését, valamint garantálja, hogy rosszindulatú kód nem jut a rendszerbe a konfigurálási folyamat során.

O(E).Integrity protection of user data and software megfelelő sértetlenség védelmet biztosít a felhasználói adatokra és a szoftverre. Ez megakadályozza, hogy a rosszindulatú kód hozzákapcsolódjon a felhasználói adatokhoz vagy szoftverekhez.

O(E).Object and data recovery free from malicious code biztosítja, hogy a rendszer egy működőképes állapotba tud visszaállni egy rosszindulatú kód bejutása és károkozása után. A rosszindulatú programkód (pl. vírus vagy féreg) eltávolítása része a visszaállítási folyamatnak.

OE.Periodically check integrity biztosítja mind a rendszer, mind a szoftver sértetlenségének időszakos ellenőrzését. Ha ezek az ellenőrzések hibát találnak, rosszindulatú kód juthatott be a rendszerbe.

O(E).Procedures for preventing malicious code eljárásokat és mechanizmusokat biztosít a rosszindulatú programkódok rendszerbe épülésének a megakadályozására.

O(E).Require inspection for downloads biztosítja, hogy a letöltött/leszállított szoftvereket megvizsgálják, mielőtt használatba vennék.

OE.Validation of security function biztosítja, hogy a biztonság-kritikus szoftver, hardver és förmver elemek helyesen működnek (olyan funkciókon és eljárásokon keresztül, melyek az alapul szolgáló gép tesztelésére, integritás ellenőrzésekre irányulnak).

OE.Lifecycle security a fejlesztési fázisban használt olyan eszközöket és technikákat biztosít, melyek csökkentik annak valószínűségét, hogy a fejlesztő rosszindulatú programkódot épít a termékbe. Ez a biztonsági cél a működtetés során észlelt olyan hibák kijavítására is irányul, mint a komponensek módosítása rosszindulatú programkódokkal.

T.Message content modification arra az esetre irányul, amikor egy támadó információt módosít, amelyet két gyanútlan entitás közötti kommunikációs kapcsolatból fog el, mielőtt azt a tervezett címzetthez továbbítaná. A módosításnak számos lehetséges módja van: egyetlen üzenet módosítása, kiválasztott üzenetek törlése vagy átrendezése, hamis üzenetek beillesztése, korábbi üzenetek visszajátszása, az üzenetekhez kapcsolódó biztonsági tulajdonságok módosítása. Ezt a veszélyt az alábbiak védik ki:

O(E).Data import/export az adatok formájában megjelenő értékeket védi a TOE felé vagy a TOE-tól történő átvitel közben. A továbbított adatok védelme lehetővé teszi a TOE vagy egy külső felhasználó számára a módosított, visszajátszott vagy hamis üzenetek észlelését.

O(E).Protect user and TSF data during internal transfer a rendszeren belül átvitt adatokat védi. A továbbított adatok védelme lehetővé teszi a TOE számára a módosított, visszajátszott vagy hamis üzenetek észlelését.

OE.Trusted Path egy megbízható útvonalat biztosít a felhasználó és a rendszer között. A megbízható útvonal megvédi az üzeneteket a támadók elfogása és módosítása ellen.

Kriptográfia

T.Disclosure of private and secret keys a magán vagy titkos kulcsok jogosulatlan felfedésére irányul. Ezt a veszélyt az alábbiak védik ki:

OE.Administrators, Operators, Officers and Auditors guidance documentation megfelelő dokumentációt biztosít a rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók számára a TOE biztonságos konfigurálásához és üzemeltetéséhez. Ezen dokumentáció megléte és a nevezett szerepkörökbe tartozó személyek rendelkezésére bocsátása minimalizálja az ezen felhasználók által elkövetett hibákat.

OE.Cryptographic functions biztosítja, hogy a TOE jóváhagyott kriptográfiai algoritmusokat valósít meg a titkosításra/dekódolásra, hitelesítésre és aláírás létrehozására/ellenőrzésére, jóváhagyott kulcsgenerálási technikákat alkalmaz, valamint tanúsított kriptográfiai modulokat használ. A tanúsított kriptográfiai modulok használata garantálja, hogy a kriptográfiai kulcsokat megfelelően védik a modulokban való tárolás során.

O(E).Limitation of administrative access biztosítja, hogy az adminisztratív funkciókat úgy tervezték, hogy a rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók automatikusan ne rendelkezzenek hozzáféréssel a felhasználói objektumokhoz, a szükséges kivételeken kívül. A kriptográfiai kulcsokhoz hozzáférő felhasználók számának korlátozása csökkenti a jogosulatlan felfedés valószínűségét.

O(E).Protect user and TSF data during internal transfer a rendszer különböző részei között átvitt titkos és magánkulcsokat védi a jogosulatlan felfedéssel szemben.

T.Modification of private/secret keys a magán és/vagy titkos kulcsok jogosulatlan módosítására irányul. Ezt a veszélyt az alábbiak védik ki:

OE.Cryptographic functions biztosítja, hogy a TOE jóváhagyott kriptográfiai algoritmusokat valósít meg a titkosításra/dekódolásra, hitelesítésre és aláírás létrehozására/ellenőrzésére, jóváhagyott kulcsgenerálási technikákat alkalmaz, valamint tanúsított kriptográfiai modulokat használ. A tanúsított kriptográfiai modulok használata garantálja, hogy a kriptográfiai kulcsokat megfelelően védik a modulokban való tárolás során.

O(E).Integrity protection of user data and software megfelelő sértetlenség védelmet biztosít a magán és titkos kulcsok számára.

O(E).Object and data recovery free from malicious code biztosítja, hogy a rendszer egy működőképes állapotba tud visszaállni egy rosszindulatú kód bejutása és károkozása után. Ha a rosszindulatú programkód jogosulatlanul magán vagy titkos kulcsokat módosít, ez a biztonsági cél garantálja, hogy azok helyes értéke visszaállítható.

O(E).Protect stored audit records biztosítja, hogy a naplórekordokat védik a jogosulatlan hozzáféréssel, módosítással vagy törléssel szemben a felhasználói tevékenységekért való felelősségre vonhatóság érdekében. Ez a biztonsági cél biztosítja, hogy a magán és titkos kulcsok módosítása a naplórekordokból észlelhető lesz.

Külső támadások

T.Hacker gains access az alábbiakra irányul:

- gyenge rendszer hozzáférés ellenőrzési mechanizmusok vagy felhasználói tulajdonságok,
- gyengén megvalósított rendszer hozzáférés ellenőrzés,
- a rendszer kódjában talált sebezhetőségek, melyek segítségével egy támadó észrevétlenül betörhet a rendszerbe.

Ezt a veszélyt az alábbiak védik ki:

O(E).Restrict actions before authentication biztosítja, hogy csak korlátozott körű tevékenységek hajthatók végre a felhasználók hitelesítése előtt. Ez megakadályozza a hozzáférés ellenőrzési mechanizmusok megkerülésére képtelen támadót abban, hogy biztonság-kritikus tevékenységeket hajtson végre.

O(E).Individual accountability and audit records biztosítja az egyéni felelősségre vonhatóságot, a naplózott események *(biztonsági szempontból releváns részének)* vonatkozásában. *(Az anonim módon igénybe vehető szolgáltatásokon kívül)* minden felhasználó egyedileg azonosított, s így a naplóesemények visszavezethetők egy felhasználóhoz. A naplóesemények egy erre feljogosított személynek információt szolgáltatnak a felhasználók múltbeli viselkedéséről. Ez lehetővé teszi a jogosulatlan tevékenységek észlelését. A már észlelt tevékenységekből származó kár megszüntethető vagy csökkenthető.

OE.Notify Authorities of Security Issues biztosítja, hogy a megfelelő vezetőket értesítik a rendszert érintő bármely biztonsági ügyről. Ez minimalizálja az adatvesztés vagy kompromittálódás lehetőségét.

O(E).React to detected attacks automatizált értesítést vagy más reagálásokat biztosít a TSF által felfedett támadások esetében, a támadások azonosítása és elrettentése érdekében. Ez a cél különösen akkor fontos, ha a szervezet által lényegesnek tartott válaszintézkedések is kihasználható támadáshoz vezethetnek.

OE.Trusted Path egy megbízható útvonalat biztosít a felhasználó és a rendszer között. A megbízható útvonalat a hitelesítő adatok megvédésére használják, s ez csökkenti annak a valószínűségét, hogy egy támadó jogosult felhasználónak álcázza magát.

T.Hacker physical access arra a veszélyre irányul, amikor egy támadó a fizikai környezetben meglévő sebezhetőségeket aknázza ki a rendszer komponensek fizikai ellenőrzésének megszerzése érdekében.. Ezt a veszélyt az alábbiak védik ki:

OE.Physical Protection biztosítja, hogy a fizikai hozzáférés ellenőrzés elegendő a rendszer komponensek fizikai támadásával szemben.

T.Social engineering arra az esetre irányul, amikor egy támadó a "social engineering" technikát alkalmazza arra, hogy információt szerezzen a rendszerbe lépésről, a rendszer felhasználásáról, a rendszer tervéről vagy a rendszer működéséről. Ezt a veszélyt az alábbiak védik ki:

OE.Administrators, Operators, Officers and Auditors guidance documentation megakadályozza az adminisztratív személyzet által elkövetett hibákat, megfelelő dokumentáció biztosításával.

O(E).Procedures for preventing malicious code eljárásokat és mechanizmusokat biztosít a rosszindulatú programkódok rendszerbe épülésének a megakadályozására. A rosszindulatú programkódok rendszerbe építése lehet az egyik célja a "social engineering" típusú támadásoknak.

OE.Social Engineering Training biztosítja, hogy az általános felhasználók, a rendszeradminisztrátorok, a rendszerüzemeltetők, a tisztviselők és a rendszervizsgálók képzést kaptak a "social engineering" típusú támadások megakadályozási technikáira.

8.1.2.2 A biztonsági célok elégségessége a biztonsági szabályzatok érvényre juttatására

P.Authorized use of information megállapítja, hogy információ csak az engedélyezett cél(ok)ra használható fel. Erre az alábbi biztonsági célok irányulnak: **O(E).Maintain user attributes, O(E).Restrict actions before authentication, O(E).Security roles** és **O(E).User authorization management** biztosítja, hogy a biztonság-kritikus tevékenységek végrehajtásának képessége az erre feljogosított személyekre van korlátozva. **O(E).Maintain user attributes, O(E).Security roles** és **O(E).User authorization management** azt biztosítja, hogy a felhasználókat csak azon tevékenységek végrehajtására jogosítják fel, melyekre szükségük van munkájuk során. Végül az **OE.Auditors Review Audit Logs** visszatartja a felhasználókat attól, hogy visszaéljenek jogosultságaikkal.

P.Cryptography megállapítja, hogy jóváhagyott kriptográfiai szabványokat és műveleteket kell alkalmazni a TOE és informatikai környezete tervezése során. Erre irányul az **OE.Cryptographic functions**, mely biztosítja, hogy csak szabványokon alapuló megoldásokat használnak.

P.Archiving megállapítja, hogy a CWA 14167-1 archiválásra vonatkozó mindhárom elvárását /AR1 (archív adatok generálása), AR2 (Szelektálható keresés) és AR3 (Az archivált adatok sértetlensége)/ biztosítani kell. Erre az **OE.Archiving** környezeti biztonsági cél irányul.

P.TimeStampToken előírja az RFC 3161 szabványnak megfelelő időbélyeg kérésekre adott időbélyeg válaszok RFC 3161-nek megfelelő érvényességét. Erre a szervezeti szabályra az **O.TimeStampToken** biztonsági cél irányul.

