NCA TWS v2.6.0
NCA megbízható rendszer hitelesítés-szolgáltatáshoz

BIZTONSÁGI ELŐIRÁNYZAT

Verzió:	1.0
Dátum:	2007. július 29.
Fájl:	NCA_ST_v10_final.doc
Minősítés:	Nyilvános
Oldalak:	168

Változáskezelés

Verzió	Dátum	Leírás
0.1	2006.07.17.	A 3., 4. és 5. fejezet tervezet elkészítése a CIMC PP alapján
0.2	2006.09.11.	A fejlesztőkkel való konzultációk és írásos véleményük alapján módosított, kiegészített változat (főbb változások: 2. fejezet vázlatos beépítése, az 5.1 és 5.2 követelményeinek átrendezése és pontosítása, 6.1 kiegészítése)
0.3	2006.10.15.	A fejlesztőkkel való konzultációk és írásos véleményük alapján tovább pontosított és kiegészített változat (főbb változások: 1. és 2. fejezetek bővítése, pontosítása, 6.1 alfejezet részletes kifejtése)
0.4	2006.10.24.	A fejlesztőkkel való konzultációk és írásos véleményük alapján tovább pontosított és kiegészített változat (főbb változások: 1. és 2. fejezetek pontosítása, 6.1 alfejezet pontosítása)
0.5	2006.10.31.	A v0.4-re való fejlesztői reagálás beépítésével készült változat. Tovább bővültek az 1., 2. és 6. fejezetek.
0.6	2006.11.13.	A v0.5-re való fejlesztői reagálás beépítésével készült változat. Átvezetésre kerültek azok a változások, melyek a CIMC_PP 3-as szintjének való megfelelésről hozott döntésből adódtak.
0.65	2006.11.27.	A 8. fejezet befejezése. Előzetes értékelésre átadott (nem hivatalos) verzió
0.9	2007.01.08.	Az előzetes értékelés eredményeit figyelembe vévő változat
0.95	2007.02.23.	Az ismételt előzetes értékelés eredményeit figyelembe vévő, a fejlesztők kiegészítéseit beépítő változat
1.0	2007.07.29.	Az értékelés alapjaként elfogadott végleges változat

Tartalomjegyzék

1. Bevezetés

Ez a fejezet dokumentum-kezelő és áttekintő információkat tartalmaz.
Az "Azonosítás" alfejezet a biztonsági előirányzatok azonosításhoz, katalogizálásához, regisztrációba vételéhez, illetve hivatkozásokhoz szükséges azonosító és leíró információkat tartalmazza.
Az "Áttekintés" alfejezet egy potenciális felhasználó számára ad olyan részletességű áttekintést, melynek alapján eldöntheti a témában való érdekeltségét.
A „Kapcsolódó dokumentumok” alfejezet felsorolja jelen biztonsági előirányzat elkészítéséhez felhasznált szakirodalmat.
„A biztonsági előirányzat szerkezete” alfejezet a 2-9. fejezetek rövid leírását tartalmazza.
A „Common Criteria (Közös szempontok) megfelelőség” alfejezet pedig a CC jelen értékelésnél irányadó verzióját határozza meg.

1.1 Azonosítás

Cím:	NCA TWS v2.6.0 megbízható rendszer hitelesítés-szolgáltatáshoz - Biztonsági előirányzat
Az értékelés tárgya:	NCA (NetLock Certification Authority) Trustworthy System v2.6.0 vagy NCA megbízható rendszer v2.6.0
Az értékelés tárgya rövid neve:	NCA TWS v2.6.0, vagy NCA rendszer v2.6.0, vagy NCA rendszer)
Értékelési garancia szint:	CC EAL4 + (ALC_FLR.2 /Hibajelentési eljárások/ garanciális összetevővel kibővített EAL4)
A biztonsági funkcióerősség:	SOF-alap
Verzió szám:	1.0
Dátum:	2007. május 9.
Szerző:	NetLock Kft.
Védelmi profil megfelelőség:	Certificate Issuing and Management Components Family of Protection Profiles (CIMC-PP) Version 1.0 /Level 3, azaz 3-as biztonsági szint/
CC-verzió:	Common Criteria v2.3

1.2 Áttekintés

Az NCA Trustworthy System v2.6.0 (NCA rendszer) olyan speciális elektronikus aláírási termék, amely különböző hitelesítés-szolgáltatást biztosító funkciókkal rendelkezik.
Az NCA rendszer v2.6.0 a meghívó alkalmazásoktól szolgáltatási üzeneteket, parancsokat fogad, azokat (amennyiben erre szükség van) jogosultságellenőrzés alá veti, majd végrehajtja.
Az alábbi hitelesítés-szolgáltatásokat támogatja:
Alap szolgáltatások (minden üzemmód része):

- regisztráció szolgáltatás,
- tanúsítvány előállítás szolgáltatás,
- tanúsítvány szétosztás szolgáltatás,
- visszavonás kezelés szolgáltatás (CRL, OCSP),
- visszavonás állapot szolgáltatás.

Kiegészítő szolgáltatások (egyes üzemmódok része):

- időbélyegzés szolgáltatás,
- általános aláírás szolgáltatás (GSU),
- titkosító magánkulcs letétbe helyezése szolgáltatás,
- titkosító magánkulcs helyreállítása szolgáltatás.

Az NCA rendszer a tanúsítvány kibocsátásra vonatkozó kérelmeket képes a konfigurációjában meghatározott ellenőrzések és folyamatvezérlési utasítások alapján emberi beavatkozás segítségével vagy anélkül végrehajtani. Képes kezelni a kérelmek, majd később tanúsítványok teljes életciklusát, a kérelem bejelentésétől (előkérelem), a kulcsgeneráláson, az ellenőrzött tanúsítványban szereplő adatok összeállításán (előtanúsítvány) keresztül, a tanúsítvány kiadásáig, valamint a tanúsítvány felfüggesztéséig, visszavonásáig. Az életciklus különböző szakaszaiban a kezelőknek, vizsgálóknak, valamint a külvilágnak pontos információkat képes adni (pl. statisztikák, egyedi státuszok és információk) ember által (HTML lapok, elektronikus levelek), valamint gépek által értelmezhető formákban (pl. CRL, OCSP vagy akár egyedi protokollok).
Az NCA rendszer napló állományai biztosítják a teljes körű ellenőrzést, a tevékenységek nyomon követhetőségét.
Az NCA rendszer széleskörűen konfigurálható és biztosítja a futó szolgáltatások monitorozhatóságát.

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 3280: X.509 Internet Public Key Infrastructure - Certificate and CRL Profile, April 2002

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 (Közös szempontok) 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 NCA rendszer v2.6.0 PKI alapú alkalmazásokhoz különböző szolgáltatásokat biztosít. 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 NCA rendszer alap szolgáltatásai

Az NCA rendszer v2.6.0 alap szolgáltatásai az alábbiak:

- regisztráció szolgáltatás,
- tanúsítvány előállítás szolgáltatás,
- tanúsítvány szétosztás szolgáltatás,
- visszavonás kezelés szolgáltatás,
- visszavonás állapot szolgáltatás (CRL, OCSP).

2.2 Az NCA rendszer kiegészítő szolgáltatásai

Az NCA rendszer v2.6.0 (konfigurációtól függően) az alábbi kiegészítő szolgáltatásokat is támogatja:

- időbélyegzés szolgáltatás,
- titkosító magánkulcs letétbe helyezése szolgáltatás,
- titkosító magánkulcs helyreállítása szolgáltatás.
- általános aláírás szolgáltatás (GSU).

2.3 Az NCA rendszer felhasználói

Az NCA rendszer v2.6.0 felhasználói két fő csoportba sorolhatók:

2.3.1 Külső felhasználók

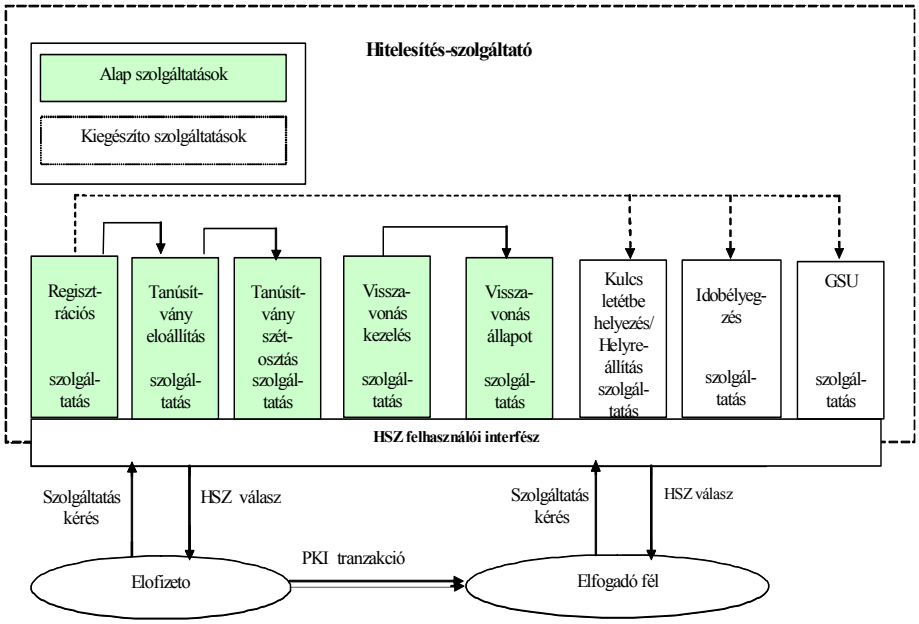
Végfelhasználó (az NCA rendszerben: ügyfél), az NCA rendszer által kibocsátott végfelhasználói tanúsítványok alanya, akinek nyilvános kulcsát a tanúsítvány összeköti személyes azonosítóival.
Érintett fél (az NCA rendszerben: anonymous), egy olyan felhasználó, alkalmazás vagy külső megbízható szolgáltatás, aki/ami döntések meghozatalánál megbízik egy tanúsítványban lévő adatokban (elfogadja azokat), egy elfogadási folyamat után, a tanúsítványban hivatkozott hitelesítési szabályzatot és a tanúsítványban esetlegesen megtalálható korlátozásokat is figyelembe véve. Az érintett fél időbélyeg és OCSP kérésekre kap választ az NCA rendszertől, illetve az NCA rendszerek által korábban kiadott tanúsítványok és CRL-ek között hajthat végre különböző kereséseket és lekérdezéseket.
Általános aláíró (az NCA rendszerben: GSU), egy olyan felhasználó, akinek aláíró magánkulcsa van az NCA rendszerben (pontosabban a HSM-ben), melynek segítségével tetszőleges üzenetek aláírását kérheti a rendszertől.

2.3.2 Belső felhasználók

Különböző jogosultságokkal rendelkező, bizalmas munkaköröket betöltő személyek, akik telepítik, konfigurálják, adminisztrálják, üzemeltetik, karban tartják, illetve ellenőrzik az NCA rendszert. (A bizalmas munkakörök részletesen a 6.1.1 alfejezetben kerülnek kifejtésre.)

2.4 Az NCA rendszer általános felépítése

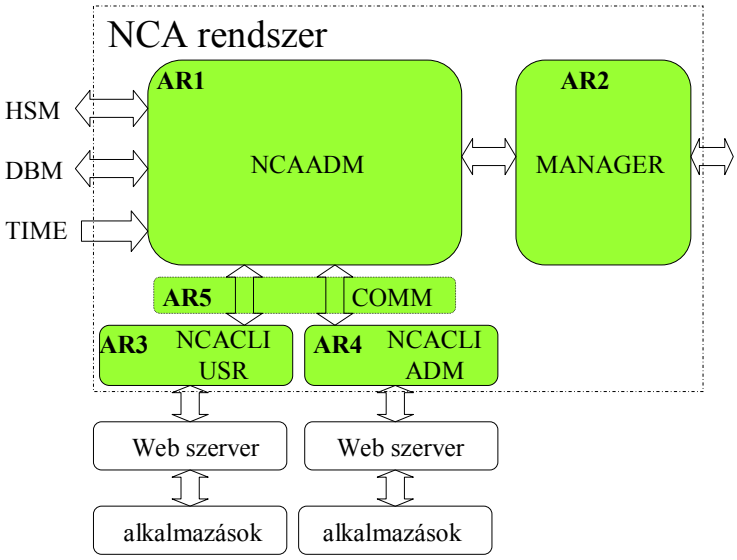
Az NCA rendszer v2.6.0 alapvetően egy hitesítés-szolgáltató megbízható rendszerének lett tervezve, mely a hitesítés-szolgáltató által nyújtott (alap és kiegészítő) szolgáltatásokat valósítja meg, vagy nyújt a megvalósításhoz műszaki/technikai támogatást, ahogyan azt az 1. ábra szemlélteti.



1. ábra: az NCA rendszer általános felépítése

2.5 Az NCA rendszer logikai szerkezete

Az NCA rendszer logikai felépítését, alrendszereit és interfészeit, egyúttal az értékelés tárgya és az informatikai környezet határát mutatja be a 2. ábra. Az ábrán szaggatott vonal jelzi az értékelés hatókörébe eső komponenseket.



2. ábra: Az NCA rendszer alrendszerei, határai és informatikai környezete

2.5.1 Az NCA rendszer alrendszerei

Az NCA rendszer **szerver**ből (a 2. ábrán NCAADM) és hozzá kapcsolódó külső felhasználói, valamint belső felhasználói **kliens**ekből (a 2. ábrán NCACLI USR és NCACLI ADM) áll. Egy szerverhez elvileg kapcsolódhat több (NCACLI USR, NCACLI ADM) kliens példány is, egy (NCACLI USR, NCACLI ADM) kliens pedig több szerverrel is képes kommunikálni (biztosítva ezzel a rendelkezésre állás növelésének, illetve a terhelésmegosztásnak a lehetőségét).

Az AR1 (NCA ADM, szerver oldali) alrendszer célja: megvalósítani az NCA rendszer alap szolgáltatásait (tanúsítvány előállítás, tanúsítvány szétosztás, visszavonás kezelés, visszavonás állapot) és kiegészítő szolgáltatásait (titkosító magánkulcs letétbe helyezése, titkosító magánkulcs helyreállítása, aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése).

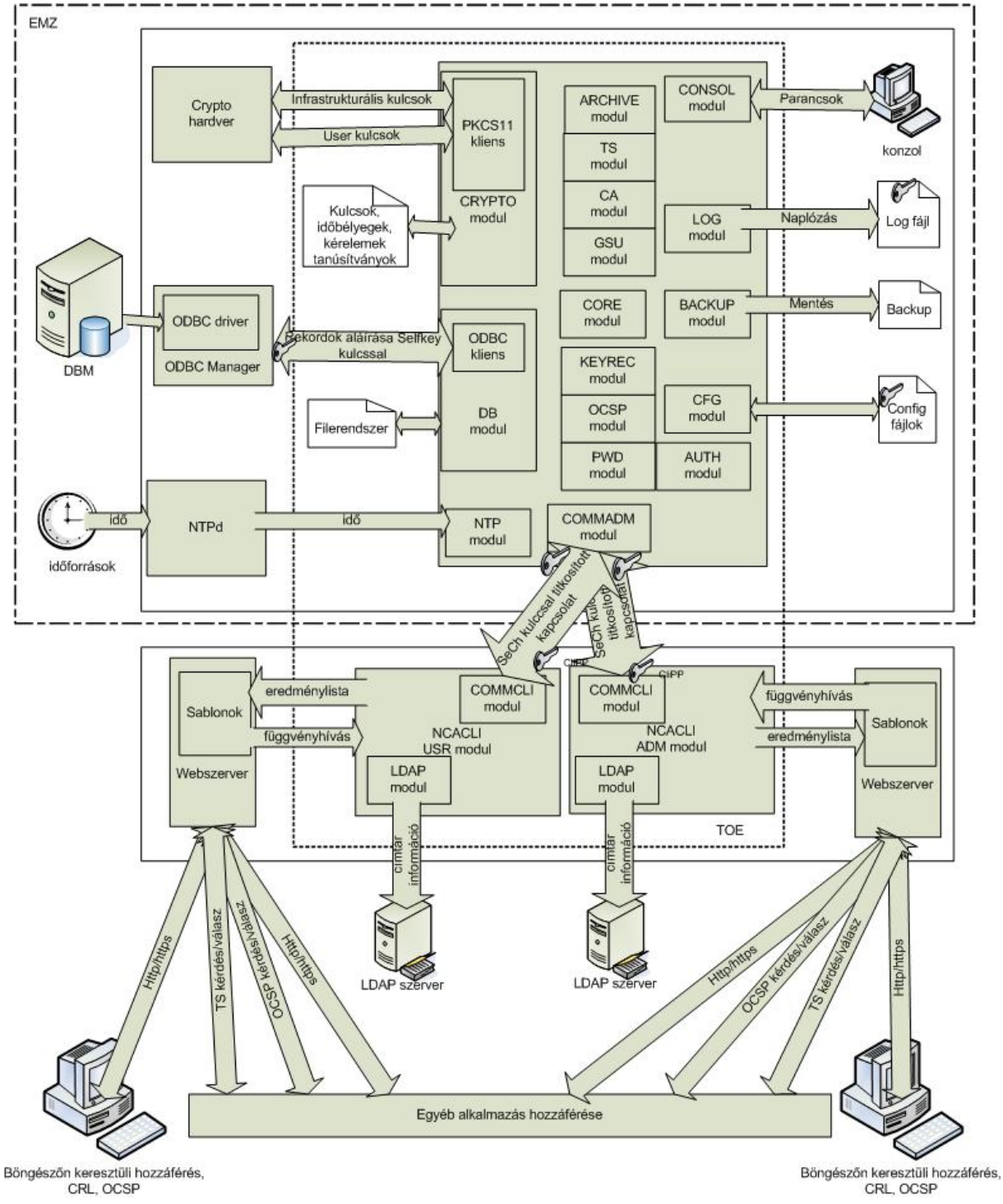
Az AR2 (MANAGER, kezelő) alrendszer célja: a konfigurációs állományokon, illetve konzol parancsokon keresztül elérhető külső interfész kezelése (s ezen keresztüll az AR1 alrendszer működésének szabályozása, vezérlése, a rendszer mentés és naplóállomány exportálás végrehajtása).

Az AR3 (NCACLI USR, külső és belső felhasználók által elérhető kliens oldali) alrendszer célja: a külső és belső felhasználók számára elérhető külső interfészének (pl. webszerver) kezelése (s ezen keresztül az NCA rendszer felhasználói számára az AR1 alrendszer szűkített szolgáltatásainak elérhetővé tétele).

Az AR4 (NCACLI ADM belső felhasználók által elérhető kliens oldali) alrendszer célja: a belső felhasználók számára elérhető külső interfészének (pl. webszerver) kezelése (s ezen keresztül az NCA rendszer privilegizált felhasználói számára az AR1 alrendszer kiegészítő szolgáltatásainak elérhetővé tétele).

Az AR5 (COMM, kommunikációs) alrendszer célja: a szerver és kliensek közötti kommunikáció bizalmasságának, sértetlenségének és hitelességének garantálása.

A 3. ábra az NCA rendszer szerkezetetét a modulok szintjén finomítja.



3. ábra: Az NCA rendszer informatikai környezete, határai és főbb moduljai

2.5.2 Az AR1 alrendszer moduljai

A **CRYPTO modul** a kriptográfiai hardver modulon keresztül elérhető külső interfészt kezeli. Alkalmas különböző PKCS#11-es interfészen keresztül elérhető HSM modulok aktivizálására, s ezen keresztül a kriptográfiai funkciók végrehajttatására. Az értékelt konfigurációkban a HSM kizárólag az alábbi hardver kriptográfiai modul: Protect Server Orange (korábbi nevén CSA 8000), s az interfész is egy ennek megfelelő speciális parancskészlet.

A **DB modul** az adatbázison keresztül elérhető külső interfészt kezeli. Az informatikai környezet részét képező adatbázis szerver (DBM) különböző típusú lehet (pl. MS SQL, Oracle, Sybase, PostgeSQL, ODBC interfésszel).

Az **NTP modul** a szinkronizált időforráson keresztül elérhető külső interfészt kezeli. Az NCA 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. Az NTP modul ellenőrzi, hogy a maximális eltérés a konfigurálható határon belül van-e. Ha belül van, akkor a modul ezt a rendszeridőt elfogadja, s az NCA rendszer ezt használja minden időfüggő szolgáltatásához. Ellenkező esetben a modul naplózza ezt a tényt, s leállít minden időkritikus hitelesítés-szolgáltatást (tanúsítvány előállítás, időbélyegzés, visszavonás állapot szolgáltatás).

Az **ARCHIVE modul** a hosszú távon megőrzendő adatok archiválását végzi el, biztosítva az archívumok teljességét, sértetlenségét és szükség esetén a rendszerbe való visszatölthetőségét.

Az **TS modul** az időbélyegzés szolgáltatást alapozza meg a beérkező időbélyeg kérések ellenőrzésével, feldolgozásával, valamint az időbélyeg válaszok előállításával (az RFC 3161 szabványnak való megfelelőséget biztosítva).

A **CA modul** szervezi (részben végrehajtva, részben a CRYPTO és DB modulokhoz fordulva) a tanúsítvány előállítás és visszavonás kezelés szolgáltatást, valamint a visszavonás állapot szolgáltatáson belül a CRL kibocsátást.

A **GSU modul** egy általános aláíró modul. Segítségével egy erre feljogosított felhasználó (gsu) a HSM modulban tárolt magánkulcsát aktivizálva képes tetszőleges dokumentumokat aláírni. Jelen biztonsági előirányzat hatókörében csak az a funkciója áll, melynek segítségével egy (az ST hatókörén kívül összeállított) viszontazonosítási választ alá lehet írni egy HSM-ben tárolt infrastrukturális kulccsal.

A **KEYREC modul** a szerver oldali kulcsvisszaállítási infrastruktúra megvalósításából, valamint több kliens szerver függvényből áll. Segítségükkel biztonságosan megvalósítható a titkosítás célú kulcspárok generálása, a magánkulcs összetevők titkosított tárolása (kulcs letétbe helyezés), visszaállítása és megszüntetése.

Az **OCSP modul** a visszavonás állapot szolgáltatás részét képező valós idejű állapot protokollt alapozza meg a beérkező OCSP kérések ellenőrzésével, feldolgozásával, illetve az OCSP válaszok előállításával (az RFC 2560 szabványnak való megfelelőséget biztosítva).

A **PWD modul** a jelszó alapú hitelesítéshez megadott titkok memóriában való védelmét biztosítja kódolással.

Az **AUTH modul** az azonosítást és hitelesítést igénylő külső kérések esetén biztosítja a kérést kezdeményező azonosítását és hitelesítését, egy aktív munkaszakasz (session) kiépítését és kezelését (beleértve a munkaszakasz lezárását az erre vonatkozó időkorlátok leteltével), a kérés jogosultság ellenőrzését, majd a jogosultságtól függő visszautasítását, vagy a teljesítésben közreműködő alrendszerhez való továbbítását.

A **LOG modul a** naplóállományokat kezeli (bejegyzéseket generál, tárol, digitálisan aláír, sértetlenséget ellenőriz, az erre jogosultak számára megtekinthetőséget és különböző szempontok szerinti kereshetőséget biztosít).

A **CORE modul** lekezeli a kívülről kapott konzol parancsokat és belső függvény hívásokat, majd megszervezi az ezekben megfogalmazott feladatokat: a helytelen vagy jogosulatlan kéréseket visszautasítja, a jogult kérések teljesítéséhez szükséges tevékenységeket pedig a különböző modulok helyes sorrendben történő meghívásával végrehajtja.

2.5.3 Az AR2 alrendszer moduljai

A **CONSOL modul** a konzolon keresztül elérhető külső interfészt kezeli.

A **BACKUP modul** a biztonságos működéshez szükséges (automatikus és kézi) adatmentéseket hajtja végre, biztosítva a mentések teljességét és sértetlenségét, valamint biztosítja a rendszer mentésből való visszaállíthatóságát.

A **CFG modul** a konfigurációs állományokon keresztül elérhető külső interfészt kezeli.

2.5.4 Az AR3 alrendszer moduljai

A **CLI USR modul** a szűkített függvénykészletet elérő interfészt (pl. webszerveren keresztül) kezeli. Fogadja a külső függvényhívásokat, részt vesz a munkaszakasz kiépítésében, a szerver oldali feldolgozást igénylő feladatok esetén belső parancsokat ad ki, s (az AR5 alrendszer védelme alatt) továbbítja azt a szervernek, az erre kapott válaszokat pedig a külső függvényt hívó felhasználó felé továbbítja.

Az **LDAP modul** a tanúsítvány szétosztás szolgáltatást támogatja azáltal, hogy az NCA rendszer által előállított tanúsítványokat és CRL-eket szabványosan elérhető LDAP-ba publikálja.