8.1.2.3 A biztonsági célok elégségessége a feltételek betartására

Személyi feltételek

A.Auditors Review Audit Logs megállapítja, hogy a biztonság-kritikus eseményekről naplóbejegyzés szükséges, s ezeket a rendszervizsgálónak át kell vizsgálnia. Erre irányul az **OE.Auditors Review Audit Logs**, mely biztosítja, hogy a naplózott biztonság-kritikus eseményeket a rendszervizsgáló átvizsgálja.

A.Authentication Data Management megállapítja, hogy a felhasználói hitelesítési adatok kezelése a TOE-n kívül esik. Erre irányul az **OE.Authentication Data Management**, mely biztosítja, a felhasználók hitelesítési adataikat megfelelő biztonsági szabályzat szerint módosítják.

A.Competent Administrators, Operators, Officers and Auditors megállapítja, hogy a TOE biztonsága a TOE-t menedzselőktől függ. Erre irányulnak az alábbiak: **OE.Competent Administrators, Operators, Officers and Auditors**, mely biztosítja, hogy a rendszert menedzselők szakértők a menedzselésben, **OE.Installation**, mely biztosítja, hogy a TOE biztonságáért felelős személyek biztosítják, hogy a TOE-t a bitonságot fenntartó módon szállítják, telepítik, kezelik és működtetik, **O(E).Security-relevant configuration management**, mely biztosítja, hogy a szervezeti biztonsági szabályzatok összhangban állnak a rendszer biztonsági adatokkal és egyéb biztonság-kritikus konfigurációs adatokkal, az **O(E).Configuration management**, mely biztosítja, hogy a konfigurációs elemek változásait nyomon követik, valamint **O(E).User authorization management** ami azt biztosítja, hogy a felhasználókat csak azon tevékenységek végrehajtására jogosítják fel, melyekre szükségük van munkájuk során.

A.Cooperative Users megállapítja, hogy biztonságos IT környezet szükséges a TOE biztonságos üzemeltetéséhez, s a felhasználóknak a környezet által támasztott korlátozásoknak

megfelelően kell dolgozniuk. Erre irányul az **OE.Cooperative Users**, mely biztosítja, hogy a felhasználók együttműködő módon, a korlátozásoknak megfelelően tevékenykednek.

A.CPS megállapítja, hogy a rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók jól ismerik azt a hitelesítési rendet (CP) és szolgáltatási szabályzatot (CPS), mely alatt a TOE-t működtetik. Erre irányulnak az alábbiak: **OE.CPS**, mely biztosítja, hogy a rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók jól ismerik azt a hitelesítési rendet (CP) és szolgáltatási szabályzatot (CPS), mely alatt a TOE-t működtetik, **O(E).Security-relevant configuration management**, mely biztosítja, hogy a szervezeti biztonsági szabályzatok összhangban állnak a rendszer biztonsági adatokkal és egyéb biztonság-kritikus konfigurációs adatokkal, **O.User authorization management**, mely biztosítja, hogy a felhasználói jogosultságokat meghatározó adatok összhangban állnak a szervezeti biztonsági és személyzeti szabályzattal, valamint az **O(E).Configuration management**, mely biztosítja, hogy a konfigurációs elemek változásait nyomon követik..

A.Disposal of Authentication Data megállapítja, hogy a felhasználóknak nem szabad hozzáférniük a rendszerhez, miután megszűnt az erre vonatkozó jogosultságuk. Erre irányul az **OE.Disposal of Authentication Data**, mely biztosítja, hogy a rendszerhez való hozzáférést visszautasítják, miután a hozzáférési jogosultság megszűnt.

A.Malicious Code Not Signed megállapítja, hogy a nem a TOE számára tervezett kódokat megbízható fél nem írja alá. Erre irányulnak az alábbiak: az **O(E).Procedures_for_preventing_ malicious_code**, mely rosszindulatú kódokat megakadályozó eljárásokat és mechanizmusokat biztosít, **O(E).Require inspection for downloads,** mely biztosítja, hogy a letöltött, továbbított kódok átvizsgálását, valamint az **OE.Malicious Code Not Signed**, mely biztosítja, hogy a TOE számára küldött kódot egy megbízható félnek alá kell írnia, különben nem lehet a rendszerbe tölteni.

A.Notify Authorities of Security Issues megállapítja, hogy a felhasználóknak értesíteniük kell a megfelelő vezetőket a rendszert érintő bármely biztonsági ügyről, a további adatvesztés vagy kompromittálódás lehetőségének minimalizálása érdekében. Erre irányul az **OE.Notify Authorities of Security Issues**, mely biztosítja, hogy a felhasználók értesítik a megfelelő vezetőket a rendszert érintő bármely biztonsági ügyről.

A.Social Engineering Training megállapítja, hogy a rendszerhez való hozzáférés érdekében "social engineering" típusú technikát alkalmazhatnak. Erre irányul az **OE.Social Engineering Training**, mely biztosítja, hogy minden felhasználó képzésben részesül a "social engineering" típusú támadások meghiúsítása érdekében.

Kapcsolódási feltételek

A.Operating System megállapítja, hogy egy nem biztonságos operációs rendszer kompromittálja a rendszer biztonságát. Erre irányul az **OE.Operating System**, mely biztosítja, hogy olyan operációs rendszert használnak, mely megfelel az elvárásoknak.

Fizikai feltételek

A.Communication Protection megállapítja, hogy a kommunikációs infrastruktúra védelme a TOE-n kívül áll. Erre irányul az **OE.Communication Protection**, mely biztosítja a kommunikációs infrastruktúra megfelelő fizikai védelmét.

A.Physical Protection megállapítja, hogy a TOE hardver, szoftver és förmver elemeinek fizikai módosítása kompromittálhatja a rendszer biztonságát. Erre irányul az **O. Physical Protection**, mely biztosítja a TOE hardver, szoftver és förmver elemeinek megfelelő fizikai védelmét.

8.2 A biztonsági követelmények indoklása

Ebben a részben kimutatjuk a biztonsági követelmények szükségességét és elégségességét.

8.2.1 A biztonsági követelmények szükségessége

Ez az alfejezet a biztonsági követelmények szükségességét mutatja ki, demonstrálva, hogy minden biztonsági cél megvalósulását támogatja legalább egy biztonsági követelmény, s hogy minden biztonsági követelmény legalább egy biztonsági cél megvalósulásához hozzájárul.

8-6. táblázat: A TOE-ra vonatkozó funkcionális biztonsági követelmények hozzájárulása a biztonsági célok eléréséhez

funkcionális biztonsági követelmény	biztonsági cél
FAU_GEN.1 Napló adatok generálása	O(E).Individual accountability and audit records
FAU_GEN.2 A felhasználói azonosítóval való összekapcsolás	O(E).Individual accountability and audit records
FDP_ACC.1 Részleges hozzáférés ellenőrzés (iteráció 2)	O(E).Limitation of administrative access
FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés (iteráció 2)	O(E).Limitation of administrative access
FDP_ACF_CIMC.2 A felhasználói magánkulcs bizalmasságának védelme	O.Certificates O(E).Procedures for preventing malicious code
FDP_ACF_CIMC.3 A felhasználói titkos kulcs bizalmasságának védelme	O.Certificates O(E).Procedures for preventing malicious code
FDP_CIMC CER.1 Tanúsítvány előállítás	O.Certificates
FDP_CIMC CRL.1 Tanúsítvány visszavonási lista érvényesítés	O.Certificates
FDP_CIMC CSE.1 Tanúsítvány állapot export	O.Certificates
FDP_CIMC OCSP.1 OCSP alap-válasz érvényesítés	O.Certificates
FDP_CWA_TS.1 Időbélyeg válasz érvényesítés	O.TimeStampToken
FDP_ETC_CIMC.5 Kiterjesztett felhasználói magán és titkos kulcs export	O(E).Data import/export
FDP_ITT.1 A belső adatátvitel alapszintű védelme (iteráció 4)	O(E).Integrity protection of user data and software O(E).Protect user and TSF data during internal transfer
FDP_SDI_CIMC.3 A tárolt nyilvános kulcs sértetlenségének figyelése és reagálás	O(E).Integrity protection of user data and software
FIA_AFL.1 Hitelesítési hibák kezelése (iteráció 2)	O(E).React to detected attacks
FIA_ATD.1 Felhasználói tulajdonságok megadása (iteráció 2)	O(E).Maintain user attributes
FIA_UAU.1 A hitelesítés időzítése (iteráció 2)	O(E).Limitation of administrative access O(E).Restrict actions before authentication
FIA_UID.1 Az azonosítás időzítése (iteráció 2)	O(E).Individual accountability and audit records O(E).Limitation of administrative access
FIA_USB.1 Felhasználó - szubjektum összerendelése (iteráció 2)	O(E).Maintain user attributes
FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése (iteráció 3)	O(E).Configuration Management O(E).Manage behavior of security functions O(E).Security-relevant configuration management
FMT_MOF_CIMC.3 Kiterjesztett tanúsítvány profil menedzsment	O(E).Configuration Management
FMT_MOF_CIMC.5 Kiterjesztett tanúsítvány visszavonási lista profil menedzsment	O(E).Configuration Management

funkcionális biztonsági követelmény	biztonsági cél
FMT_MOF_CIMC.6 OCSP profil menedzsment	O(E).Configuration Management
FMT_MOF_CWA.1 Időbélyeg profil menedzsment	O(E).Configuration Management
FMT_MSA.1 Biztonsági tulajdonságok kezelése (iteráció 2, 3)	O(E).Maintain user attributes O(E).User authorization management
FMT_MSA.2 Biztonságos biztonsági tulajdonságok (iteráció 2)	O(E).Security-relevant configuration management
FMT_MSA.3 Statikus tulajdonságok kezdeti értékadása (iteráció 2)	O(E).Security-relevant configuration management
FMT_SMF.1 Menedzsment funkciók megadása (iteráció 2)	O(E).Manage behavior of security functions
FMT_SMR.2 Megszorítások a biztonsági szerepkörökre (iteráció 2)	O(E).Security roles
FPT_CIMC_TSP.1 Napló lista aláírása	O(E).Protect stored audit records
FPT_ITT.1 A belső adatátvitel alapszintű védelme (iteráció 4)	O(E).Protect user and TSF data during internal transfer
FPT_RVM.1 A TSP megkerülhetetlensége (iteráció 2)	O(E).Limitation of administrative access