2.5.5 Az AR4 alrendszer moduljai

A **CLI ADM modul** a bővített függvénykészletet elérő interfészt (pl. webszerveren keresztül) kezeli. Fogadja a külső függvényhívásokat, részt vesz a munkaszakasz kiépítésében, a szerver oldali feldolgozást igénylő feladatok esetén belső parancsokat ad ki, s (az AR5 alrendszer védelme alatt) továbbítja azt a szervernek, az erre kapott válaszokat pedig a külső függvényt hívó felhasználó felé továbbítja.

Az **LDAP modul** a tanúsítvány szétosztás szolgáltatást támogatja azáltal, hogy az NCA rendszer által előállított tanúsítványokat és CRL-eket szabványosan elérhető LDAP-ba publikálja.

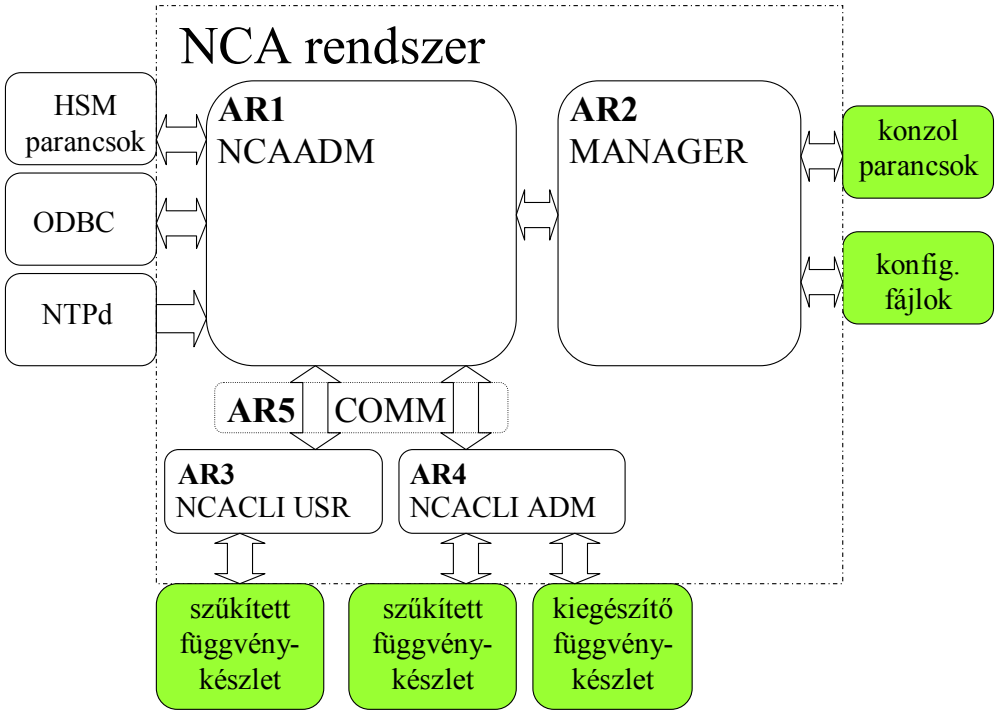
2.5.6 Az AR5 alrendszer moduljai

A **COMM CLI modul** a kliens és szerver közötti kommunikáció bizalmasságát, sértetlenségét és hitelesítését biztosítja a kliens oldalán: digitálisan aláírja és titkosítja a szerver felé küldött csomagokat, illetve dekódolja az onnan fogadott csomagokat, s ellenőrzi azok digitális aláírását.

A **COMM ADM modul** a a kliens és szerver közötti kommunikáció bizalmasságát, sértetlenségét és hitelesítését biztosítja a szerver oldalán: digitálisan aláírja és titkosítja a kliens felé küldött csomagokat, illetve dekódolja az onnan fogadott csomagokat, s ellenőrzi azok digitális aláírását.

2.5.7 Külső interfészek

A 4. ábra a (kívülről is látható) külső interfészeket azonosítja, szemlélteti:



4.

4. ábra: Az NCA rendszer külső interfészei

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

Az **NCACLI USR** felhasználói kliens **szűkített függvénykészlet**ének meghívásán keresztül az érintett felek és az ügyfelek szabadon elérhetik az NCA rendszer alábbi szolgáltatásait:

- keresés a tanúsítványtárban,
- időbélyeg kérés,
- OCSP kérés,
- CRL letöltés.

azonosítás és hitelesítés után pedig az NCA rendszer alábbi szolgáltatásait is elérik:

- regisztrációs adatok felvétele, módosítása,
- tanúsítvány igénylés,
- visszavonás kezelés szolgáltatás (tanúsítvány felfüggesztés és visszavonás).

Az **NCACLI ADM** adminisztrátori kliens **szűkített függvénykészlet**ének meghívásán keresztül a belső felhasználók szabadon elérhetik az NCA rendszer alábbi szolgáltatásait:

- keresés a tanúsítványtárban,
- időbélyeg kérés,
- OCSP kérés,
- CRL letöltés,

azonosítás és hitelesítés után az NCA rendszer alábbi szolgáltatásait is elérik:

- regisztrációs adatok felvétele, módosítása,
- tanúsítvány igénylés,
- visszavonás kezelés szolgáltatás (tanúsítvány felfüggesztés és visszavonás),

Az **NCACLI ADM** adminisztrátori kliens **kiegészítő függvénykészlet**ének meghívásán keresztül a belső felhasználók (azonosításuk és betöltött munkakörüket is érintő hitelesítésük után) az NCA rendszer alábbi szolgáltatásait érhetik el (munkakörüktől függően):

- regisztráció szolgáltatás
- tanúsítvány előállítás szolgáltatás,
- tanúsítvány szétosztás szolgáltatás,
- visszavonás kezelés szolgáltatás (felfüggesztés, visszavonás),
- visszavonás állapot szolgáltatás (CRL, OCSP),
- az NCA rendszer adminisztrálása.

Konzolon keresztül a belső felhasználók (azonosításuk és betöltött munkakörüket is érintő hitelesítésük után) az NCA rendszer telepítésére, üzemeltetésére, karbantartására és ellenőrzésére vonatkozó funkciókat érhetnek el.

Konfigurációs állományokon keresztül (a 4. ábrán Config fájlok) az NCA rendszer működése szabályozható, vezérelhető (az erre feljogosított belső felhasználók által).

2.6 Az NCA rendszer fizikai architektúrája az értékelt kiépítésben

Az NCA rendszer különböző fizikai kiépítésekben működőképes.

Egy szerverhez (a 2. ábrán NCAADM) több kliens (a 2. ábrán NCACLI) is kapcsolódhat, egy kliens pedig több szerverrel is képes kommunikálni, biztosítva ezzel többek között a rendelkezésre állás növelésének, illetve a terhelésmegosztásnak a lehetőségét.

A CRYPTO alrendszer az értékelt kiépítésben a Protect Server Orange HSM-et PKCS#11 interfészen keresztül éri el.

A szerver (NCAADM) az értékelt kiépítésekben az alábbi platformokon futott:

- MS Windows 2003 Server SP1
- Slackware Linux
- Solaris

A kliensek (NCACLI USR és NCACLI ADM) az értékelt kiépítésekben az alábbi platformokon futottak:

- MS Windows 2003 Server SP1
- Slackware Linux
- Solaris

A szerver (NCAADM) és kliensek (NCACLI USR és NCACLI ADM) az értékelt kiépítésekben futott azonos, és külön gépeken egyaránt.

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

- Apache 1.3.33

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

- Mysql 4.0.27 with innodb

Az informatikai környezet részét képező időforrások is különbözők lehetnek.

2.7 Az NCA rendszer különböző üzemmódjai

Az előző alfejezet bemutatta, hogy bár az NCA rendszer különböző fizikai kiépítésekben működőképes, a jelen biztonsági előirányzatnak megfelelő értékelés tárgya azonban egy jól meghatározott kiépítésre (az értékelt kiépítésre) szorítkozik.

Az NCA rendszer értékelt kiépítésének működése nagy szabadsági fokkal tovább szabályozható, különböző biztonsági jellemzők (konfigurációs paraméterek) értékadásával. Bizonyos konfigurációs paraméter csoportok beállításával az NCA 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):

- CWAmode (CWA mód, értéke: 0 vagy 1)
- QualifiedMode (minősített mód, értéke: 0 vagy 1)
- CertificateMode (tanúsítvány-kibocsátási mód, értéke: „none”, „sign”, „pki”, „general”)

Jelen biztonsági előirányzat kizárólag a CWAmode=1 beállításra vonatkozik. CWAmode=1 beállítás mellett az NCA v2.6.0 kielégíti a CWA 14167-1 dokumentumban meghatározott funkcionális és biztonsági követelményeket.

A rendszer üzemmódjai az NCA licenc állományában megadott értékek, s a következő kizárások érvényesülnek:

- QualifiedMode = 1 és CertificateMode = „pki” együtt nem lehetséges
- QualifiedMode = 1 és CertificateMode = „general” együtt nem lehetséges
- ha a licencben a kiadható tanúsítványok száma nem 0, akkor CertificateMode = „none” nem lehet

Az alábbi táblázatok meghatározzák azokat a biztonsági jellemzőket (konfigurációs paramétereket), melyek rögzítésével az NCA rendszer a fenti üzemmódokba állítható (ismét hangsúlyozva, hogy a táblázat a CWAmode=1 beállítás mellett érvényes).

Általános biztonsági jellemzők			
neve	**jelentése**	**üzemmódok**	
		CWAmode = 1 QualifiedMode = 1	**CWAmode = 1 QualifiedMode = 0**
AdminPwdType	jelszó hosszra és jelkészletre vonatkozó szabály (adminisztrátorok részére)	dddd6, ahol legalább 2 „d” értéke 1, a többi lehet 0	dddd6, ahol legalább 2 „d” értéke 1, a többi lehet 0
UserPwdType	jelszó hosszra és jelkészletre vonatkozó szabály (ügyfelek részére)	dddd6, ahol legalább 2 „d” értéke 1, a többi lehet 0	dddd6, ahol legalább 2 „d” értéke 1, a többi lehet 0
KeyPwdType	jelszó hosszra és jelkészletre vonatkozó szabály (kulcsok részére)	dddd6, ahol legalább 2 „d” értéke 1, a többi lehet 0	dddd6, ahol legalább 2 „d” értéke 1, a többi lehet 0
LoginAttemptNum	büntetés nélküli jelszópróbák maximuma (adminisztrátorok részére)	5	5
LoginAttemptTMO	jelszópróbák maximumának elérése utáni büntetés (sec) (adminisztrátorok részére)	60	60
	használható hash algoritmusok készlete	sha1, sha-224, sha-256, ripemd160	sha1, sha-224, sha-256, ripemd160
	minimális RSA kulcshossz	1024	1024 (CertificateMode = „general”-nál nincs megkötés)
	maximális offset	100ms	1,000ms
AutoCA	onlinesign funkció lehetősége	AutoCA=0	AutoCA=0
	mentés védelme digitális aláírás alkalmazásával	kötelező	kötelező
Szerepkör összeférhetetlenség		egy (biztonsági, regisztrációs vagy kulcsvisszaállítási) tisztviselő munkakört betöltő felhasználó nem lehet rendszervizsgáló, egy rendszeradminisztrátori munkakört betöltő felhasználó nem kaphat (biztonsági, regisztrációs vagy kulcsvisszaállítási) tisztviselői vagy rendszervizsgálói jogokat	egy (biztonsági, regisztrációs vagy kulcsvisszaállítási) tisztviselő munkakört betöltő felhasználó nem lehet rendszervizsgáló, egy rendszeradminisztrátori munkakört betöltő felhasználó nem kaphat (biztonsági, regisztrációs vagy kulcsvisszaállítási) tisztviselői vagy rendszervizsgálói jogokat

2-1. táblázat– Általános biztonsági jellemzők

Tanúsítványkiadással kapcsolatos jellemzők			
jelentése	**üzemmódok**		
	CWAmode = 1 QualifiedMode = 1 CertificateMode = „sign”	**CWAmode = 1 QualifiedMode = 0 CertificateMode = „sign”**	**CWAmode = 1 QualifiedMode = 0 CertificateMode = „pki”**
kiadható tanúsítványok	minősített aláíró	nem minősített aláíró	aláírón kívül bármi
tanúsítvány kibocsátás „N” személyes kontrollja	N >=2	N>=1	N>=1
visszajátszás elleni védelem az időbélyeg, OCSP üzenetekben („nonce” használata)	kötelező	nem kötelező	nem kötelező
PolicyQualifier kiterjesztés időbélyegben	a válaszban kötelező, amilyen Policy-val kérték, olyat kap, ha nem kért, akkor alapértelmezettet kap	a válaszban kötelező, amilyen Policy-val kérték, olyat kap, ha nem kért, akkor alapértelmezettet kap	a válaszban kötelező, amilyen Policy-val kérték, olyat kap, ha nem kért, akkor alapértelmezettet kap
„CRL kiadás változás után ennyivel” paraméter, a visszavonási üzenet terjesztési időigénye ($V_{üt}$ maximális értéke)	$V_{üt}$<24 óra	$V_{üt}$<24 óra	nincs megkötés
„automata CRL kiadás ennyi időnként” paraméter, a CRL frissítés ideje	<24 óra	<24 óra	nincs megkötés

2-2. táblázat– Tanúsítványkiadással kapcsolatos jellemzők

Tanúsítványok és kulcsok konfigurálható típusai, jellemzői					
Felhasználási cél	**basicConstraints kritikus kiterjesztés**	**engedélyezett keyUsage halmaz (legalább 1 érték benne) kritikus kiterjesztés**	**KeyRecovery**	**qcCompliance**	**egyéb**
minősített aláírási	cA=false	nonRep (kötelező)	tilos	kötelező (az elemek választhatóak)	PolicyQualifier kötelező
nem minősített aláírási	cA=false	nonRep (kötelező), digSig	tilos	tilos	
autentikációs	cA=false	digSig, keyAgreement	tilos	tilos	
titkosítási	cA=false	keyEncipherment, dataEncipherment	opcionális	tilos	
titkosítási és autentikációs	cA=false	keyEncipherment, dataEncipherment, digSig, keyAgreement	opcionális	tilos	
időbélyeg kiadási	cA=false	nonRep (kötelező)	tilos	tilos	ExtKeyUsage: TimeStamping (kötelező), kritikus kiterjesztés
OCSP válaszadási	cA=false	nonRep (kötelező)	tilos	tilos	engedélyezett ExtKeyUsage halmaz: OCSPSigning (kötelező); engedélyezett még: OCSPNoCheck
láncolt HSz	cA=true	keyCertSign (kötelező), CRLSign, Off-line CRLSign	tilos	tilos	
infrastrukturális kulcsok	cA=false	tilos	tilos	tilos	
általános	nincs megkötés (tehát benne sem kell legyen)	nincs megkötés (tehát benne sem kell legyen)	nincs megkötés	tilos	nincs megkötés

2-3. táblázat– Tanúsítványok és kulcsok konfigurálható típusai, jellemzői

3. A TOE biztonsági környezete

Az NCA rendszert a CIMC védelmi profil 3-as biztonsági szintje követelményeinek kielégítésére tervezték. Következésképpen az NCA rendszer olyan környezetekre megfelelő, ahol a kockázatok és az adatfelfedések és adat sértetlenség elvesztésének következményei közepesek. A 3-as szint védelmet tartalmaz olyan személyekkel szemben is, akik fizikai hozzáféréssel rendelkeznek a komponensekhez, és (a 2-es szinthez képest) további garancia követelményeket tartalmaz annak biztosítására, hogy a TOE biztonságosan működik.

Ez a biztonsági szint védelmet nyújt az alacsony támadóképességgel rendelkező külső támadók ellen.

Ez a biztonsági szint bizonyos védelmet nyújt a rosszindulatú jogosult felhasználókkal szemben is azáltal, hogy legalább három elkülönített szerepkört ír elő, valamint kettős személyi ellenőrzést ír elő a magán kulcs exportra, valamint naplózást ír elő a titkos és magán kulcsok importjára, exportjára, valamint az információ kérelmekre.

3.1 Védendő értékek

Az NCA rendszer által védendő értékek az alábbiak:

Rendelkezésre állás szempontjából:

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

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

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

Bizalmasság szempontjából:

Az alábbi felhasználói adatok bizalmassága:

- a felhasználókról tárolt regisztrációs adatok,
- a felhasználók hitelesítő adatai (jelszavak),
- 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 belső felhasználók jelszavai.

Sértetlenség szempontjából:

Az alábbi felhasználói adatok sértetlensége:

- az ügyfél fiókok (account-ok) tartalma (az ügyfél szerepkör által meghatározott jogosultságok),
- tanúsítványok,
- időbélyeg kérések,
- időbélyeg tokenek (válaszok),
- OCSP kérések,
- OCSP válaszok.

Az alábbi rendszeradatok sértetlensége:

- a belső felhasználói fiókok (account-ok) tartalma (a belső felhasználó által betölthető munkakörök, s az ezek által meghatározott jogosultságok),
- konfigurációs állományok,
- napló állományok,
- adatbázis rekordok,
- szinkronizált idő érték.

3.2 A biztonságos használatra vonatkozó feltételezések[1]

3.2.1 Személyi feltételek

A.Auditors Review Audit Logs
A biztonság-kritikus eseményekről naplóbejegyzés készül, s ezeket a rendszervizsgáló átvizsgálja.

A.Authentication Data Management
A TOE működési környezetében érvényben van egy olyan hitelesítési adat (jelszó és 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
Szakértő rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók vannak kijelölve a TOE és az általa tartalmazott információk biztonságának kezelésére.

A.CPS
Minden rendszeradminisztrátor, rendszerüzemeltető, tisztviselő és rendszervizsgáló 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.

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

A.Notify Authorities of Security Issues
A rendszeradminisztrátoroknak, a rendszerüzemeltetőknek, a tisztviselőknek, a rendszervizsgálóknak és az egyéb felhasználóknak értesíteniük kell a megfelelő vezetőket a rendszert érintő bármely biztonsági eseményről, a további adatvesztés vagy kompromittálódás lehetőségének minimalizálása érdekében.

A.Social Engineering Training
Az általános felhasználók, a rendszeradminisztrátorok, a rendszerüzemeltetők, a tisztviselők és a rendszervizsgálók 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.

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[2]

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

3.3.1 Jogosult felhasználók

T.Administrative errors of omission
Egy rendszeradminisztrátor, rendszerüzemeltető, tisztviselő vagy rendszervizsgáló elmulaszt végrehajtani bizonyos funkciókat, amelyek alapvetően fontosak a biztonság szempontjából.

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

T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
Egy rendszeradminisztrátor, rendszerüzemeltető, tisztviselő vagy rendszervizsgáló véletlenül olyan hibát követ el, amely megváltoztatja a rendszer vagy alkalmazás célul tűzött biztonsági politikáját, 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
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.

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/titkos kulcs módosítva lesz.

T.Sender denies sending information
Egy üzenet küldője letagadja az üzenet elküldését, hogy elkerülje az üzenet küldéséért és az ezt követő cselekvés vagy nem cselekvés miatti felelősségre vonhatóságot.

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[3]

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).

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

4. Biztonsági célok[4]

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

A csak a TOE-ra vonatkozó biztonsági célok négy csoportra oszthatók: jogosult felhasználók, rendszer, kriptográfia, illetve külső támadások.

4.1.1 Jogosult felhasználók

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).

4.1.2 Rendszer

O.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.

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

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

4.1.3 Kriptográfia

O.Non-repudiation
Meg kell akadályozni, hogy a felhasználó elkerülhesse a felelősségre vonhatóságot egy biztonsági szempontból kritikus üzenet elküldéséért, bizonyítékot szolgáltatva arra, hogy a felhasználó küldte az üzenetet.

4.1.4 Külső támadások

O.Control unknown source communication traffic
Ismeretlen forrásból származó kommunikációs forgalmat ellenőrizni kell (pl. átirányítással vagy eldobással) a lehetséges károk elkerülésére.

[4] 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.

4.2 A környezetre 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 rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók 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, hozzáértő és feljogosított rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók kijelölésével a TOE és az általa tartalmazott információk biztonságának kezelésére.

OE.CPS
Minden rendszeradminisztrátornak, rendszerüzemeltetőnek, tisztviselőnek és rendszervizsgálónak 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
Az általános felhasználók, a rendszeradminisztrátorok, a rendszerüzemeltetők, a tisztviselők és a rendszervizsgálók 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.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.Validation of security function
Funkciók és eljárások alkalmazásával biztosítani kell, hogy a biztonság-kritikus szoftver, hardver és förmver elemek helyesen működnek.

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.

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).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.

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 rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók automatikusan ne rendelkezzenek hozzáféréssel a felhasználói objektumokhoz, a szükséges kivételeken kívül. Ellenőrizni kell a rendszeradminisztrátorok és rendszerüzemeltetők 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:

- aláhúzott betűtípus: a CC 2. kötetében szereplő követelményekhez képest a CIMC-PP védelmi profilban tett kiegészítések (végrehajtott műveletek).
- félkövér betűtípus: a jelen biztonsági előirányzat által tett kiegészítések, művelet befejezések, illetve szerkesztői finomítások (esetenként [ ] jelek között).

5.1 Az informatikai környezetre vonatkozó funkcionális biztonsági követelmények

Ez az alfejezet a TOE informatikai környezetére vonatkozó funkcionális biztonsági követelményeket határozza meg.

Az alfejezetben a funkcionális biztonsági követelmény összetevőknél az alábbi jelöléseket alkalmazzuk:

- aláhúzott betűtípus: a CC 2. kötetében szereplő követelményekhez képest a CIMC-PP védelmi profilban tett kiegészítések, művelet végrehajtások.
- félkövér betűtípus: a jelen biztonsági előirányzat által tett kiegészítések, művelet befejezések.

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. táblázat felsorolja az informatikai környezetre vonatkozó funkcionális biztonsági követelményeket (az átláthatóság megkönnyítése érdekében osztályonként csoportosítva).

Biztonsági naplózás (FAU)	Napló adatok generálása (iteráció 1)	FAU_GEN.1
	A felhasználói azonosítóval való összekapcsolás (iteráció 1)	FAU_GEN.2
	Napló áttekintés (iteráció 1)	FAU_SAR.1
	Kiválogatható napló áttekintés (iteráció 1)	FAU_SAR.3
	Kiválasztható napló (iteráció 1)	FAU_SEL.1
	A naplóesemények védett tárolása (iteráció 1)	FAU_STG.1
	A napló adatok elvesztésének meggátolása (iteráció 1)	FAU_STG.4
Kriptográfiai támogatás (FCS)	A kriptográfiai kulcsok generálása	FCS_CKM.1
	A kriptográfiai kulcsok megsemmisítése	FCS_CKM.4
	Kriptográfiai eljárás (iteráció 1)	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
	A belső adatátvitel alapszintű védelme (iteráció 1 és 2)	FDP_ITT.1
	Alapszintű adatcsere bizalmasság	FDP_UCT.1
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)	FMT_MOF.1
	TSF adatok kezelése (iteráció 1)	FMT_MTD.1
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 és 2)	FPT_ITT.1
	A TSP megkerülhetetlensége (iteráció 1)	FPT_RVM.1
	TSF tartomány szétválasztás	FPT_SEP.1
	Megbízható időbélyegzés (iteráció 1)	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

A fenti táblázatban szereplő összetevők többsége a CC 2. kötetéből való.
Az alábbi két összetevő nem szerepel a CC 2. kötetében (kiterjesztett összetevők):

- FPT_TST_CIMC.2
- FPT_TST_CIMC.3

Ezek az összetevők ahhoz szükségesek, hogy egy olyan egyedi követelményt határozzanak meg, amelyekkel a Common Criteria nem foglalkozik. Mindkettő a CIMC-PP védelmi profilban került meghatározásra.

5.1.1Biztonsági naplózás

FAU_GEN.1 Napló adatok generálása (iteráció 1)

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

FAU GEN.1.1 Az IT környezetnek 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) **A TOE fájlrendszerben tárolt állományainak (köztük a napló állományoknak), valamint az adatbázisban tárolt rekordok módosítása, törlése**.

FAU_GEN.1.2 Az IT környezetnek 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) Nincs egyéb naplózandó kiegészítő információ.

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

FAU_GEN.2 A felhasználói azonosítóval való összekapcsolás (iteráció 1)

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

FAU_GEN.2.1 Az IT környezetnek képesnek kell lennie arra, hogy minden naplózható eseményt összekapcsoljon az eseményt kiváltó felhasználó azonosítójával.

FAU_SAR.1 Napló áttekintés (iteráció 1)

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 (iteráció 1)

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 események típusa, valamint az esemény kiváltásáért felelős felhasználó szerint.

FAU_SEL.1 Kiválasztható napló (iteráció 1)

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

FAU_SEL.1.1 Az IT környezetnek képesnek kell lennie arra, hogy a naplózott események halmazába bevegyen, vagy abból kizárjon naplózható eseményeket a következő jellemzők alapján:

a) [az esemény típusa]

b) [nincs egyéb jellemző]

FAU_STG.1 A naplóesemények védett tárolása (iteráció 1)

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 (iteráció 1)

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

FAU_STG.4.1 Az IT környezetnek meg kell gátolnia a naplózható eseményeket a **rendszervizsgáló** által végzetteken kívül, ha a naplóbejegyzések számára rendelkezésre álló tárhely betelt.