8-7. táblázat: Az informatikai környezetrevonatkozó funkcionális biztonsági követelmények hozzájárulása a biztonsági célok eléréséhez

funkcionális biztonsági követelmény	biztonsági cél
FAU_ARP.1 Biztonsági riasztások	O(E).React to detected attacks
FAU_SAA.1 A biztonság potenciális megsértésének vizsgálata	O(E).React to detected attacks
FAU_SAR.1 Napló áttekintés	O(E).Individual accountability and audit records
FAU_SAR.3 Kiválogatható napló áttekintés	O(E).Individual accountability and audit records
FAU_STG.1 A naplóesemények védett tárolása	O(E).Protect stored audit records
FAU_STG.4 A napló adatok elvesztésének meggátolása	O(E).Respond to possible loss of stored audit records
FCS_CKM.1 A kriptográfiai kulcsok generálása	OE.Cryptographic functions
FCS_CKM.4 A kriptográfiai kulcsok megsemmisítése	O(E).Procedures for preventing malicious code O(E).React to detected attacks
FCS_CKM_CIMC.5 A TOE magán és titkos kulcsának nullázása	O(E).Procedures for preventing malicious code O(E).React to detected attacks
FCS_COP.1 Kriptográfiai eljárás	OE.Cryptographic functions
FDP_ACC.1 Részleges hozzáférés ellenőrzés (iteráció 1)	O(E).Limitation of administrative access
FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés (iteráció 1)	O(E).Limitation of administrative access
FDP_CIMC_BKP.1 CIMC mentés és visszaállítás	O(E).Object and data recovery free from malicious code OE.Preservation/trusted recovery of secure state OE.Sufficient backup storage and effective restoration
FDP_CIMC_BKP.2 Kiterjesztett CIMC mentések és visszaállítások	O(E).Detect modifications of firmware, software, and backup data O(E).Object and data recovery free from malicious code
FDP_ITT.1 A belső adatátvitel alapszintű védelme (iteráció 1)	O(E).Integrity protection of user data and software O(E).Protect user and TSF data during internal transfer
FDP_ITT.1 A belső adatátvitel alapszintű védelme (iteráció 2,3)	O(E).Protect user and TSF data during internal transfer
FDP_UCT.1 Alapszintű adatcsere bizalmasság	O(E).Data import/export
FIA_AFL.1 Hitelesítési hibák kezelése (iteráció 1)	O(E).React to detected attacks

funkcionális biztonsági követelmény	biztonsági cél
FIA_ATD.1 Felhasználói tulajdonságok megadása (iteráció 1)	O(E).Maintain user attributes
FIA_UAU.1 A hitelesítés időzítése (iteráció 1)	O(E).Limitation of administrative access O(E).Restrict actions before authentication
FIA_UID.1 Az azonosítás időzítése (iteráció 1)	O(E).Individual accountability and audit records O(E).Limitation of administrative access
FIA_USB.1 Felhasználó - szubjektum összerendelése (iteráció 1)	O(E).Maintain user attributes
FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése (iteráció 1,2)	O(E).Configuration Management O(E).Manage behavior of security functions O(E).Security-relevant configuration management
FMT_MSA.1 Biztonsági tulajdonságok kezelése (iteráció 1)	O(E).Maintain user attributes O(E).User authorization management
FMT_MSA.2 Biztonságos biztonsági tulajdonságok (iteráció 1)	O(E).Security-relevant configuration management
FMT_MSA.3 Statikus tulajdonságok kezdeti értékadása (iteráció 1)	O(E).Security-relevant configuration management
FMT_MTD.1 TSF adatok kezelése (iteráció 1,2)	O(E).Individual accountability and audit records O(E).Protect stored audit records
FMT_MTD_CIMC.4 A TSF magánkulcs bizalmasságának védelme	O(E).Detect modifications of firmware, software, and backup data O(E).Integrity protection of user data and software
FMT_MTD_CIMC.7 Kiterjesztett TSF magán és titkos kulcs export	O(E).Data import/export
FMT_SMF.1 Menedzsment funkciók megadása (iteráció 1)	O(E).Manage behavior of security functions
FMT_SMR.2 Megszorítások a biztonsági szerepkörökre (iteráció 1)	O(E).Security roles
FPT_AMT.1 Az absztrakt gép tesztelése	OE.Periodically check integrity OE.Validation of security function
FPT_ITC.1 A TSF-ek közötti bizalmasság az adatátvitel során	O(E).Data import/export
FPT_ITT.1 A belső adatátvitel alapszintű védelme (iteráció 1,2,3)	O(E).Protect user and TSF data during internal transfer
FPT_RVM.1 A TSP megkerülhetetlensége (iteráció 1)	OE.Operating System
FPT_SEP.1 TSF tartomány szétválasztás	OE.Operating System
FPT_STM.1 Megbízható időbélyegzés	O(E).Individual accountability and audit records O(E).Time stamps
FPT_TST_CIMC.2 Szoftver/förmver sértetlenség teszt	O(E).Detect modifications of firmware, software, and backup data O(E).Integrity protection of user data and software O(E).Object and data recovery free from malicious code OE.Periodically check integrity O(E).Procedures for preventing malicious code OE.Validation of security function
FPT_TST CIMC.3 Szoftver/förmver betöltés teszt	O(E).Integrity protection of user data and software O(E).Object and data recovery free from malicious code OE.Periodically check integrity O(E).Require inspection for downloads
FTP_TRP.1 Megbízható útvonal	OE.Trusted Path

8-8. táblázat: A garanciális biztonsági követelmények hozzájárulása a biztonsági célok eléréséhez

garanciális biztonsági követelmény	biztonsági cél
ACM_AUT.1 Részleges konfiguráció kezelés automatizálás	EAL4 választás O(E).Configuration Management
ACM_CAP.4 A generálás támogatása és elfogadási eljárások	EAL4 választás O(E).Configuration Management
ACM_SCP.2 A biztonsági hibákat követő konfiguráció kezelés	EAL4 választás O(E).Configuration Management
ADO_DEL.2 A módosítás kimutatása	EAL4 választás
ADO_IGS.1 Hardver telepítés, szoftver telepítés, a beindítás eljárásai	EAL4 választás OE.Installation
ADV_FSP.2 Teljesen meghatározott külső interfészek	EAL4 választás OE.Lifecycle security
ADV_HLD.2 Biztonságot érvényre juttató magas szintű tervezés	EAL4 választás OE.Lifecycle security
ADV_IMP.1 A biztonsági funkciók részleges kivitelezési dokumentálása	EAL4 választás OE.Lifecycle security
ADV_LLD.1 Leíró alacsony szintű terv	EAL4 választás OE.Lifecycle security
ADV_RCR.1 A kölcsönös megfelelés informális szemléltetése	EAL4 választás OE.Lifecycle security
ADV_SPM.1 Informális biztonságpolitikai modell	EAL4 választás OE.Lifecycle security
AGD_ADM.1 Adminisztrátori útmutató	OE.Administrators, Operators, Officers and Auditors guidance documentation OE.Auditors Review Audit Logs OE.Competent Administrators, Operators, Officers and Auditors O(E).Configuration Management OE.Installation OE.Malicious Code Not Signed O(E).Procedures for preventing malicious code O(E).Require inspection for downloads O(E).Security-relevant configuration management O(E).User authorization management EAL4 választás
AGD_USR.1 Felhasználói útmutató	OE.Administrators, Operators, Officers and Auditors guidance documentation OE.Competent Administrators, Operators, Officers and Auditors OE.Malicious Code Not Signed O(E).Procedures for preventing malicious code O(E).Require inspection for downloads EAL4 választás
ALC_DVS.1 A biztonsági intézkedések azonosítása	EAL4 választás
ALC_FLR.2 Hibajelentési eljárások	OE.Lifecycle security OE.Repair identified security flaws kibővített EAL4 választás
ALC_LCD.1 A fejlesztő által meghatározott életciklus modell	EAL4 választás
ALC_TAT.1 Jól meghatározott fejlesztői eszközök	EAL4 választás
ATE_COV.2 A teszt lefedettség elemzése	EAL4 választás
ATE_DPT.1 A magas szintű terv tesztelése	EAL4 választás
ATE_FUN.1 Funkcionális tesztelés	EAL4 választás
ATE_IND.2 Független tesztelés - mintán	EAL4 választás

garanciális biztonsági követelmény	biztonsági cél
AVA_MSU.2 A vizsgálatok megerősítése	EAL4 választás
AVA_SOF.1 Az értékelés tárgya biztonsági funkcióinak erősségértékelése	EAL4 választás
AVA_VLA.2 Független sebezhetőség vizsgálat	EAL4 választás

8.2.2 A biztonsági követelmények elégségessége

Ez a rész a biztonsági követelmények elégségességét mutatja ki, demonstrálva, hogy a biztonsági követelmények összességükben minden biztonsági célt maradéktalanul megvalósítanak.

8.2.2.1 A TOE-ra vonatkozó biztonsági célok

O.Certificates teljesülését az alábbiak biztosítják: **FDP_CIMC_CER.1 (Tanúsítvány előállítás)**, amely azt garantálja, hogy a tanúsítvány érvényes, **FDP_CIMC_CRL.1 (Tanúsítvány visszavonási lista érvényesítés), FDP_CIMC_CSE.1 (Tanúsítvány állapot export)** és **FDP_CIMC OCSP.1,** amelyek azt garantálják, hogy a tanúsítvány visszavonási listák és a tanúsítvány állapot információk érvényesek. Abban az esetben, amikor a TOE a végfelhasználói magánkulcs egy másolatát is kezeli **FDP_ACF_CIMC.2 (A felhasználói magánkulcs bizalmasságának védelme)** garantálja, hogy a tanúsítvány nem válik érvénytelenné azáltal, hogy a TOE felfedi a magánkulcsot. Abban az esetben, amikor a tanúsítvány végfelhasználója egy titkos kulcsot használ, egy tanúsítványkérelem hitelesítésére **FDP_ACF_CIMC.3 (A felhasználói titkos kulcs bizalmasságának védelme)** garantálja, hogy egy támadó nem szerezhet meg egy hamis tanúsítványt azáltal, hogy megszerzi a TOE-tól a titkos kulcsot, s ezzel hamis tanúsítványt igényel.

O.TimeStampToken teljesülését az alábbiak biztosítják: **FDP_CWA_TS.1 (Időbélyeg válasz érvényesítés)**, amely azt garantálja, hogy szabványos időbélyeg kérésekre szabványos és érvényes időbélyeg válaszok születnek, **FMT_MOF_CWA.1 (Időbélyeg profil menedzsment)**, amely azt biztosítja, hogy a rendszeradminisztrátorok ellenőrizhessék a TOE által generált időbélyeg válaszokba kerülő információ típusát.

8.2.2.2 A környezetre vonatkozó biztonsági célok

A környezetre vonatkozó nem informatikai biztonsági célok

OE.Administrators, Operators, Officers and Auditors guidance documentation teljesülését biztosítják: **AGD_ADM.1 (Adminisztrátori útmutató)** és **AGD_USR.1 (Felhasználói útmutató)**, melyek megfelelő útmutatókat garantálnak a rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók számára a TOE biztonságos működtetéséhez.

OE.Auditors Review Audit Logs teljesülését biztosítja: **A.Auditors Review Audit Logs,** mely biztosítja, hogy a rendszervizsgáló átvizsgálja a naplóbejegyzéseket. Támogatja még e biztonsági cél teljesülését **AGD_ADM.1 (Adminisztrátori útmutató)** is, mely garantálja, hogy a rendszervizsgálók rendelkezésére állnak a naplóbejegyzések tartalmának megértéséhez szükséges információk.

OE.Authentication Data Management teljesülését biztosítja: **A.Authentication Data Management,** mely arra vonatkozó követelmény (környezetre tett feltételezés), hogy érvényre juttatnak egy szabályzatot a hitelesítési adatok kezelésre.

OE.Communication Protection teljesülését biztosítja: **A.Communication Protection** mely arra vonatkozó követelmény (környezetre tett feltételezés), hogy a rendszert fizikailag megfelelően védik a kommunikáció elvesztése ellen.

OE.Competent Administrators, Operators, Officers and Auditors teljesülését biztosítja: **A.Competent Administrators, Operators, Officers and Auditors,** mely arra vonatkozó követelmény (környezetre tett feltételezés), hogy a rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók képesek a TOE és az általa tartalmazott információk biztonságának kezelésére. Támogatja még e biztonsági cél teljesülését **AGD_ADM.1 (Adminisztrátori útmutató) és AGD_USR.1 (Felhasználói útmutató)** is, melyek garantálják, hogy a rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók rendelkezésére állnak a TOE és a TOE biztonsági funkcióinak kezeléséhez szükséges információk.

OE.Cooperative Users teljesülését biztosítja: **A.Cooperative Users,** mely arra vonatkozó követelmény (környezetre tett feltételezés), hogy a felhasználók együttműködő módon tevékenykednek.

OE.CPS teljesülését biztosítja: **A.CPS,** mely arra vonatkozó követelmény (környezetre tett feltételezés), hogy a rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók jól ismerik azt a hitelesítési rendet (CP) és szolgáltatási szabályzatot (CPS), mely alatt a TOE-t működtetik.

OE.Disposal of Authentication Data teljesülését biztosítja: **A.Disposal of Authentication Data,** mely arra vonatkozó követelmény (környezetre tett feltételezés), hogy a hitelesítési adatokat megfelelő módon eltávolítják a hozzáférési jogosultság megszűnése után.

OE.Installation teljesülését biztosítja: **ADO_IGS.1 (Hardver telepítés, szoftver telepítés, a beindítás eljárásai)** és **AGD_ADM.1 (Adminisztrátori útmutató),** melyek arra vonatkozó követelmények, hogy a rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók számára biztosítva legyenek a TOE biztonságos telepítéséhez és működtetéséhez szükséges eljárásokat leíró dokumentációk. Támogatja még e biztonsági cél teljesülését **A.Competent Administrators, Operators, Officers and Auditors** is, mely arra vonatkozó követelmény (környezetre tett feltételezés), hogy a rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók képesek a TOE biztonságos kezelésére.

OE.Lifecycle security teljesülését az alábbiak biztosítják: **ADV_FSP.2 (Teljesen meghatározott külső interfészek), ADV_HLD.2 (Biztonságot érvényre juttató magas szintű tervezés), ADV_IMP.1 (A biztonsági funkciók részleges kivitelezési dokumentálása), ADV_LLD.1 (Leíró alacsony szintű terv), ADV_RCR.1 (A kölcsönös megfelelés informális szemléltetése), ADV_SPM.1 (Informális biztonságpolitikai modell)**, melyek arra vonatkozó követelmények, hogy a biztonságot tervezzék be a TOE-be. **ALC_FLR.2 (Hibajelentési eljárások)** arra vonatkozó követelmény, hogy a működtetés során észlelt hibákat javítani kell.

OE.Malicious Code Not Signed teljesülését biztosítja: **A.Malicious Code Not Signed,** mely arra vonatkozó követelmény (környezetre tett feltételezés), hogy a TOE-nek címzett rosszindulatú kódokat nem írja alá egy megbízható entitás. Támogatja még e biztonsági cél teljesülését **AGD_ADM.1 (Adminisztrátori útmutató)** és **AGD_USR.1 (Felhasználói útmutató)** is, melyek garantálják, hogy azok az entitások, melyeket megbízhatónak tekintenek a kódok aláírására, tisztában vannak felelősségükkel.

OE.Notify Authorities of Security Issues teljesülését biztosítja: **A.Notify Authorities of Security Issues,** mely arra vonatkozó követelmény (környezetre tett feltételezés), hogy a megfelelő vezetőket értesítik a rendszerüket érintő bármely biztonsági ügyről.

OE.Physical Protection teljesülését biztosítja: **A.Physical Protection,** mely arra vonatkozó követelmény (környezetre tett feltételezés), hogy a TOE biztonság-kritikus hardver, szoftver és förmver elemei védve legyenek a jogosulatlan fizikai módosítással szemben.

OE.Repair identified security flaws teljesülését biztosítja: **ALC_FLR.2 (Hibajelentési eljárások),** mely arra vonatkozó követelmény, hogy a gyártó kijavítja a felhasználók által azonosított hibákat.

OE.Social Engineering Training teljesülését biztosítja: **A.Social Engineering Training,** mely arra vonatkozó követelmény (környezetre tett feltételezés), hogy az általános felhasználók, a rendszeradminisztrátorok, a rendszerüzemeltetők, a tisztviselők és a rendszervizsgálók képzést kapnak a "social engineering" típusú támadások megakadályozási technikáira.

A környezetre vonatkozó informatikai biztonsági célok

OE.Cryptographic functions teljesülését biztosítja: **FCS_CKM.1 (A kriptográfiai kulcsok generálása)** és **FCS_COP.1 (Kriptográfiai eljárás),** melyek arra vonatkozó követelmények, hogy jóváhagyott kriptográfiai algoritmusokat kell megvalósítani a titkosításra/dekódolásra, hitelesítésre és aláírás létrehozására/ellenőrzésére, valamint jóváhagyott kulcsgenerálási technikákat kell alkalmazni.

OE.Operating System teljesülését biztosítja: **A.Operating System,** mely arra vonatkozó követelmény (környezetre tett feltételezés), hogy a TOE-nak futási környezetet biztosító operációs rendszer(ek)nek megfelelő biztonsági funkciókat kell biztosítaniuk a TOE számára a felismert veszélyek elhárítására. Támogatja még e biztonsági cél teljesülését **FPT_RVM.1 (A TSP megkerülhetetlensége, iteráció 1)** és **FPT_SEP.1 (TSF tartomány szétválasztás)** is, melyek elvárják, hogy a TOE-nak futási környezetet biztosító operációs rendszer(ek) biztosítsák a tartomány szétválasztást és a biztonsági funkciók megkerülhetetlenségét.

OE.Periodically check integrity teljesülését az alábbiak biztosítják: **FPT_AMT.1 (Az absztrakt gép tesztelése),** mely megköveteli a rendszer időszakos sértetlenség ellenőrzését, **FPT_TST_CIMC.2 (Szoftver/förmver sértetlenség teszt)** és **FPT_TST_CIMC.3 (Szoftver/förmver betöltés teszt)** melyek a szoftver sértetlenségének időszakos ellenőrzését követeli meg.

OE.Preservation/trusted recovery of secure state teljesülését biztosítja: **FDP_CIMC_BKP.1 (CIMC mentés és visszaállítás),** mely arra vonatkozó követelmény, hogy úgy kell megőrzi a rendszer állapotát, hogy egy biztonsági komponens hibája esetén az helyreállítható legyen.

OE.Sufficient backup storage and effective restoration teljesülését biztosítja: **FDP_CIMC_BKP.1 (CIMC mentés és visszaállítás),** mely arra vonatkozó követelmény, hogy elegendő mentési adat keletkezzen és tárolódjon, valamint egy hatékony visszaállítási eljárás legyen biztosítva.

OE.Trusted Path teljesülését biztosítja: **FTP_TRP.1 (Megbízható útvonal),** mely arra vonatkozó követelmény, hogy egy megbízható útvonalat kell biztosítani a felhasználó és a rendszer között.

OE.Validation of security function teljesülését az alábbiak biztosítják: **FPT_AMT.1 (Az absztrakt gép tesztelése)**, amely annak garantálását követeli meg, hogy a biztonság-kritikus szoftver, hardver és förmver elemek helyesen működnek, valamint **FPT_TST_CIMC.2**

(Szoftver/förmver sértetlenség teszt), amely annak garantálását követeli meg, hogy a biztonság-kritikus szoftver helyesen működik.

A TOE-ra és környezetére egyaránt vonatkozó biztonsági célok

O(E).Configuration Management teljesülését az alábbiak biztosítják: **FMT_MOF.1 (A biztonsági funkciók viselkedésének kezelése, iteráció 1,2,3),** mely megköveteli, hogy csak erre jogosult személy változtathassa meg a rendszer konfigurációját, **FMT_MOF_CIMC.3 (Kiterjesztett tanúsítvány profil menedzsment), FMT_MOF_CIMC.5 (Kiterjesztett tanúsítvány visszavonási lista profil menedzsment), FMT_MOF_CIMC.6 (OCSP profil menedzsment)** és **FMT_MOF_CWA.1 (Időbélyeg profil menedzsment)**, melyek megkövetelik, hogy a rendszeradminisztrátorok ellenőrizhessék a TOE által generált tanúsítványokba, tanúsítvány visszavonási listákba, OCSP válaszokba és időbélyeg válaszokba kerülő információ típusát. Támogatják még e biztonsági cél teljesülését a következők is: **AGD_ADM.1 (Adminisztrátori útmutató)**, mely elvárja, hogy a rendszeradminisztrátorok számára biztosítva legyen a TOE konfiguráció kezelési tulajdonságait leíró dokumentáció, **A.Competent Administrators, Operators, Officers and Auditors** és **A.CPS,** melyek feltételezik, hogy a rendszeradminisztrátorok hozzáértők, jól ismerik azt a hitelesítési rendet (CP) és szolgáltatási szabályzatot (CPS), mely alatt a TOE-t működtetik. Végül támogatást adnak e biztonsági cél teljesüléséhez a következők is: **ACM_AUT.1 (Részleges konfiguráció kezelés automatizálás), ACM_CAP.4 (A generálás támogatása és elfogadási eljárások)** és **ACM_SCP.2 (A biztonsági hibákat követő konfiguráció kezelés),** melyek garantálják, hogy egy konfiguráció kezelés rendszert valósítanak meg és használnak.

O(E).Data import/export teljesülését az alábbiak biztosítják: **FDP_UCT.1 (Alapszintű adatcsere bizalmasság)** és **FPT_ITC.1 (A TSF-ek közötti bizalmasság az adatátvitel során),** amelyek azt követelik meg, hogy a magán és titkos kulcsokon kívüli adatokat védjék a TOE-ból, illetve a TOE-ba történő továbbítás során, **FDP_ETC_CIMC.5 (Kiterjesztett felhasználói magán és titkos kulcs export)** és **FMT_MTD_CIMC.7 (Kiterjesztett TSF magán és titkos kulcs export)** pedig azt követelik meg, hogy a magán és titkos kulcsok is védve legyenek a TOE-ból, illetve a TOE-ba történő továbbítás során.

O(E).Detect modifications of firmware, software, and backup data teljesülését az alábbiak biztosítják: **FPT_TST_CIMC.2 (Szoftver/förmver sértetlenség teszt)**, amely a szoftver vagy förmver módosítások detektálását követeli meg, **FDP_CIMC_BKP.2 (Kiterjesztett CIMC mentések és visszaállítások),** amely a mentett adatok módosításának észlelését követeli meg. Mivel **FPT_TST_CIMC.2** és **FDP_CIMC_BKP.2** digitális aláírást használ a módosítások észlelésére, ezért **FMT_MTD_CIMC.4 (A TSF magánkulcs bizalmasságának védelme)** követelményre is szükség van annak garantálására, hogy egy szoftvert, förmvert vagy mentett adatokat módosító támadó ne tudja megakadályozni a módosítás észlelését új digitális aláírás kiszámításával.

O(E).Individual accountability and audit records teljesülését követelmények kombinációja biztosítja. **FIA_UID.1 (Az azonosítás időzítése, iteráció 1,2)** azt követeli meg, hogy a felhasználókat azonosítsák, mielőtt biztonság-kritikus műveleteket hajtanának végre. **FAU_GEN.1 (Napló adatok generálása)** azt követeli meg, hogy a biztonság-kritikus eseményeket naplózzák, **FAU_GEN.2 (A felhasználói azonosítóval való összekapcsolás)** és **FPT_STM.1 (Megbízható időbélyegzés)** azt követelik meg, hogy a naplózott események dátumát és időpontját is rögzítsék, a tevékenységért felelős felhasználó azonosítójával együtt. **FMT_MTD.1 (TSF adatok kezelése, iteráció 1,2)** egyrészt azt követeli meg, hogy a naplóadatokat csak a rendszervizsgáló vizsgálhassa át és törölhesse, másrészt azt, hogy csak a rendszeradminisztrátor módosíthasa a rendszeridőt. Végül **FAU_SAR.1 (Napló áttekintés)** és

FAU_SAR.3 (Kiválogatható napló áttekintés) azt követelik meg, hogy a naplóadatok olyan formában legyenek átvizsgálhatók, amely biztosítja az egyének felelősségre vonhatóságát az általuk végrehajtott tevékenységekért.