FPT_STM.1 Megbízható időbélyegzés (iteráció 1)

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 független időforrások biztosításával támogatja a megbízható időpont előállítását.

5.1.2 Szerepkörök

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:
[napló paraméterek konfigurálása, hitelesítési mechanizmusok konfigurálása, felhasználói fiókok és szerepkörök kezelése**]**

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: **rendszer**adminisztrátor, **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, hogy:
a) egy felhasználó nem tölthet be egyszerre **rendszer**adminisztrátor és rendszervizsgáló 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 az 5-2. táblázatban meghatározott szerepkörökre kell korlátoznia az 5-2. táblázatban felsorolt biztonsági funkciók viselkedésének módosítását.

Funkció	Esemény
Biztonsági naplózás	A rendszeradminisztrátorokra kell korlátozni azt a lehetőséget, hogy a napló paramétereket konfigurálják.
Azonosítás és hitelesítés	Az adminisztrátorokra kell korlátozni azt a lehetőséget, hogy meghatározzák a *hitelesítési kísérletek maximális számá*t. Az adminisztrátorokra kell korlátozni azt a lehetőséget, hogy megváltoztassák a hitelesítési mechanizmusokat.
Fiók (account) kezelés	Az adminisztrátorokra kell korlátozni a felhasználói fiókok és szerepkörök létrehozásának lehetőségét. Az adminisztrátorokra kell korlátozni a felhasználói fiókokhoz és szerepkörökhöz történő jogosultság hozzárendelés lehetőségét.

5-2. táblázat: Jogosult szerepkörök a biztonsági funkciók viselkedésének kezelésére

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 rendszervizsgálóra kell korlátoznia a naplóállományok megtekintését és törlését.

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 az CIMC IT környezet hozzáférés ellenőrzés szabály[5] 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[6] SFP-nek az objektumok vonatkozásában a szubjektum azonossága és a szubjektum által felvehető szerepkörök alapján.

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 az adminisztrátorokra, rendszervizsgálókra és tisztviselőkre 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.

[5] melynek meghatározását lásd az 5.1.3.1 pontban
[6] 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 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 halmaza, **[nincs további biztonsági tulajdonság].**

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 Amennyiben a hitelesítést nem egy FIPS 140 szerint 2-es vagy magasabb szinten (a „szerepkörök és szolgáltatások" területén 3-as vagy magasabb szinten) értékelt kriptográfiai modul hajtja végre, az IT környezetnek észlelnie kell, amikor az adminisztrátor által konfigurálható „hitelesítési kísérletek maximális száma" 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 „hitelesítési kísérletek maximális száma"-ban megadott értéket, az IT környezetnek az alábbiakat kell végrehajtania: **[az érintett felhasználó fiókját blokkolni kell, vagy egy meghatározott idejű késleltetést kell beiktatni a következő hitelesítési kísérlet megkezdhetősééig].**

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 [**lokális és 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 lokális felhasználók, 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 kezdeti felhasználói hitelesítésre és a következőkre: [**nincs egyéb szolgáltatás, amelyhez megbízható útvonal szükséges**].

5.1.5 Távoli adatmegadás és export

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[7], 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[8], a bizalmas felhasználói adatok felfedésének megakadályozása érdekében, az IT környezet fizikailag elkülönülő részei közötti átvitel közben.

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

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[9], hogy képes legyen objektumokat a jogosulatlan felfedésekkel szemben védett módon átvinni.

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.

[9] melynek meghatározását lásd az 5.1.3.1 pontban

5.1.6 Kulcs menedzsment

5.1.6.1 Kulcs generálás

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: [**RSA, DES, 3DES, AES**], melyek megfelelnek a következőknek: [**FIPS PUB 186-2 (RSA), FIPS PUB 186-2 Appendix3 (DES, 3DES), FIPS PUB 197 (AES)**].

5.1.6.2 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**].

5.1.7 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_.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**].

A fenti összetevő egy kiterjesztett (CC 2. kötetben nem szereplő) követelményt határoz meg.
A következő biztonsági célokat támogatja: O(E).Integrity protection of user data and software és OE.Periodically check integrity.

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**].

A fenti összetevő egy kiterjesztett (CC 2. kötetben nem szereplő) követelményt határoz meg.
A következő biztonsági célokat támogatja: O(E).Integrity protection of user data and software és OE.Periodically check integrity.

5.1.8 Kriptográfiai modulok

A TOE egy külön hardver kriptográfiai modult alkalmaz a legtöbb kriptográfiai funkció végrehajtására. Az alábbi követelmény erre a modulra (HSM) vonatkozik.

FCS_COP.1 Kriptográfiai eljárás (iteráció 1)

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 197 (AES titkosítás és dekódolás), FIPS PUB 186-2 (RSA aláírás létrehozás és aláírás ellenőrzés), FIPS 180-2 (SHA1 lenyomat generálás és lenyomat ellenőrzés)**].

5.2 A TOE-ra vonatkozó funkcionális biztonsági követelmények

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

Az alfejezetben a funkcionális biztonsági követelmény összetevőknél az alábbi jelöléseket alkalmazzuk:

- aláhúzott betűtípus: a CC 2. kötetében szereplő követelményekhez képest a CIMC-PP védelmi profilban tett kiegészítések, művelet végrehajtások.
- félkövér betűtípus: a jelen biztonsági előirányzat által tett kiegészítések, művelet befejezések.

Az 5-3. táblázat felsorolja a TOE-ra vonatkozó funkcionális biztonsági követelményeket (az átláthatóság megkönnyítése érdekében osztályonként csoportosítva).

Biztonsági naplózás (FAU)	Biztonsági riasztások	FAU_ARP.1
	Napló adatok generálása (iteráció 2)	FAU_GEN.1
	A felhasználói azonosítóval való összekapcsolás (iteráció 2)	FAU_GEN.2
	A biztonság potenciális megsértésének vizsgálata	FAU_SAA.1
	Napló áttekintés (iteráció 2)	FAU_SAR.1
	Kiválogatható napló áttekintés (iteráció 2)	FAU_SAR.3
	Kiválasztható napló (iteráció 2)	FAU_SEL.1
	A naplóesemények védett tárolása (iteráció 2)	FAU_STG.1
	A napló adatok elvesztésének meggátolása (iteráció 2)	FAU_STG.4
Kommunikáció (FCO)	Kötelező eredet bizonyítás és eredet ellenőrzés	FCO_NRO_CIMC.3
	Az eredet fokozott ellenőrzése	FCO_NRO_CIMC.4
Kriptográfiai támogatás (FCS)	Kriptográfiai műveletek (iteráció 2)	FCS_COP.1
	A TOE magán és titkos kulcsának nullázása	FCS_CKM_CIMC.5
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
	CIMC mentés és visszaállítás	FDP_CIMC_BKP.1
	Kiterjesztett CIMC mentések és visszaállítások	FDP_CIMC_BKP.2
	Archiválás	FDP_CWA_ARC.1
	Szelektálható keresés az archívumban	FDP_CWA_ARC.2
	Kiterjesztett archiválás	FDP_CWA_ARC.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 előállítás	FDP_CWA_TS.1
	Kiterjesztett felhasználói magán és titkos kulcs export	FDP_ETC_CIMC.5
	A belső adatátvitel alapszintű védelme (iteráció 3 és 4)	FDP_ITT.1
	A tárolt nyilvános kulcs sértetlenségének figyelése és reagálás	FDP_SDI_CIMC.3
Azonosítás és hitelesítés (FIA)	Hitelesítési hibák kezelése (iteráció 2)	FIA_AFL.1
	Felhasználói tulajdonságok megadása (iteráció 2)	FIA_ATD.1
	A titkok ellenőrzése	FIA_SOS.1
	A hitelesítés időzítése (iteráció 2)	FIA_UAU.1
	Az azonosítás időzítése (iteráció 2)	FIA_UID.1
	Felhasználó - szubjektum összerendelése (iteráció 2)	FIA_USB.1
Biztonsági menedzsment (FMT)	A biztonsági funkciók viselkedésének kezelése (iteráció 2)	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	FMT_MSA.1
	Biztonságos biztonsági tulajdonságok	FMT_MSA.2
	Statikus tulajdonságok kezdeti értékadása	FMT_MSA.3
	TSF adatok kezelése (iteráció 2)	FMT_MTD.1
	A TSF magánkulcs bizalmasságának védelme	FMT_MTD_CIMC.4
	A TSF titkos kulcs bizalmasságának védelme	FMT_MTD_CIMC.5
	Kiterjesztett TSF magán és titkos kulcs export	FMT_MTD_CIMC.7
	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 3 és 4)	FPT_ITT.1
	Megbízható időbélyegzés (iteráció 2)	FPT_STM.1

5-3. táblázat– A TOE-ra vonatkozó funkcionális biztonsági követelmények

A fenti táblázatban szereplő összetevők többsége a CC 2. kötetéből való.

Az alábbi összetevők nem szerepelnek a CC 2. kötetében (kiterjesztett összetevők):

- FCO_NRO_CIMC.3
- FCO_NRO_CIMC.4
- FCS_CKM_CIMC.5
- FDP_ACF_CIMC.2
- FDP_ACF_CIMC.3
- FDP_CIMC_BKP.1
- FDP_CIMC_BKP.2
- FDP_CWA_ARC.1
- FDP_CWA_ARC.2
- FDP_CWA_ARC.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
- FMT_MTD_CIMC.4
- FMT_MTD_CIMC.5
- FMT_MTD_CIMC.7
- FPT_CIMC_TSP.1

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

5.2.1 Biztonsági naplózás

FAU_GEN.1 Napló adatok generálása (iteráció 2)

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 5-4. 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) Minden esemény típusra azok az információk, amelyek az 5-4. táblázat "Kiegészítő információk" oszlopában vannak leírva.

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

FAU_GEN.2 A felhasználói azonosítóval való összekapcsolás (iteráció 2)

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.

FAU_SAR.1 Napló áttekintés (iteráció 2)

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

FAU_SAR.1.1 A TSF-nek biztosítania kell a rendszervizsgálók számára azt a lehetőséget, hogy a napló állományokból kiolvassák az összes információt.

FAU_SAR.1.2 A TSF-nek a napló állományokat olyan formában kell szolgáltatnia, amelyek alkalmas arra, hogy a felhasználó értelmezze az információkat.

5-4. táblázat – Naplózandó események és naplóadatok

Funkció	Összetevő	Esemény	Kiegészítő információk
Biztonsági naplózás	FAU_GEN.1 Napló adatok generálása	A napló paraméterekben történő minden változás (pl. napló gyakoriság, naplózott esemény típusa). Minden kísérlet a napló állomány törlésére	
	FPT_CIMC_TSP.1 A napló állomány aláírása	A napló állomány aláírása.	A **digitális aláírást**, kulcsolt lenyomatot vagy hitelesítési kódot be kell venni a napló állományba.
Azonosítás és hitelesítés	FIA_ATD.1 Felhasználói tulajdonságok megadása	Sikeres és sikertelen kísérletek egy szerepkör felvételére	
	FIA_AFL.1 A hitelesítési hiba kezelése	A *hitelesítési kísérletek maximális száma* értékének módosítása.	
	FIA_AFL.1 A hitelesítési hiba kezelése	A felhasználói login során a sikertelen kísérletek száma eléri *a hitelesítési kísérletek maximális számá*-t.	
	FIA_AFL.1 A hitelesítési hiba kezelése	Egy adminisztrátor feloldja egy account zárolását, amely a sikertelen hitelesítési kísérletek következtében történt meg.	
		Egy adminisztrátor megváltoztatja a hitelesítési mechanizmus típusát, pl. jelszóról **tanúsítvány** alapúra.	
Account adminisztráció		Szerepkörök és felhasználók hozzáadása és törlése. Egy felhasználói account vagy egy szerepkör hozzáférés- ellenőrzési jogosultságainak módosítása.	
Lokális adatmegadás		Minden olyan, a biztonság-kritikus adat, amelyet a rendszer számára megadtak.	Az adatot megadó egyén azonosítója, ha a megadott adat valamilyen más adathoz kapcsolódik (pl. klikkelés egy "accept" gombra). Ezt csatolni kell az elfogadott adattal együtt.
Távoli adatmegadás		Minden biztonság-kritikus üzenet, amelyet a rendszer kapott.	
Adat export és output		Minden, bizalmas és biztonság-kritikus információ iránti, sikeres és sikertelen kérelem.	
Kulcs generálás	FCS_CKM.1 Kriptográfiai kulcsgenerálás (IT környezetre vonatkozó követelmény)	Valahányszor a TSF egy kriptográfiai kulcs generálást kér. (Nem kötelező egy munkaszakasz (session) által használt vagy egyszeri használatú szimmetrikus kulcsok esetén.)	A generált aszimmetrikus kulcs-párok nyilvános komponense
Magán kulcs betöltés		A komponens (infrastrukturális) magán kulcsok betöltése	