O(E).Integrity protection of user data and software teljesülését az alábbiak biztosítják: **FDP_ITT.1 (A belső adatátvitel alapszintű védelme, iteráció 1,4)** és **FDP_SDI_CIMC.3 (A tárolt nyilvános kulcs sértetlenségének figyelése és reagálás)** a felhasználói adatok védelmét követelik meg, míg **FPT_TST_CIMC.2 (Szoftver/förmver sértetlenség teszt)** és **FPT_TST CIMC.3 (Szoftver/förmver betöltés teszt)** a szoftver és förmver védelmét követelik meg. Mivel az adatokat és szoftvereket digitális aláírás alkalmazásával védik meg, **FMT_MTD_CIMC.4 (A TSF magánkulcs bizalmasságának védelme)** követelményre is szükség van, hogy az adatok és szoftverek védelméhez használt magánkulcsok bizalmasságát is megvédjék.

O(E).Limitation of administrative access teljesülését az alábbiak biztosítják: **FDP_ACC.1 (Részleges hozzáférés ellenőrzés, iteráció 1,2), FDP_ACF.1 (Biztonsági tulajdonság alapú hozzáférés ellenőrzés, iteráció 1,2), FIA_UAU.1 (A hitelesítés időzítése, iteráció 1,2), FIA_UID.1 (Az azonosítás időzítése, iteráció 1,2)** és **FPT_RVM.1 (A TSP megkerülhetetlensége, iteráció 2). FIA_UID.1** és **FIA_UAU.1** azt követelik meg, hogy a rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók ne hajthassanak végre biztonság-kritikus műveleteket, mielőtt azonosítanák és hitelesítenék őket. **FDP_ACC.1** és **FDP_ACF.1** azt garantálják, hogy a rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók csak a munkájukhoz szükséges műveleteket hajthassák végre. Végül **FPT_RVM.1** azt biztosítja, hogy a rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók nem hajthatnak végre számukra nem engedélyezett műveleteket, a TSP-t érvényre juttató biztonsági funkciók megkerülésével.

O(E).Maintain user attributes teljesülését az alábbiak biztosítják: **FIA_ATD.1 (Felhasználói tulajdonságok megadása, iteráció 1,2)** és **FIA_USB.1 (Felhasználó - szubjektum összerendelése, iteráció 1,2),** melyek biztonsági tulajdonságok kezelését követelik meg, amelyeket az egyéni felhasználókhoz, vagy a helyettük fellépő szubjektumokhoz kell rendelni. **FMT_MSA.1 (Biztonsági tulajdonságok kezelése, iteráció 1,2,3)** azt biztosítja, hogy csak erre jogosult felhasználók módosíthatják a biztonsági tulajdonságokat.

O(E).Manage behavior of security functions teljesülését biztosítja: **FMT_MOF.1 (A biztonsági funkciók viselkedésének kezelése, iteráció 1,2,3),** mely arra vonatkozó követelmény, hogy a jogosult felhasználók konfigurálhassák, működtethessék és kezelhessék a biztonsági mechanizmusokat, illetve az **FMT_SMF.1 (Menedzsment funkciók megadása**, **iteráció 1,2),** ami a biztonsági menedzsment funkciókat adja meg.

O(E).Object and data recovery free from malicious code teljesülését az alábbiak biztosítják: **FPT_TST_CIMC.2 (Szoftver/förmver sértetlenség teszt)** és **FPT_TST_CIMC.3 (Szoftver/förmver betöltés teszt),** melyek azt követelik meg, hogy a visszaállított állapot rosszindulatú programkódtól mentes legyen. **FDP_CIMC_BKP.1 (CIMC mentés és visszaállítás)** és **FDP_CIMC_BKP.2 (Kiterjesztett CIMC mentések és visszaállítások)** pedig a működőképes állapotba való visszaállíthatóságot követelik meg.

O(E).Procedures for preventing malicious code teljesülését az alábbiak biztosítják: **FPT_TST_CIMC.2 (Szoftver/förmver sértetlenség teszt),** mely azt garantálja, hogy csak aláírt kód futtatható, illetve **AGD_ADM.1 (Adminisztrátori útmutató), AGD_USR.1 (Felhasználói útmutató)** és **A.Malicious Code Not Signed,** melyek azt garantálják, hogy akik képesek aláírni kódokat, nem fognak rosszindulatú programkódot aláírni. Támogatja még

ennek a biztonsági célnak a teljesülését: **FDP_ACF_CIMC.2 (A felhasználói magánkulcs bizalmasságának védelme), FDP_ACF_CIMC.3 (A felhasználói titkos kulcs bizalmasságának védelme), FCS_CKM.4 (A kriptográfiai kulcsok megsemmisítése)** és **FCS_CKM_CIMC.5 (A TOE magán és titkos kulcsának nullázása),** melyek azt garantálják, hogy egy nem megbízható entitás nem képes egy megbízható entitás kulcsát használva rosszindulatú programkódot aláírni.

O(E).Protect stored audit records teljesülését az alábbiak biztosítják: **FAU_STG.1 (A naplóesemények védett tárolása),** mely arra vonatkozó követelmény, hogy a naplórekordokat védeni kell a jogosulatlan módosítással vagy törléssel szemben, és **FMT_MTD.1 (TSF adatok kezelése, iteráció 1,2),** mely azt követeli meg, hogy a naplórekordokat és az abba bekerülő rendszeridőt védeni kell a jogosulatlan hozzáférésekkel szemben. **FPT_CIMC_TSP.1 (Napló lista aláírása)** követelmény alapján pedig a naplórekordok módosítása is észlelhető.

O(E).Protect user and TSF data during internal transfer teljesülését az alábbiak biztosítják: **FDP_ITT.1 (A belső adatátvitel alapszintű védelme, iteráció 1,2,3,4),** mely a rendszeren belül átvitt felhasználó adatok védelmét követeli meg, valamint **FPT_ITT.1 (A belső adatátvitel alapszintű védelme, iteráció 1,2,3,4),** mely a rendszeren belül átvitt TSF adatok védelmét követeli meg.

O(E).React to detected attacks teljesülését az alábbiak biztosítják: **FCS_CKM.4 (A kriptográfiai kulcsok megsemmisítése)** és **FCS_CKM_CIMC.5 (A TOE magán és titkos kulcsának nullázása),** melyek arra vonatkozó követelmények, hogy a támadást észlelő felhasználó képes a TOE-n belül nyílt formában tárolt összes kulcs megsemmisítésére, annak megakadályozása érdekében, hogy a támadó megszerezze ezeknek a kulcsoknak a másolatait. **FIA_AFL.1 (Hitelesítési hibák kezelése, iteráció 1,2)** arra vonatkozó követelmény, hogy a TSF válaszoljon az észlelt (ismételt hitelesítési kísérletekben megnyilvánuló) támadásra, olyan ellenintézkedésekkel, melyek megakadályozzák a támadót abban, hogy sikeresen hitelesítse magát. A **FAU_ARP.1 (Biztonsági riasztások)** és **FAU_SAA.1 (A biztonság potenciális megsértésének vizsgálata)** szintén a lehetséges támadások felderítéséhez és kezeléséhez hozzájáruló követelmények.

O(E).Require inspection for downloads teljesülését az alábbiak biztosítják: **FPT_TST CIMC.3 (Szoftver/förmver betöltés teszt),** mely arra vonatkozó követelmény, hogy a letöltendő szoftver csak aláírva szabad elérhetővé tenni, illetve **AGD_ADM.1 (Adminisztrátori útmutató), AGD_USR.1 (Felhasználói útmutató)** és **A.Malicious Code Not Signed,** melyek azt garantálják, hogy akik képesek aláírni szoftvereket, nem fognak rosszindulatú programkódot aláírni.

O(E).Respond to possible loss of stored audit records teljesülését biztosítja: **FAU_STG.4 (A napló adatok elvesztésének meggátolása),** mely arra vonatkozó követelmény, hogy a rendszervizsgáló által végzett tevékenységeken kívül nem lehet naplózni, ha a naplóbejegyzések számára rendelkezésre álló tárhely betelt.

O(E).Restrict actions before authentication teljesülését biztosítja: **FIA_UAU.1 (A hitelesítés időzítése, iteráció 1,2),** mely arra vonatkozó követelmény, hogy biztonság-kritikus tevékenységet nem lehet egy felhasználó nevében végrehajtani, amíg a felhasználót nem hitelesítik.

O(E).Security-relevant configuration management teljesülését az alábbiak biztosítják: **FMT_MSA.3 (Statikus tulajdonságok kezdeti értékadása, iteráció 1,2)** és **FMT_MSA.2 (Biztonságos biztonsági tulajdonságok, iteráció 1,2),** melyek arra vonatkozó követelmények, hogy a biztonsági tulajdonságok biztonságos értékeket vegyenek fel. **FMT_MOF.1 (A biztonsági funkciók viselkedésének kezelése, iteráció 1,2,3)** azt garantálja, hogy a biztonság-

kritikus konfigurációs adatokat csak erre feljogosított személyek módosíthatják. Támogatják még ennek a biztonsági célnak a teljesülését: **AGD_ADM.1 (Adminisztrátori útmutató),** mely arra vonatkozó követelmény, hogy a rendszeradminisztrátorok rendelkezésére álljon a TOE konfiguráció kezelési tulajdonságait leíró dokumentáció, valamint **A.Competent Administrators, Operators, Officers and Auditors** és **A.CPS,** melyek arra vonatkozó követelmények (környezetre tett feltételezések), hogy a rendszeradminisztrátorok hozzáértők, jól ismerik azt a szolgáltatási szabályzatot (CPS), mely alatt a TOE-t működtetik.

O(E).Security roles teljesülését biztosítja: **FMT_SMR.2 (Megszorítások a biztonsági szerepkörökre, iteráció 1,2),** mely arra vonatkozó követelmény, hogy biztonsági szerepköröket kell fenntartani, és a felhasználókat hozzá kell rendelni ezen szerepkörökhöz.

O(E).Time stamps teljesülését biztosítja: **FPT_STM.1 (Megbízható időbélyegzés),** mely arra vonatkozó követelmény, hogy az időpont megbízható.

O(E).User authorization management teljesülését biztosítja: **FMT_MSA.1 (Biztonsági tulajdonságok kezelése, iteráció 1,2,3),** mely arra vonatkozó követelmény, hogy a rendszeradminisztrátorok rendszer biztonsági tisztviselők és biztonsági tisztviselők kezelik és frissítik az általuk kezelt felhasználói biztonsági tulajdonságokat. Támogatják még ennek a biztonsági célnak a teljesülését: **AGD_ADM.1 (Adminisztrátori útmutató),** mely arra vonatkozó követelmény, hogy a rendszeradminisztrátorok rendelkezésére álljon a TOE felhasználói jogosultság kezelési tulajdonságait leíró dokumentáció, valamint **A.Competent Administrators, Operators, Officers and Auditors** és **A.CPS**, melyek arra vonatkozó követelmények (környezetre tett feltételezések), hogy a rendszeradminisztrátorok, hozzáértők, jól ismerik azt a szolgáltatási szabályzatot (CPS), mely alatt a TOE-t működtetik.

8.3 A belső ellentmondás mentesség és a kölcsönös támogatás indoklása

Ez a rész kimutatja, hogy a biztonsági követelmények összessége egy egymást támogató, ellentmondásmentes egységet alkot. A belső ellentmondás mentességet egy függőség elemzés mutatja ki. A kölcsönös támogatás kimutatása a funkcionális biztonsági követelmények közötti egymásra hatás figyelembe vételével történik.

8.3.1 A belső ellentmondás mentesség (a függőségek kielégítése) indoklása

A kiválasztott funkcionális biztonsági követelmények között közvetlen és közvetett függőségi viszonyok vannak. A közvetett függőségek a közvetlen függőségek következményei. Valamennyi függőséget teljesíteni kell, illetve az esetleges nem teljesítéseket meg kell indokolni.

8.3.1.1 A funkcionális biztonsági követelmények függőségei

A 8-9. táblázat összefoglalja a funkcionális biztonsági követelmények között végzett függőség elemzés eredményeit.

8-9. táblázat: A funkcionális biztonsági követelmények közötti függőség elemzés összefoglalása

Követelmény összetevő	függőség	teljesülés
FAU_ARP.1 Biztonsági riasztások	FAU_SAA.1 A biztonság potenciális megsértésének vizsgálata	Igen
FAU_GEN.1 Napló adatok generálása	FPT_STM.1 Megbízható időbélyegzés	Igen
FAU_GEN.2 A felhasználói azonosítóval való összekapcsolás	FAU_GEN.1 Napló adatok generálása	Igen
	FIA_UID.1 Az azonosítás időzítése	Igen
FAU_SAA.1 A biztonság potenciális megsértésének vizsgálata	FAU_GEN.1 Napló adatok generálása	Igen
FAU_SAR.1 Napló áttekintés	FAU_GEN.1 Napló adatok generálása	Igen
FAU_SAR.3 Kiválogatható napló áttekintés	FAU_SAR.1 Napló áttekintés	Igen
FAU_STG.1 A naplóesemények védett tárolása	FAU_GEN.1 Napló adatok generálása	Igen
FAU_STG.4 A napló adatok elvesztésének meggátolása	FAU_STG.1 A naplóesemények védett tárolása	Igen
FCS_CKM.1 Kriptográfiai kulcs generálás	FCS_COP.1 Kriptográfiai műveletek	Igen
	FCS_CKM.4 A kriptográfiai kulcsok megsemmisítése	
	FMT_MSA.2 Biztonságos biztonsági tulajdonságok	
FCS_CKM.4 A kriptográfiai kulcsok megsemmisítése	FCS_CKM.1 Kriptográfiai kulcs generálás	Igen
	FMT_MSA.2 Biztonságos biztonsági tulajdonságok	
FCS_CKM_CIMC.5 A TOE magán és titkos kulcsának nullázása	FCS_CKM.4 A kriptográfiai kulcsok megsemmisítése	Igen
	FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés	Igen
FCS_COP.1 Kriptográfiai műveletek	FCS_CKM.4 A kriptográfiai kulcsok megsemmisítése	Igen
	FDP_ITC.1 Felhasználói adat importálás biztonsági jellemzők nélkül, vagy FCS_CKM.1 A kriptográfiai kulcsok generálása	Igen (FCS_CKM.1)

Követelmény összetevő	függőség	teljesülés
	FMT_MSA.2 Biztonságos biztonsági tulajdonságok	Igen
FDP_ACC.1 Részleges hozzáférés ellenőrzés	FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés	Igen
FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés	FDP_ACC.1 Részleges hozzáférés ellenőrzés	Igen
	FMT_MSA.3 Statikus tulajdonságok kezdeti értékadása	Igen
FDP_ACF_CIMC.2 A felhasználói magánkulcs bizalmasságának védelme	---	---
FDP_ACF_CIMC.3 A felhasználói titkos kulcs bizalmasságának védelme	---	---
FDP_CIMC_BKP.1 CIMC mentés és visszaállítás	FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése	Igen
FDP_CIMC_BKP.2 Kiterjesztett CIMC mentések és visszaállítások	FDP_CIMC_BKP.1 CIMC mentés és visszaállítás	Igen
FDP_CIMC CER.1 Tanúsítvány előállítás	---	---
FDP_CIMC CRL.1 Tanúsítvány visszavonási lista érvényesítés	---	---
FDP_CIMC CSE.1 Tanúsítvány állapot export	---	---
FDP_CIMC OCSP.1 OCSP alap-válasz érvényesítés	---	---
FDP_CWA_ARC.1 Archiválás	FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése	Igen
FDP_CWA_ARC.2 Szelektálható keresés az archívumban	FDP_CWA_ARC.1 Archiválás	Igen
FDP_CWA_ARC.3 Kiterjesztett archiválás	FDP_CWA_ARC.1 Archiválás	Igen
FDP_CWA_TS.1 Időbélyeg válasz érvényesítés	---	Igen
FDP_ETC_CIMC.5 Kiterjesztett felhasználói magán és titkos kulcs export	---	---
FDP_ITT.1 A belső adatátvitel alapszintű védelme	FDP_ACC.1 Részleges hozzáférés ellenőrzés, vagy FDP_IFC.1 Részleges információ áramlás ellenőrzés	Igen (FDP_ACC.1)
FDP_SDI_CIMC.3 A tárolt nyilvános kulcs sértetlenségének figyelése és reagálás	---	---
FDP_UCT.1 Alapszintű adatcsere bizalmasság	FTP_TRP.1 Megbízható útvonal	Igen
	FDP_ACC.1 Részleges hozzáférés ellenőrzés	
FIA_AFL.1 Hitelesítési hibák kezelése	FIA_UAU.1 A hitelesítés időzítése	Igen
FIA_ATD.1 Felhasználói tulajdonságok megadása	---	---
FIA_UAU.1 A hitelesítés időzítése	FIA_UID.1 Az azonosítás időzítése	Igen
FIA_UID.1 Az azonosítás időzítése	---	---
FIA_USB.1 Felhasználó - szubjektum összerendelése	FIA_ATD.1 Felhasználói tulajdonságok megadása	Igen
FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése	FMT_SMR.1 Biztonsági szerepkörök	Igen (FMT_SMR.2)
FMT_MOF_CIMC.3 Kiterjesztett tanúsítvány profil menedzsment	FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése	Igen
	FMT_SMR.1 Biztonsági szerepkörök	Igen (FMT_SMR.2)
FMT_MOF_CIMC.5 Kiterjesztett tanúsítvány visszavonási lista profil menedzsment	FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése	Igen
	FMT_SMR.1 Biztonsági szerepkörök	Igen (FMT_SMR.2)

Követelmény összetevő	függőség	teljesülés
FMT_MOF_CIMC.6 OCSP profil menedzsment	FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése	Igen
	FMT_SMR.1 Biztonsági szerepkörök	Igen (FMT_SMR.2)
FMT_MOF_CWA.1 Időbélyeg profil menedzsment	FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése	Igen
	FMT_SMR.1 Biztonsági szerepkörök	Igen (FMT_SMR.2)
FMT_MSA.1 Biztonsági tulajdonságok kezelése	FDP_ACC.1 Részleges hozzáférés ellenőrzés, vagy FDP_IFC.1 Részleges információ áramlás ellenőrzés	Igen (FDP_ACC.1)
	FMT_SMR.1 Biztonsági szerepkörök	Igen (FMT_SMR.2)
FMT_MSA.2 Biztonságos biztonsági tulajdonságok	ADV_SPM.1 Informális TSP biztonságpolitikai modell	Igen
	FDP_ACC.1 Részleges hozzáférés ellenőrzés, vagy FDP_IFC.1 Részleges információ áramlás ellenőrzés	Igen (FDP_ACC.1)
	FMT_MSA.1 Biztonsági tulajdonságok kezelése	Igen
	FMT_SMR.1 Biztonsági szerepkörök	Igen (FMT_SMR.2)
FMT_MSA.3 Statikus tulajdonságok kezdeti értékadása	FMT_MSA.1 Biztonsági tulajdonságok kezelése	Igen
	FMT_SMR.1 Biztonsági szerepkörök	Igen (FMT_SMR.2)
FMT_MTD.1 TSF adatok kezelése	FMT_SMR.1 Biztonsági szerepkörök	Igen (FMT_SMR.2)
FMT_MTD_CIMC.4 A TSF magánkulcs bizalmasságának védelme	---	---
FMT_MTD_CIMC.7 Kiterjesztett TSF magán és titkos kulcs export	---	---
FMT_SMF.1 Menedzsment funkciók megadása	---	---
FMT_SMR.2 Megszorítások a biztonsági szerepkörökre	FIA_UID.1 Az azonosítás időzítése	Igen
FPT_AMT.1 Az absztrakt gép tesztelése	---	---
FPT_CIMC_TSP.1 Napló lista aláírása	FAU_GEN.1 Napló adatok generálása	Igen
	FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése	Igen
FPT_ITC.1 A TSF-ek közötti bizalmasság az adatátvitel során	---	---
FPT_ITT.1 A belső adatátvitel alapszintű védelme	---	---
FPT_RVM.1 A TSP megkerülhetetlensége	---	---
FPT_STM.1 Megbízható időbélyegzés	---	---
FPT_TST_CIMC.2 Szoftver/förmver sértetlenség teszt	FPT_AMT.1 Az absztrakt gép tesztelése	Igen
FPT_TST_CIMC.3 Szoftver/förmver betöltés teszt	FPT_AMT.1 Az absztrakt gép tesztelése	Igen
FTP_TRP.1 Megbízható útvonal	---	---

8.3.1.2 A garanciális biztonsági követelmények függőségei

A 8-10. táblázat a garanciális biztonsági követelmények között végzett függőség elemzés eredményeit foglalja össze.