Funkció	Összetevő	Esemény	Kiegészítő információk
Magán kulcs tárolás		Minden, a tanúsítvány alany magánkulcsaihoz való hozzáférés, amelyeket a TOE-n belül megőriztek kulcs-visszaállítás céljából.	
Megbízható nyilvános kulcs megadása, törlése és tárolása		A megbízható nyilvános kulcsokban történő minden változtatás, beleértve a hozzáadásokat és törléseket is.	A nyilvános kulcs és a kulcshoz kapcsolódó minden információ
Titkos kulcs tárolás		A hitelesítésre szolgáló titkos kulcsok manuális beadása.	
Magán és titkos kulcs export	FDP_ETC_CIMC.5 Kiterjesztett felhasználói magán és titkos kulcs export; FMT_MTD_CIMC.7 Kiterjesztett TSF magán és titkos kulcs export	A magán és titkos kulcsok exportálása (kivéve azokat a kulcsokat, amelyeket egy egyszeres munkaszakaszhoz vagy üzenethez használnak)	
Kulcs törlés	FCS_CKM_CIMC.5 A TOE magán és titkos kulcsának nullázása	Valahányszor a TSF egy kriptográfiai kulcs törlését kéri. (Nem kötelező egy munkaszakasz (session) által használt vagy egyszeri használatú szimmetrikus kulcsok esetén.)	
Tanúsítvány előállítás	FDP_CIMC_CER.1 Tanúsítvány előállítás	Minden tanúsítvány kérelem, beleértve mindkét tanúsítvány megújítási kérelmet (újra hitelesítés, kulcs megújítás) is. Minden tanúsítvány kérelem jóváhagyással kapcsolatos esemény.	Ha elfogadásra kerül, akkor a tanúsítvány egy másolata. Ha elutasításra kerül, akkor a visszautasítás oka (pl. érvénytelen adat, a kérelmet a tisztviselő visszautasította, stb.)
Tanúsítvány állapot megváltoztatás jóváhagyása		Tanúsítvány állapot megváltoztatására vonatkozó minden kérelem	A kérelem jóváhagyásra vagy elutasításra került
Tanúsítvány visszavonási állapot		Minden OCSP kérés és válasz	
Időbélyeg szolgáltatás		A megbízható időforrásokkal kapcsolatos minden hiba (beleértve a megengedett tűréshatárt meghaladó időeltolódást).	
TOE konfiguráció		Minden biztonság-kritikus változtatás a TOE konfigurációjában	
Tanúsítvány profil menedzsment	FMT_MOF_CIMC.3 Kiterjesztett tanúsítvány profil menedzsment	Minden változtatás a tanúsítvány profilban	A profilban történt változtatás
Visszavonási profil menedzsment		Minden változtatás a visszavonási profilban	A profilban történt változtatás

Funkció	Összetevő	Esemény	Kiegészítő információk
Tanúsítvány visszavonási lista profil menedzsment	FMT_MOF_CIMC.5 Kiterjesztett tanúsítvány visszavonási lista profil menedzsment	Minden változtatás a tanúsítvány visszavonási lista profilban	A profilban történt változtatás
Valós idejű tanúsítvány állapot protokoll (OCSP) profil menedzsment	FMT_MOF_CIMC_6 OCSP profil menedzsment	Minden változtatás az OCSP profilban	A profilban történt változtatás
Időbélyeg profil menedzsment	FMT_MOF_CWA_1 Időbélyeg profil menedzsment	Minden változtatás az időbélyeg profilban	A profilban történt változtatás

FAU_SAR.3 Kiválogatható napló áttekintés (iteráció 2)

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

FAU_SAR.3.1 A TSF-nek lehetőséget kell biztosítania a napló állományokban történő keresések végrehajtására az alábbiak alapján: az események típusa, az esemény kiváltásáért felelős felhasználó, az 5-5. táblázatban megadottak szerint.

5-5. táblázat: Keresési lehetőségek a naplóállományokban

Funkció	Keresési kritérium
Távoli és lokális tanúsítvány kérelem	A kért tanúsítvány alanyának azonosítója
Távoli és lokális tanúsítvány visszavonási kérelem	A visszavonandó tanúsítvány alanyának azonosítója

FAU_SEL.1 Kiválasztható napló (iteráció 2)

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

FAU_SEL.1.1 A TSF-nek képesnek kell lennie arra, hogy a naplózott események halmazába bevegyen, vagy abból kizárjon naplózható eseményeket a következő jellemzők alapján:

a) [az esemény típusa (meghívott szerver oldali függvény)]

b) [az esemény kiváltásában érintett felhasználó szerepköre]

FAU_STG.1 A naplóesemények védett tárolása (iteráció 2)

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

FAU_STG.1.1 A TSF-nek védenie kell a tárolt naplóállományokat a jogosulatlan törléssel szemben.

FAU_STG.1.2 A TSF-nek képesnek kell lennie arra, hogy észlelje a naplóállományok megváltoztatását.

FAU_STG.4 A napló adatok elvesztésének meggátolása (iteráció 2)

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

FAU_STG.4.1 A TSF-nek meg kell gátolnia a naplózható eseményeket a rendszervizsgáló által végzetteken kívül, ha a napló állományok számára rendelkezésre álló tárhely betelt.

FPT_STM.1 Megbízható időbélyegzés (2. iteráció)

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FPT_STM.1.1 A TSF-nek képesnek kell lennie arra, hogy megbízható időpontot állítson elő saját használatra.

Megjegyzés: A TSF az IT környezet által biztosított független időforrások szinkronizálásával támogatja a megbízható időpont előállítását.

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.

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 A TSF-nek 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 A TSF-nek a következő szabályokat kell érvényre juttatnia a naplóesemények figyelemmel kísérése során:

a) Az alábbi naplóesemények összegzése vagy kombinálása [ncasa, **ncaroot, ncaop, ncaau, ncara, ncaca és ncakr esetén legalább három egymást követő sikertelen hitelesítési kísérlet bekövetkezése**], 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 A TSF-nek a biztonság potenciális megsértése esetén az alábbiakat kell tennie: [**Az nca rendszer konfigurációban megadható címen, http(s) protokollon meg tud hívni eljárást, s annak a naplóesemény adatait átadja. A meghívott eljárás levelet vagy egyéb módon értesítést küldhet a megfelelő címzetteknek**.]

5.2.2 Bizalmi munkakörök (szerepkörök)

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:
[konfigurálás (napló paraméterek, hitelesítési mechanizmusok, mentési paraméterek, egyéb konfigurációs paraméterek), felhasználói fiókok és szerepkörök kezelése, mentés és visszaállítás, TOE magánkulcs exportálása, (tanúsítvány-, CRL-, OCSP-, időbélyeg-) profilok menedzselése]

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: **biztonsági** adminisztrátor, **rendszer**adminisztrátor, rendszervizsgáló, tisztviselő és **rendszerüzemeltető**.

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

FMT_SMR.2.3 A TSF-nek biztosítania kell, hogy:

a) egy felhasználó nem tölthet be egyszerre **biztonsági** adminisztrátor és tisztviselő szerepkört,

b) egy felhasználó nem tölthet be egyszerre **rendszer**adminisztrátor és tisztviselő szerepkört,

c) egy felhasználó nem tölthet be egyszerre rendszervizsgáló és tisztviselő szerepkört,

d) egy felhasználó nem tölthet be egyszerre **biztonsági** adminisztrátor és rendszervizsgáló szerepkört,

e) egy felhasználó nem tölthet be egyszerre **rendszer**adminisztrátor és rendszervizsgáló szerepkört,

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 A TSF-nek az 5-6. táblázatban meghatározott szerepkörökre kell korlátoznia az 5-6. táblázatban felsorolt biztonsági funkciók viselkedésének módosítását.

Funkció	Összetevő	Esemény
Biztonsági naplózás		A rendszeradminisztrátorokra kell korlátozni azt a lehetőséget, hogy a napló paramétereket konfigurálják. A rendszeradminisztrátorokra kell korlátozni azt a lehetőséget, hogy a napló lista aláírási esemény gyakoriságát megváltoztassák.
Azonosítás és hitelesítés		A rendszeradminisztrátorokra kell korlátozni azt a lehetőséget, hogy meghatározzák a *hitelesítési kísérletek maximális számá*t. A rendszeradminisztrátorokra kell korlátozni azt a lehetőséget, hogy megváltoztassák a hitelesítési mechanizmusokat.
Fiók (account) kezelés		A biztonsági adminisztrátorokra kell korlátozni a felhasználói fiókok és szerepkörök létrehozásának lehetőségét. A biztonsági adminisztrátorokra kell korlátozni a felhasználói fiókokhoz és szerepkörökhöz történő jogosultság hozzárendelés lehetőségét.
Mentések és visszaállítások		A rendszeradminisztrátorokra kell korlátozni azt a lehetőséget, hogy a mentési paramétereket konfigurálják. A rendszeroperátorokra kell korlátozni azt a lehetőséget, hogy a mentés vagy visszaállítás funkciót kezdeményezzék.
Tanúsítvány regisztrálás		A tisztviselőkre kell korlátozni azt a lehetőséget, hogy a tanúsítványokba kerülő mezőket és kiterjesztéseket jóváhagyják. Ha automatizált eljárást alkalmaznak arra, hogy tanúsítványok által tartalmazott mezőket vagy kiterjesztéseket jóváhagyjanak, akkor ezen eljárás konfigurálásának lehetőségét a tisztviselőkre kell korlátozni.
Adat export és output		A TOE magánkulcs exportálásához legalább két rendszeradminisztrátor, vagy egy rendszeradminisztrátor és egy tisztviselő, rendszervizsgáló vagy rendszerüzemeltető jóváhagyása szükséges.
Tanúsítvány állapot megváltoztatásának jóváhagyása		Csak tisztviselők konfigurálhatják azt az automatizált folyamatot, amely egy tanúsítvány visszavonásának jóváhagyására, vagy a tanúsítvány visszavonására vonatkozó információk nyújtására szolgálnak. Csak tisztviselők konfigurálhatják azt az automatizált folyamatot, amely egy tanúsítvány felfüggesztésének jóváhagyására, vagy a tanúsítvány felfüggesztett állapotára vonatkozó információk nyújtására szolgálnak.
TOE konfiguráció		A rendszeradminisztrátorokra kell korlátozni a TOE valamennyi biztonsági funkcionalitásának a konfigurálását. (Ez a követelmény minden konfigurációs paraméterre vonatkozik, hacsak nem egy olyan TOE funkcionalitásról van szó, amelynek konfigurálási lehetősége egy másik szerepkörre van kiosztva valahol ebben a dokumentumban.)

Funkció	Összetevő	Esemény
Tanúsítvány profil menedzsment	FMT_MOF_CIMC.3 Kiterjesztett tanúsítvány profil menedzsment	A biztonsági adminisztrátorokra kell korlátozni azt a lehetőséget, hogy a tanúsítvány profilt módosítsák.
Tanúsítvány visszavonási lista profil menedzsment	FMT_MOF_CIMC.5 Kiterjesztett tanúsítvány visszavonási lista profil menedzsment	A biztonsági adminisztrátorokra kell korlátozni azt a lehetőséget, hogy a tanúsítvány visszavonási lista profilt módosítsák.
Valós idejű tanúsítvány állapot protokoll (OCSP) profil menedzsment	FMT_MOF_CIMC.6 OCSP profil menedzsment	A biztonsági adminisztrátorokra kell korlátozni azt a lehetőséget, hogy az OCSP profilt módosítsák.
Időbélyeg profil menedzsment	FMT_MOF_CWA.1 Időbélyeg profil menedzsment	A biztonsági adminisztrátorokra kell korlátozni azt a lehetőséget, hogy az időbélyeg profilt módosítsák.

5-6. táblázat: Jogosult szerepkörök a biztonsági funkciók viselkedésének kezelésére

FMT_MTD.1 TSF adatok kezelése (iteráció 2)

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

FMT_MTD.1.1 A TSF-nek a rendszervizsgálóra kell korlátoznia a naplóállományok megtekintését és törlését.

FMT_MSA.1 Biztonsági tulajdonságok kezelése

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[10] SFP-nek, azáltal, hogy a biztonsági adminisztrátorra korlátozza az alábbi biztonsági tulajdonságok módosítását: **[azonosító, szerepkör]**

FMT_MSA.2 Biztonságos biztonsági tulajdonságok

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

[10] melynek meghatározását lásd az 5.2.5.1 pontban

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[11] 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.