8-10. táblázat: A garanciális biztonsági követelmények közötti függőség elemzés összefoglalása

Követelmény összetevő	függőség	teljesülés
ACM_AUT.1 Részleges konfiguráció kezelés automatizálás	ACM_CAP.3	Igen (ACM_CAP.4)
	(közvetett) ACM_SCP.1	Igen (ACM_SCP.2)
	(közvetett) ALC_DVS.1	Igen
ACM_CAP.4 A generálás támogatása és elfogadási eljárások	ACM_SCP.1	Igen
	ALC_DVS.1	Igen
ACM_SCP.2 A biztonsági hibákat követő konfiguráció kezelés	ACM_CAP.3	Igen (ACM_CAP.4)
	(közvetett) ALC_DVS.1	Igen
ADO_DEL.2 A módosítás kimutatása	ACM_CAP.3	Igen (ACM_CAP.4)
	(közvetett) ACM_SCP.1	Igen (ACM_SCP.2)
	(közvetett) ALC_DVS.1	Igen
ADO_IGS.1 Hardver telepítés, szoftver telepítés, a beindítás eljárásai	AGD_ADM.1	Igen
	(közvetett) ADV_FSP.1	Igen (ADV_FSP.2)
	(közvetett) ADV_RCR.1	Igen
ADV_FSP.2 Teljesen meghatározott külső interfészek	ADV_RCR.1	Igen
ADV_HLD.2 Biztonságot érvényre juttató magas szintű tervezés	ADV_FSP.1	Igen (ADV_FSP.2)
	ADV_RCR.1	Igen
ADV_IMP.1 A biztonsági funkciók részleges kivitelezési dokumentálása	ADV_LLD.1	Igen
	ADV_RCR.1	Igen
	ALC_TAT.1	Igen
	(közvetett) ADV_FSP.1	Igen
	(közvetett) ADV_HLD.2	Igen
ADV_LLD.1 Leíró alacsony szintű terv	ADV_HLD.2	Igen
	ADV_RCR.1	Igen
	(közvetett) ADV_FSP.1	Igen (ADV_FSP.2)
ADV_RCR.1 A kölcsönös megfelelés informális szemléltetése	---	---
ADV_SPM.1 Informális biztonságpolitikai modell	ADV_FSP.1	Igen (ADV_FSP.2)
	(közvetett) ADV_RCR.1	Igen
AGD_ADM.1 Adminisztrátori útmutató	ADV_FSP.1	Igen (ADV_FSP.2)
	(közvetett) ADV_RCR.1	Igen
AGD_USR.1 Felhasználói útmutató	ADV_FSP.1	Igen (ADV_FSP.2)
	(közvetett) ADV_RCR.1	Igen
ALC_DVS.1 A biztonsági intézkedések azonosítása	---	---
ALC_FLR.2 Hibajelentési eljárások	---	---
ALC_LCD.1 A fejlesztő által meghatározott életciklus modell	---	---
ALC_TAT.1 Jól meghatározott fejlesztői eszközök	ADV_IMP.1	Igen
	(közvetett) ADV_FSP.1	Igen (ADV_FSP.2)
	(közvetett) ADV_HLD.2	Igen
	(közvetett) ADV_LLD.1	Igen
	(közvetett) ADV_RCR.1	Igen
ATE_COV.2 A teszt lefedettség elemzése	ADV_FSP.1	Igen (ADV_FSP.2)
	ATE_FUN.1	Igen
	(közvetett) ADV_RCR.1	Igen
ATE_DPT.1 A magas szintű terv	(közvetett) ADV_HLD.2	Igen (ADV_HLD.2)

Követelmény összetevő	függőség	teljesülés
tesztelése	ATE_FUN.1	Igen
	(közvetett) ADV_FSP.1	Igen (ADV_FSP.2)
	(közvetett) ADV_RCR.1	Igen
ATE_FUN.1 Funkcionális tesztelés	---	---
ATE_IND.2 Független tesztelés - mintán	ADV_FSP.1	Igen (ADV_FSP.2)
	AGD_ADM.1	Igen
	AGD_USR.1	Igen
	ATE_FUN.1	Igen
	(közvetett) ADV_RCR.1	Igen
AVA_MSU.2 A vizsgálatok megerősítése	ADO_IGS.1	Igen
	ADV_FSP.1	Igen (ADV_FSP.2)
	AGD_ADM.1	Igen
	AGD_USR.1	Igen
	(közvetett) ADV_RCR.1	Igen
AVA_SOF.1 Az értékelés tárgya biztonsági funkcióinak erősségértékelése	ADV_FSP.1	Igen (ADV_FSP.2)
	ADV_HLD.1	Igen (ADV_HLD.2)
	(közvetett) ADV_RCR.1	Igen
AVA_VLA.2 Független sebezhetőség vizsgálat	ADV_FSP.1	Igen
	ADV_HLD.2	Igen
	ADV_IMP.1	Igen
	ADV_LLD.1	Igen
	AGD_ADM.1	Igen
	AGD_USR.1	Igen
	(közvetett) ADV_RCR.1	Igen
	(közvetett) ALC_TAT.1	Igen

8.3.2 A követelmények kölcsönös támogatásának indoklása

A biztonsági követelmények kölcsönösen támogatják egymást oly módon, hogy minden funkcionális biztonsági követelményt (SFR-t) védenek más biztonsági követelmények a megkerülhetőség, hamisíthatóság és kikapcsolhatóság ellen, illetve a támadások észlelhetők.

8.3.2.1 Megkerülhetőség

A megkerülhetőség elleni védelem az alábbiakból származik:

FIA_UID.1 és FIA_UAU.1 támogatja a többi funkciót azáltal, hogy a felhasználók adatokhoz való hozzáférését úgy szabályozza, hogy azonosítás és hitelesítés előtt csak korlátozott tevékenységet tesz lehetővé.

A menedzsment funkciók, köztük a FMT_MOF.1, FMT_MSA.1 és FMT_MTD.1 támogatják az összes többi SFR-t azzal, hogy az egyes menedzsment funkciók változtatásának képességét egyes szerepkörökre korlátozzák, garantálva ezzel, hogy más felhasználók ne játszhassák ki ezen SFR-eket.

FPT_TST_CIMC.2 sértetlenség tesztelést biztosít, mely garantálja, hogy a kiválasztott funkcionális biztonsági követelmények működnek, s így ellenőrzöttek a megkerülés ellen.

FMT_MSA.2 és FMT_MSA.3 korlátozza a biztonsági adatoknak (tulajdonságoknak) adható elfogadható értékek körét, ezzel védve az ilyen adatoktól függő SFR-eket a megkerülés ellen.

8.3.2.2 Hamisíthatóság

A hamisíthatóság elleni védelem az alábbiakból származik:

FAU_STG.1 védi a naplóállományok sértetlenségét.

FCS_CKM.1 és FCS_COP.1 garantálja a biztonságos kulcsgenerálást és kulcskezelést, támogatva így mindazon SFR-eket, melyek ezeknek a kulcsoknak a használatára építenek.

FIA_UID.1 és FIA_UAU.1 támogatja a többi funkciót azáltal, hogy a felhasználók adatokhoz való hozzáférését úgy szabályozza, hogy azonosítás és hitelesítés előtt csak korlátozott tevékenységet tesz lehetővé.

A menedzsment funkciók, köztük a FMT_MOF.1, FMT_MSA.1 és FMT_MTD.1 támogatják az összes többi SFR-t azzal, hogy az egyes menedzsment funkciók változtatásának képességét egyes szerepkörökre korlátozzák, garantálva ezzel, hogy más felhasználók ne játszhassák ki ezen SFR-eket.

FPT_TST_CIMC.2 sértetlenség tesztelést biztosít, mely garantálja, hogy a kiválasztott funkcionális biztonsági követelmények működnek, s így ellenőrzöttek a hamisítás ellen.

FDP_ETC_CIMC.5 véd a titkos és/vagy magánkulcsok exportálása során bekövetkező módosítási hibák ellen.

FIA_AFL.1 támogatja az összes többi hitelesítéssel foglalkozó SFR-t azzal, hogy korlátozza a belépési kísérletek számát, s megfelelő ellenlépéseket tesz a TOE védelmében, ha túl sok kísérlet történik.

FMT_MSA.2 és FMT_MSA.3 korlátozza a biztonsági adatoknak (tulajdonságoknak) adható elfogadható értékek körét, ezzel védve az ilyen adatoktól függő SFR-eket a hamisítás ellen.

8.3.2.3 Kikapcsolhatóság

A kikapcsolhatóság elleni védelem az alábbiakból származik:

Az FDP_ACF.1 által részletezett hozzáférés ellenőrzési SFP a többi hozzáférés ellenőrzéssel kapcsolatos SFR-rel szigorú ellenőrzést biztosít az engedélyezett adatmanipulációk felett, s így megakadályozza a jogosulatlan kikapcsolást.

A menedzsment funkciók, köztük a FMT_MOF.1, FMT_MSA.1 és FMT_MTD.1 támogatják az összes többi SFR-t azzal, hogy az egyes menedzsment funkciók változtatásának képességét egyes szerepkörökre korlátozzák, garantálva ezzel, hogy más felhasználók ne játszhassák ki ezen SFR-eket.

FPT_TST_CIMC.2 sértetlenség tesztelést biztosít, mely garantálja, hogy a kiválasztott funkcionális biztonsági követelmények működnek, s így ellenőrzöttek a kikapcsolás ellen.

FMT_MSA.2 és FMT_MSA.3 korlátozza a biztonsági adatoknak (tulajdonságoknak) adható elfogadható értékek körét, ezzel védve az ilyen adatoktól függő SFR-eket a kikapcsolhatóság ellen.

8.3.2.4 Észlelhetőség

A támadások észlelhetősége az alábbiakból származik:

A biztonsági naplózás funkciók, köztük a FAU_GEN.1 és FAU_GEN.2 biztosítják azoknak a napló adatoknak a generálását, melyekkel észlelhetők az egyes SFR-ekre irányuló speciális

érvénytelenítési kísérletek, illetve a TOE támadhatóságához vezető potenciális rossz konfigurálások.

FAU_SAR.1 és FAU_SAR.3 azzal támogatják a biztonsági naplózás funkciókat, hogy a naplórekordokban választható kereséseket tesznek lehetővé.

FAU_STG.1 és FAU_STG.4 a naplórekordok védelmet biztosítják.

A menedzsment funkciók, köztük a FMT_MOF.1, FMT_MSA.1 és FMT_MTD.1 támogatják az összes többi SFR-t azzal, hogy az egyes menedzsment funkciók változtatásának képességét egyes szerepkörökre korlátozzák, garantálva ezzel, hogy más felhasználók ne játszhassák ki ezen SFR-eket.

FMT_MSA.2 és FMT_MSA.3 korlátozza a biztonsági adatoknak (tulajdonságoknak) adható elfogadható értékek körét, ezzel biztosítva az ilyen adatoktól függő SFR-ek észlelhetőség védelmét.

FMT_SMR.2 különböző szerepkörök meghatározását biztosítja, mely támogatja a többi észlelhetőséget megalapozó SFR-t.

8.4 A funkcióerősség indoklása

A jelen biztonsági előirányzatban leírt TOE-t jó- és rosszindulatú környezetben is működtethetik. A felhasználók is lehetnek rosszindulatúak. Következésképpen a TOE kriptográfiai funkciókat igényel a sértetlenség, bizalmasság, felfedhetetlenség és hitelesség garantálására.

A kriptográfiai mechanizmusok erőssége ugyanakkor a Common Criteria hatókörén kívül esik. A funkcióerősség a CC-ben csak a valószínűségi és permutációs mechanizmusokra alkalmazandó. Mivel ilyen mechanizmust a TOE nem alkalmaz, jelen biztonsági előirányzat nem fogalmaz meg funkcióerősségre vonatkozó elvárást.

8.5 Az értékelési garanciaszint indoklása

A jelen biztonsági előirányzat által elvárt értékelési garanciaszint: kibővített EAL 4.

Ez megfelelő választás olyan TOE-kre, amelyek közepestől magas szintig terjedő függetlenül garantált biztonságot igényelnek a hagyományos piaci TOE-kre, és magasabb biztonsággal kapcsolatos megvalósítási költségeket is készek a gyártók áldozni a termékre. Jelen esetben ez a helyzet.

Az EAL 4-es értékelési garanciaszint komoly garanciákat biztosít a biztonsági funkciók elemzése által. A biztonsági funkciók működésének megértéséhez az alábbiak feldolgozására kerül sor: funkcionális és a teljes interfész specifikáció, az útmutató leírások, magas és alacsony szintű terv, továbbá a megvalósítás egy részhalmaza. Az EAL 4 értékelési garanciaszint olyan fejlett mechanizmusokat és/vagy eljárásokat is megkövetel, amelyek biztosítják, hogy a TOE-t nem hamisították meg a fejlesztés vagy a szállítás során.

Az EAL4 garanciaszint kibővül az ALC_FLR.2 (Hibajelentési eljárások) garanciaösszetevővel, ami biztosítja a biztonsági hibák és igények felhasználói bejelentésének módszeres kezelését, és ez a TOE összetett biztonsági funkcionalitása miatt indokolt garanciakövetelmény.

8.6 Az összefoglaló előírás indoklása

A 8-11. táblázat visszavezeti a TOE biztonsági funkcióit a TOE funkcionális biztonsági követelményeire (mely biztonsági funkció mely TOE funkcionális biztonsági követelményeket elégíti ki). Ennek alapján látható, hogy minden biztonsági funkció hozzájárul a TOE legalább

egy funkcionális biztonsági követelményének a kielégítéséhez (a biztonsági funkciók szükségessége).

A 8-12. táblázat a TOE funkcionális biztonsági követelményeit vezeti vissza a biztonsági funkciókra (mely TOE funkcionális biztonsági követelmény mely biztonsági funkció kielégítéséhez járul hozzá. Ebből látható, hogy minden funkcionális biztonsági követelményt lefed egy biztonsági funkció (a biztonsági funkciók elégségessége).

8-11. táblázat: A biztonsági funkciók visszavezetése a TOE funkcionális biztonsági követelményeire

Biztonsági funkció (BF)	**Funkcionális biztonsági követelmény (SFR) /melynek kielégítéséhez az adott BF hozzájárul/**
BF1 Bizalmi munkakörök kezelése	FMT_SMF.1 (iteráció 2), FMT_SMR.2 (iteráció 2), FMT_MOF.1 (iteráció 3), FMT_MSA.1 (iteráció 2 és 3), FMT_MSA.2 (iteráció 2), FMT_MSA.3 (iteráció 2),
BF2 Azonosítás és hitelesítés	FIA_ATD.1 (iteráció 2), FIA_UID.1 (iteráció 2), FIA_UAU.1 (iteráció 2), FIA_AFL.1 (iteráció 2), FIA_USB.1 (iteráció 2)
BF3 Hozzáférés ellenőrzés	FDP_ACC.1 (iteráció 2), FDP_ACF.1 (iteráció 2), FPT_RVM.1 (iteráció 2)
BF4 Kulcskezelés	FDP_ACF_CIMC.2, FDP_ACF_CIMC.3, FDP_ETC_CIMC.5 FDP_SDI_CIMC.3
BF5 Biztonsági naplózás	FAU_GEN.1, FAU_GEN.2, FPT_CIMC_TSP.1
BF6 A szolgáltatások által létrehozott és fogadott üzenetek védelme	FDP_ITT.1 (iteráció 4), FPT_ITT.1 (iteráció 4)
BF7 Tanúsítvány előállítás	FDP_CIMC_CER.1 FMT_MOF_CIMC.3
BF8 Tanúsítvány visszavonás kezelés	FDP_CIMC_CSE.1, FDP_CIMC_CRL.1, FMT_MOF_CIMC.5 FDP_MOF_OCSP.1 FMT_MOF_CIMC.6
BF9 Időbélyegzés	FDP_CWA_TS.1 FMT_MOF_CWA.1

8-12. táblázat: A funkcionális biztonsági követelmények visszavezetése a biztonsági funkciókra

Funkcionális biztonsági követelmény (SFR)		Biztonsági funkció (BF)
FAU_GEN.1	Napló adatok generálása	5
FAU_GEN.2	A felhasználói azonosítóval való összekapcsolás	5
FDP_ACC.1	Részleges hozzáférés ellenőrzés (iteráció 2)	3
FDP_ACF.1	Biztonsági tulajdonság alapú hozzáférés ellenőrzés (iteráció 2)	3
FDP_ACF_CIMC.2	A felhasználói magánkulcs bizalmasságának védelme	4
FDP_ACF_CIMC.3	A felhasználói titkos kulcs bizalmasságának védelme	4
FDP_CIMC CER.1	Tanúsítvány előállítás	7
FDP_CIMC CRL.1	Tanúsítvány visszavonási lista érvényesítés	8
FDP_CIMC CSE.1	Tanúsítvány állapot export	8
FDP_ETC_CIMC.5	Kiterjesztett felhasználói magán és titkos kulcs export	4
FDP_ITT.1	A belső adatátvitel alapszintű védelme (iteráció 4)	6
FDP_SDI_CIMC.3	A tárolt nyilvános kulcs sértetlenségének figyelése és reagálás	4
FIA_AFL.1	Hitelesítési hibák kezelése (iteráció 2)	2
FIA_ATD.1	Felhasználói tulajdonságok megadása (iteráció 2)	2
FIA_UAU.1	A hitelesítés időzítése (iteráció 2)	2
FIA_UID.1	Az azonosítás időzítése (iteráció 2)	2
FIA_USB.1	Felhasználó - szubjektum összerendelése (iteráció 2)	2
FMT_MOF.1	A biztonsági funkciók viselkedésének kezelése (iteráció 3)	1
FMT_MOF_CIMC.3	Kiterjesztett tanúsítvány profil menedzsment	7
FMT_MOF_CIMC.5	Kiterjesztett tanúsítvány visszavonási lista profil menedzsment	8
FMT_MSA.1	Biztonsági tulajdonságok kezelése (iteráció 2 és 3)	1
FMT_MSA.2	Biztonságos biztonsági tulajdonságok (iteráció 2)	1
FMT_MSA.3	Statikus tulajdonságok kezdeti értékadása (iteráció 2)	1
FMT_SMF.1	Menedzsment funkciók megadása (iteráció 2)	1
FMT_SMR.2	Megszorítások a biztonsági szerepkörökre (iteráció 2)	1
FPT_CIMC_TSP.1	Napló lista aláírása	5
FPT_RVM.1	A TSP megkerülhetetlensége (iteráció 2)	3
FPT_ITT.1	A belső adatátvitel alapszintű védelme (iteráció 4)	6

9. Rövidítések

CA	**Certification Authority**	**Hitelesítés-szolgáltató**
CC	**Common Criteria**	**Közös szempontok**
CIMC	**Certificate Issuing and Management Components**	**Tanúsítványt kibocsátó és kezelő komponensek** /Az alapot képező védelmi profil TOE elnevezése./
CP	**Certification Policy**	**Hitelesítési rend**
CPS	**Certificate Practice Statement**	**Szolgáltatási szabályzat**
CRL	**Certificate Revocation List**	**Tanúsítvány visszavonási lista**
EAL	**Evaluation Assurance Level**	**Értékelési garanciaszint** /A CC 3. rész olyan garanciális összetevőiből álló csomag, amely a CC előre meghatározott garanciális skáláján egy szintet képvisel./
GUI	**Graphical User Interface**	**Grafikus felhasználói interfész**
HSM	**Hardware Cryptographic Module**	**Hardver kriptográfiai modul**
HSZ		**Hitelesítés-szolgáltató**
HTML	**HyperText Markup Language**	Leíró nyelv, előre defiált tag-ekkel.
HTTP	**HyperText Transfer Protocol**	Protokoll (elsődleges mód információ átvitelére web hálózaton)
HTTPS	**HyperText Transfer Protocol Secure**	A http protokoll titkosítással megerősített változata
LDAP	**Lightwieght Directory Access Protocol**	**Egyszerűsített könyvtár elérési protokoll**
NHH		**Nemzeti Hírközlési Hatóság**
OCSP	**Online Certificate Status Protocol**	**Valós idejű tanúsítvány állapot protokoll**
PIN	**Personal Identification Number**	**Személyi azonosító szám**
PKCS	**Public Key Cryptographic Standards**	**Nyilvános kulcsú kriptográfiai szabványok**
PP	**Protection Profile**	**Védelmi profil** /Biztonsági követelmények és célok megvalósítás-független összessége IT termékek vagy rendszerek számára./
RA	**Registration Authority**	**Regisztráló szervezet**
RO	**Registration Officer**	**Regisztrációs tisztviselő**
SAR	**Security Assurance Requirement**	**Garanciális biztonsági követelmény** /A TOE által kielégítendő garanciális biztonsági követelmény, melyeket az 5.3 alfejezet határoz meg./
SC	**Smart Card**	**Intelligens kártya**
SF	**Security Function**	**Biztonsági funkció** /Az értékelés tárgyának (TOE) olyan része vagy részei, amelyekben meg kell bízni ahhoz, hogy a vonatkozó biztonsági szabályzatból (TSP) egy szorosan összefüggő szabályhalmaznak érvényt lehessen szerezni./
SFP	**Security Function Policy**	**Biztonsági funkció szabályzata** /A biztonsági funkciók (TSF) által érvényre juttatott biztonsági szabályzat./

SFR	**Security Functional Requirement**	**Funkcionális biztonsági követelmény** /A TOE vagy annak környezete által kielégítendő funkcionális biztonsági követelmény, melyeket az 5.1 és 5.2 alfejezetek határoznak meg./
SO	**Security Officer**	**Biztonsági tisztviselő**
SOF	**Strength of Function**	**Funkcióerősség** /Az értékelés tárgya (TOE) valamelyik biztonsági funkciójának minősítése, amely azt fejezi ki, hogy minimálisan mekkora erőkifejtést tartanak szükségesnek az elvárt biztonsági működés legyőzéséhez a mögöttes biztonsági mechanizmusok közvetlen megtámadása esetén./
SQL	**Structured Query Language**	Adatbázis lekérdező nyelv
SSO	**System Security Officer**	**Biztonsági tisztviselő**
ST	**Security Target**	**Biztonsági előirányzat** /Biztonsági követelmények és előírások olyan összessége, amelyet egy adott értékelés tárgyának (TOE) értékelésének alapjaként használnak./
SOF	**Strength of Function**	**Funkcióerősség** /Az értékelés tárgya (TOE) valamelyik biztonsági funkciójának minősítése, amely azt fejezi ki, hogy minimálisan mekkora erőkifejtést tartanak szükségesnek az elvárt biztonsági működés legyőzéséhez a mögöttes biztonsági mechanizmusok közvetlen megtámadása esetén./
InfoCA	**InfoCA**	Az értékelés tárgyának neve
TOE	**Target of Evaluation**	**Az értékelés tárgya** /Az az informatikai termék vagy rendszer, valamint a hozzákapcsolódó (rendszer) adminisztrátori és felhasználói útmutatók, amelyre az értékelés irányul./
TS	**TimeStamp**	**Időbélyeg**
TSP	**TOE Security Policy**	**TOE biztonsági szabályzata, biztonság politikája** /Szabályok olyan összessége, amely szabályozza a vagyontárgyak kezelését, védelmét, elosztását az értékelés tárgyán (TOE-n) belül./
TSF	**TOE Security Functions**	**TOE biztonsági funkciói (a TOE biztonsági funkcionalitása)** /Az értékelés tárgyát (TOE) képező minden olyan hardver, szoftver és förmver összessége, amelyben meg kell bízni ahhoz, hogy a vonatkozó biztonságpolitikát (TSP-t) megfelelő módon érvényre lehessen juttatni./
TSF data	**TSF data**	**TSF adat** /Az értékelés tárgya (TOE) által és részére létrehozott adat, amely befolyásolhatja annak (TOE) működését./
TSC	**TSF Scope of Control**	**TSF ellenőrzési kör** /Azon kölcsönhatások összessége, amelyek az értékelés tárgyán (TOE-n) belül vagy azzal kapcsolatban felléphetnek, és amelyeknek a vonatkozó biztonsági szabályzat (TSP) szabályait be kell tartaniuk./
TXT	**Text**	**Szöveges formátum**
ÜKI		**Ügyfél Kapcsolati Iroda**
XML	**eXtensible Markup Language**	**XML formátum**