[11] melynek meghatározását lásd az 5.2.5.1 pontban

5.2.3 Mentés és helyreállítás

A mentés és helyreállítás magában foglalja egy rendszer helyreállítását rendszer hiba vagy más súlyos hiba esetén.

Abból a célból, hogy hiba vagy más váratlan nemkívánatos esemény után a rendszer vissza tudjon állni, a TOE-nak képeseknek kell lennie arra, hogy a rendszert lementsék. A mentést használják arra, hogy a TOE-t egy korábbi időpontban létező működőképes állapotba állítsák vissza. A mentések gyakorisága (pl. óránként, naponta vagy hetente) az alkalmazás vagy a rendszer kritikusságától függ.

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 A TSF-nek tartalmaznia kell egy mentés funkciót.

FDP_CIMC_BKP.1.2 A TSF-nek 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, kulcsolt lenyomat vagy hitelesítési kód 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 A TSF-nek 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, kulcsolt lenyomatok vagy hitelesítési kódok felhasználásával.

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

5.2.4 Archiválás

Az archiválás azt biztosítja, hogy a TSF biztosítsa az általa 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 A TSF-nek tartalmaznia kell egy archiválási funkciót.

FDP_CWA_ARC.1.2 A TSF-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.

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 A TSF-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.

5.2.5 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[12] SFP-nek, az alábbi szubjektumok és objektumok között, az alábbi műveletekre: **[az NCA rendszer minden sikeresen azonosított és hitelesített felhasználójára (szubjektumok), az NCA rendszer kliens oldali függvényeire és konzol parancsaira (objektumok) és a kliens oldali függvények és konzol parancsok végrehajtása (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[13] SFP-nek az objektumok vonatkozásában a szubjektum azonossága és a szubjektum által felvehető szerepkörök alapján.

FDP_ACF.1.2 A TSF-nek érvényre kell juttatnia az 5-7. 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].**

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.

[12] melynek meghatározását lásd az 5.2.5.1 pontban
[13] melynek meghatározását lásd az 5.2.5.1 pontban

5-7. táblázat: Hozzáférés ellenőrzések

Funkció	Összetevő	Esemény
Távoli és lokális tanúsítvány kérelem		A tanúsítvány iránti kérelem benyújtását a tisztviselőkre és az igényelt tanúsítvány alanyaira kell korlátozni.
Távoli és lokális tanúsítvány visszavonási kérelem		A tanúsítvány visszavonási kérelem benyújtását a tisztviselőkre és a visszavonandó tanúsítvány alanyaira kell korlátozni.
Adat export és output		A bizalmas és biztonság-kritikus adatok exportálása vagy outputja csak jogosult felhasználók kérésére történhet meg.
Kulcs generálás	FCS_CKM.1 Kriptográfiai kulcsok generálása	A komponens (infrastrukturális) kulcsok (amelyek olyan adatok védelmére szolgálnak, amelyet nem csak egy egyszeres munkaszakasznál vagy üzenetnél használnak) előállításának képességét a rendszeradminisztrátorokra kell korlátozni.
Magánkulcs betöltés		A komponens magánkulcsok kriptográfiai modulokba való betöltésének lehetőségét a rendszeradminisztrátorokra kell korlátozni.
Magánkulcs tárolás		A tanúsítvány alanyok magánkulcsainak dekódolási kérelmét a tisztviselőkre kell korlátozni. A TSF-nek nem szabad lehetőséget biztosítania digitális aláírás célú magánkulcsok dekódolására. A tanúsítvány alanyok magánkulcsainak dekódolását az érintett alanyra, illetve a kulcsvisszaállítási tisztviselőre kell korlátozni.
Megbízható nyilvános kulcs megadása, törlése és tárolása		A megbízható nyilvános kulcsok megváltoztatásának lehetőségét (hozzáadás, javítás, törlés) a rendszeradminisztrátorokra kell korlátozni.
Titkos kulcs tárolás		A TOE titkos kulcsainak kriptográfiai modulokba töltését a rendszeradminisztrátorokra kell korlátozni.
Magán és titkos kulcs megsemmisítés		A TOE nyílt formában lévő magán és titkos kulcsainak nullázását a rendszeradminisztrátorokra, a rendszervizsgálókra a tisztviselőkre és a rendszerüzemeltetőkre kell korlátozni.
Magán és titkos kulcs export		A rendszeradminisztrátorokra kell korlátozni azt a lehetőséget, hogy egy komponens magánkulcsot exportáljanak. A tisztviselőkre kell korlátozni azt a lehetőséget, hogy tanúsítvány alanyok magánkulcsait exportálják. A tanúsítvány alanyok magánkulcsainak exportjához legalább két tisztviselő általi feljogosítás szükséges.
Tanúsítvány állapot megváltoztatásának jóváhagyása[14]		Csak tisztviselő és az adott tanúsítvány alanyai kérhetik egy tanúsítvány felfüggesztését. Csak tisztviselők szüntethetik meg egy tanúsítvány felfüggesztési állapotát. Csak tisztviselők hagyhatnak jóvá egy tanúsítvány felfüggesztését. Csak tisztviselő és az adott tanúsítvány alanya kérheti egy tanúsítvány visszavonását. Csak tisztviselők hagyhatnak jóvá egy tanúsítvány visszavonást és a tanúsítvány visszavonásra vonatkozó információk nyújtását.

[14] Minden tanúsítvány állapot változtatási kérelmet (tanúsítvány visszavonási kérelem, tanúsítvány felfüggesztési kérelem, tanúsítvány felfüggesztésének megszüntetésére irányuló kérelem) jóvá kell hagyni, illetve el kell utasítani. Ha egy kérelem elfogadásra kerül, a kérelemre vonatkozó bármilyen, a TOE-ból exportálható információt jóvá kell hagyni. A jóváhagyás történhet manuális úton, vagy automatizáltan.

5.2.5.1 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, 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 jelen biztonsági előirányzatnak megfelelő kijelölése és kezelése.

5.2.6 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, **[nincs további biztonsági tulajdonság].**

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 Amennyiben a hitelesítést nem egy FIPS 140 szerint 2-es vagy magasabb szinten (a „szerepkörök és szolgáltatások" területén 3-as vagy magasabb szinten) tanúsított kriptográfiai modul hajtja végre, a TSF-nek észlelnie kell, amikor a rendszeradminisztrátor által konfigurálható „hitelesítési kísérletek maximális száma" 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 „hitelesítési kísérletek maximális száma"-ban megadott értéket, a TSF-nek az alábbiakat kell végrehajtania: **[egy rendszeradminisztrátor által konfigurálható „késleltetés" időtartamra le kell tiltania a következő hitelesítési kísérletet].**

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: **[a hitelesítés lehetséges módjának lekérdezése, „keresés a tanúsítványtárban", CRL lekérdezés, időbélyeg kérés, OCSP kérés]**

Megjegyzés: Az NCA rendszerben az időbélyeg és OCSP kérések konfigurálhatók úgy is, hogy azonosításhoz kötöttek. Ebben az esetben a FIA_UID.1.1-ben az „időbélyeg kérés" és az „OCSP kérés" nem szerepel.

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: **[a hitelesítés lehetséges módjának lekérdezése, „keresés a tanúsítványtárban", CRL lekérdezés, időbélyeg kérés, OCSP kérés, távoli tanúsítvány kérelem].**

Megjegyzés: Az NCA rendszerben az időbélyeg és OCSP kérések konfigurálhatók úgy is, hogy azonosításhoz kötöttek. Ebben az esetben a FIA_UAU.1.1-ben az „időbélyeg kérés" és az „OCSP kérés" nem szerepel.

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_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.

FIA_SOS.1 A titkok ellenőrzése

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs

Függések: nincs

FIA_SOS.1.1 A TSF-nek biztosítania kell egy mechanizmust, mely ellenőrzi, hogy a titkok megfelelnek-e a következő követelményeknek: **[a felhasználói jelszavaknak, a privilegizált felhasználók (ncasa, ncaroot, ncaop, ncaca, ncara, ncakr) jelszavainak, valamint az infrastrukturális kulcsok akivizálásához szükséges kulcs jelszavaknak meg kell felelniük a fenti három csoportra külön-külön konfigurálható, alábbi értékektől függő szabályoknak:**

- **a jelszó minimális hossza,**
- **a jelszó tartalmazzon-e legalább egy számot,**
- **a jelszó tartalmazzon-e legalább egy nagybetűt,**
- **a jelszó tartalmazzon-e legalább egy kisbetűt,**
- **a jelszó tartalmazzon-e legalább egy írásjelet,**
- **hány napig használható a jelszó,**
- **hány korábbi jelszóval nem egyezhet meg egy új jelszó.**

Mindhárom csoportra egységesen a TSF (CWA üzemmódjában) kikényszeríti legalább az alábbiakat:

- **legalább 6 hosszú jelszó,**
- **A négy csoportból (szám, nagybetű, kisbetű, írásjel) legalább kettő legyen megkövetelve.].**

5.2.7 Távoli adatmegadás és export

FCO_NRO_CIMC.3 Kötelező eredet bizonyítás és eredet ellenőrzés

Hierarchikus fölérendeltség más összetevőkhöz képest: FCO_NRO.2
Függések: FIA_UID.1 Az azonosítás időzítése

FCO_NRO_CIMC.3.1 A TSF-nek minden esetben érvényre kell juttatnia az eredet bizonyítékának generálását a tanúsítvány állapot információkra, valamint minden más biztonság-kritikus információ esetén.

FCO_NRO_CIMC.3.2 A TSF-nek képesnek kell lennie arra, hogy az azonosítót és **[*az információ létrehozójának tanúsítványát*]** összekapcsolja az információ létrehozójával, és az információ azon biztonság-kritikus részével, amelyre a bizonyíték vonatkozik.

FCO_NRO_CIMC.3.3 A TSF-nek minden biztonság-kritikus információ esetén ellenőriznie kell az információ eredetének bizonyítékát.

Megjegyzés: Az FCO_NRO_CIMC.3 alapján a TSF-nek vissza kell utasítania minden olyan információt, amelynek eredete nem ellenőrizhető, kivéve, ha:

a) Az információ elfogadása nem váltja ki azt, hogy a TSF valamilyen biztonság-kritikus funkciót hajtson végre; és
b) Az információ elfogadása nem váltja ki azt, hogy a TSF valamilyen bizalmas információt adjon ki vagy exportáljon.

A TSF elfogadhat például olyan információt, amelynek eredete nem ellenőrizhető, a következő esetekben:

a) A kapott információ egy nyilvános információk iránti kérelem (pl. egy OCSP kérelem).

b) A kapott információ nem lesz feldolgozva mindaddig, amíg egy jogosult felhasználó jóvá nem hagyja annak tartalmát (pl. egy tanúsítvány kérelem). Ebben az esetben a kapott információt úgy lehet feldolgozni, mintha attól a jogosult felhasználótól származna, aki azt jóváhagyta.

FCO_NRO_CIMC.4 Az eredet fokozott ellenőrzése

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FCO_NRO_CIMC.3 Kötelező eredet bizonyítás és eredet ellenőrzés

FCO_NRO_CIMC.4.1 A TSF a tanúsítvány alany által küldött kezdeti tanúsítvány regisztrálási üzenetek vonatkozásában csak azokat az üzeneteket fogadhatja el, amelyek egy hitelesítési kód, kulcsolt lenyomat vagy digitális aláírási algoritmus felhasználásával védve vannak.

FCO_NRO_CIMC.4.2 A TSF minden egyéb biztonság-kritikus információt csak akkor fogadhat el, ha az alá lett írva egy digitális aláírási algoritmus felhasználásával.

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 A TSF-nek érvényre kell juttatnia a CIMC TOE hozzáférés ellenőrzés szabályt[15], a biztonság-kritikus felhasználói adatok módosításának megakadályozása érdekében, a TOE fizikailag elkülönülő részei közötti átvitel közben.

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[16], a bizalmas felhasználói adatok felfedésének megakadályozása érdekében, a TOE 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 A TSF-nek az adatátvitel során védenie kell a módosítással szemben a biztonság-kritikus TSF adatokat, 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 felfedéssel szemben a bizalmas TSF adatokat, a TOE fizikailag elkülönülő részei közötti átvitel közben.

[15] melynek meghatározását lásd az 5.2.5.1 pontban
[16] melynek meghatározását lásd az 5.2.5.1 pontban

5.2.8 Kulcskezelés és kriptográfiai műveletek

A TOE különböző célokból használhat kriptográfiai kulcsokat: egy nem megbízható hálózaton keresztül küldött üzenetek sértetlenségének biztosítására, felhasználók hitelesítésére, magán információk bizalmasságának védelmére, vagy tárolt információk (pl. napló listák) bizalmasságának védelmére. Ezen kulcsok bármelyikének a jogosulatlan módosítása, felfedése vagy helyettesítése a biztonság elvesztését eredményezheti.

A kulcsoknak életciklusa van, amely a generálásukkal kezdődik. A generálás után a kulcsokat tárolják, aktiválják, deaktiválják és megsemmisítik. Sok esetben a kulcsokat mentik és naplózzák. A nyilvános kulcsok általában szétosztásra kerülnek. Bizonyos esetekben a magán és titkos kulcsok is szétosztásra kerülnek.

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 rövidtávú 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)

5.2.8.1 Magánkulcs tárolás

A TOE különböző célból használhat és tárolhat hosszú időre magánkulcsokat. A TOE tárolhat infrastrukturális, rendszervezérlési és (kulcsvisszaállítás céljából) végfelhasználói magán-kulcsokat.

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.

FMT_MTD_CIMC.4 A TSF magánkulcs bizalmasságának védelme

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FMT_MTD_CIMC.4.1 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.

5.2.8.2 Nyilvános kulcs tárolás

Ez az alfejezet olyan biztonsági követelményeket határoz meg, amelyeket a TOE-ban tárolt nyilvános kulcsok jogosulatlan módosításainak észlelésére terveztek.

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].**

5.2.8.3 Titkos kulcs tárolás

A TOE-ben különböző célokból használhatnak titkos (szimmetrikus) kulcsokat. Ezek alkalmazhatók más titkos vagy magánkulcsok titkosítására, amikor azok a TOE-n belül tárolásra kerülnek, vagy ha azokat a TOE-ból exportálják. Használhatók előfizetők (ügyfelek) és más TOE-k hitelesítésére is. A titkos kulcsokat védeni kell a jogosulatlan módosításokkal és felfedéssel szemben.

A tanúsítvány kérelmezőknek adható PIN vagy jelszó hitelesítő. Ezen hitelesítők generálása és a kérelmezők felé történő továbbítása kívül esik jelen biztonsági előirányzat hatókörén.

A következő követelmények kötelezőek, ha a TOE tárol titkos kulcsokat.

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.

FMT_MTD_CIMC.5 A TSF titkos kulcs bizalmasságának védelme

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs

FMT_MTD_CIMC.5.1 Azokat a TSF 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.

5.2.8.4 Magán és titkos kulcs megsemmisítés

Ez az alfejezet a TOE-n belül nyílt formában tárolt magán és titkos kulcsok nullázására/megsemmisítésére vonatkozó követelményeket határozza meg.

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 A TSF-nek lehetőséget kell biztosítania a FIPS 140 szerint tanúsított kriptográfiai modulon belül nyílt formában tárolt titkos és magán kulcsok nullázására.

A fenti összetevő egy kiterjesztett (CC 2. kötetben nem szereplő) követelményt határoz meg.

5.2.8.5 Magán és titkos kulcs export

Különféle okokból lehet kulcsokat exportálni a kriptográfiai modulokból, beleértve a kulcsok mentését, másolását és a TOE-ben generált végfelhasználói magánkulcsok továbbítását.

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.

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 A TSF 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.

5.2.8.6 Kriptográfiai műveletek

FCS_COP.1 Kriptográfiai eljárás (iteráció 2)

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 **szoftver** kriptográfiai modulnak a következő műveleteket: **[aláírás ellenőrzés, lenyomat generálás, lenyomat ellenőrzés]** olyan algoritmussal kell végrehajtania, amely megfelel a következőknek: **[FIPS PUB 186-2 – RSA (aláírás ellenőrzés), FIPS 180-2 - SHA1 (lenyomat generálás, lenyomat ellenőrzés)].**

5.2.9 Tanúsítvány profil menedzsment

Egy tanúsítvány profil meghatározza a tanúsítványokban előforduló mezőkre és kiterjesztésekre elfogadható értékek egy összességét. A tanúsítvány profilban megadható információkra példák az alábbiak:

- korlátozások a kulcs tulajdonosának azonosítójára (pl. az X.509-ben definiált subject és/vagy subjectAltName);
- az alany nyilvános/magán kulcspárjára alkalmazható megengedett algoritmusok;
- a tanúsítvány kibocsátójának azonosítója (pl. az X.509-ben definiált issuer és/vagy issuerAltName);
- a tanúsítvány érvényességi időtartamának hosszára vonatkozó korlátozások;
- további információk, amelyek belevehetők, illetve amelyeket bele kell venni egy tanúsítványba (pl. mely kiterjesztéseket lehet/kell egy X.509 tanúsítványba belevenni);
- a tanúsítvány alanya lehet-e egy CA;
- azon műveletek típusa, amelyeket végre lehet hajtani a tanúsítványban szereplő nyilvános kulcsnak megfelelő magán kulcs felhasználásával (pl. az X.509-ben definiált keyUsage és/vagy extKeyUsage lehetséges értékei);
- az(ok) a hitelesítési rend(ek), amely(ek) mellett a tanúsítványt ki lehet/kell adni.

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 adminisztrátor megadja 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 rendszeradminisztrátor megadja a következő mezőkre és kiterjesztésekre vonatkozó elfogadható értékek összességét:

- keyUsage;
- basicConstraints;
- certificatePolicies.

FMT_MOF_CIMC.3.4 A biztonsági adminisztrátornak meg kell adnia a tanúsítvány kiterjesztések elfogadható összességét.

5.2.10 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 biztonsági adminisztrátor 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 biztonsági adminisztrátornak meg kell adnia a tanúsítvány visszavonási listák és tanúsítvány visszavonási lista bejegyzés kiterjesztések elfogadható összességét.

5.2.11 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 Ha a TSF OCSP válaszokat bocsát ki, akkor 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 Ha a TSF OCSP válaszokat bocsát ki, akkor 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 Ha a TSF úgy van konfigurálva, hogy engedélyez alap-válasz típusú OCSP válaszokat, akkor a TSF-nek meg kell követelnie, hogy a biztonsági adminisztrátor megadja az alap-válasz típusban szereplő ResponderID mezőre vonatkozó elfogadható értékek összességét.

5.2.12 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.

5.2.13 Tanúsítvány regisztrálás

Az ebben az alfejezetben megadott funkciók a nyilvános kulcs tanúsítványok érvényesítésével, jóváhagyásával és aláírásával foglalkoznak.

A TOE által kibocsátott X.509 nyilvános kulcs tanúsítványoknak meg kell felelniük az X.509 szabványnak. Minden X.509 tanúsítványba kerülő mezőt és kiterjesztést vagy a TOE-nak kell előállítania az X.509 szabvány szabályainak megfelelően, vagy a TOE-nak érvényesítenie kell a megfelelés biztosítása céljából.

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 manuális úton.
2. Egy automatizált eljárás alkalmazható az adatok átvizsgálására és jóváhagyására.
3. A mező vagy kiterjesztés értékét generálhatja automatikusan a TOE.
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 kibocsátókra 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** bővítést.

h.) A **signature** mező és a **subjectPublicKeyInfo** mezőben szereplő **algorithm**-nak egy FIPS-által jóváhagyott algoritmus OID-jét kell tartalmaznia.

5.2.14 Visszavonás állapot

Ennek az alfejezetnek a funkciói a tanúsítvány visszavonási információk érvényesítésével és jóváhagyásával foglalkoznak.

5.2.14.1 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 esorozatából 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.

5.2.14.2 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 Ha a TSF úgy van konfigurálva, hogy engedélyez alap-válasz típusú OCSP válaszokat, akkor a TSF-nek ellenőriznie kell, hogy az OCSP alap-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.

5.2.14.3 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: X.509 szabvány, OCSP esetén: RFC 2560.

5.2.15 Időbélyegzés

Ez az alfejezet az időbélyegzés szolgáltatásra vonatkozó követelményekkel foglalkozik.

A TOE által kiadott időbélyeg válaszoknak meg kell felelniük az IETF RFC 3161-nek. Egy időbélyeg válaszban 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.

5.3 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 5-8. 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

5-8. 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 NCA rendszer v2.6.0 biztonsági követelményeit teljesítő biztonsági funkciókat tartalmazza. Leírja az NCA rendszer összes biztonsági funkcióját és garanciális intézkedését, amelyek az NCA rendszer biztonsági követelményeinek a kielégítéséhez járulnak hozzá.

6.1 A TOE biztonsági funkciói

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

Általános (szolgáltatásoktól független) biztonsági funkciók:

- BF1: Bizalmi munkakörök kezelése
- BF2: Időszinkronizálás
- BF3: Azonosítás és hitelesítés
- BF4: Hozzáférés ellenőrzés
- BF5: Kulcskezelés és kriptográfiai műveletek
- BF6: Biztonsági naplózás
- BF7: Mentés és helyreállítás
- BF8: Archiválás

Az egyes szolgáltatásokra vonatkozó biztonsági funkciók

- BF9: Távoli adatbevitel és export
- BF10: Tanúsítvány előállítás
- BF11: Visszavonás kezelés
- BF12: Visszavonás állapot
- BF13: 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.

6.1.1.1 Az NCA jogosultság kezelése

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

- **Biztonsági adminisztrátor (ncasa)**: az a személy, aki új felhasználó létrehozásakor hozzárendelheti a felhasználót az egyes munkakörökhöz (s ezzel a felhasználói fiókhoz jogosultságokat rendelhet), valamint meghatározhatja a különböző (tanúsítvány-, CRL-, OCSP- és időbélyeg-) profilokat. Nincs semmilyen operatív üzemeltetési jogosultsága.
- **Rendszeradminisztrátor (ncaroot)**: az NCA rendszer telepítésére, konfigurálására (a profilok meghatározásán kívül) és karbantartására feljogosított személy. Nincs semmilyen operatív üzemeltetési jogosultsága.
- **Rendszerüzemeltető (ncaop)**: az NCA rendszer mindennapos működéséért felelős személy, aki az NCA rendszer elindítására és leállítására, valamint kézi mentésére és helyreállítására is fel van hatalmazva.
- **Rendszervizsgáló (ncaau):** az NCA rendszer naplóinak (naplóállományok és adatbázis rekordok) karbantartására (olvasására, keresések végrehajtására), valamint az archívumok megtekintésére feljogosított személy. Nincs semmilyen operatív üzemeltetési jogosultsága.
- **Tisztviselő (ncara, ncaca, ncakr)**: a végfelhasználói tanúsítványok előállításának, visszavonásának, felfüggesztésének és visszaállításának a jóváhagyásáért felelős személyek. Ez a munkakör az alábbi al-munkakörre bomlik:
    - Előkészítő regisztrációs tisztviselő (ncara) /előkészítést végző, előtanúsítványt jóváhagyó/,
    - Jóváhagyó regisztrációs tisztviselő (ncaca) /tanúsítvány kiadást jóváhagyó/.
    - Kulcsvisszaállítási tisztviselő (ncakr) /kizárólag az NCA rendszer PKI üzemmódjában értelmezett munkakör, melyet betöltő személy az alábbiakra jogosult:
        - titkosító magánkulcs letétbe helyezési kérelmének jóváhagyása és közvetítése,
        - titkosító magánkulcs (más hitelesítés-szolgáltató felé történő) exportálás kezdeményezése, külső letétbe helyezés céljából,
        - titkosító magánkulcs visszaállítási kérelmének jóváhagyása és közvetítése./
- **GSU (gsu):** speciális aláírásokat kívülről kezdeményező külső felhasználó (személy vagy automatizmus). A GSU jogosultsága a viszontazonosítás válaszok aláírásának kezdeményezése.
- **Ügyfél (ncauser):** azonosított végfelhasználó. Azonosításhoz kötött szolgáltatásokat (tanúsítvány igénylés, felfüggesztési kérelem, visszavonási kérelem, kulcsvisszaállítási kérelem, …) vehet az NCA rendszerben igénybe.
- **Érintett fél (anonymous):** nem azonosított végfelhasználó. Azonosításhoz nem kötött szolgáltatásokat (teszt tanúsítvány igénylést, tanúsítványtárban való keresést, továbbá ilyen irányú konfigurálás esetén időbélyeg kérést és OCSP kérést is) vehet az NCA rendszerben igénybe.

Az NCA rendszer képes a felhasználókat összekapcsolni a fenti munkakörökkel.

Az NCA rendszer biztosítja az alábbiakat is:

- egy tisztviselő munkakört betöltő felhasználó nem lehet rendszervizsgáló,
- egy biztonsági adminisztrátori vagy rendszeradminisztrátori munkakört betöltő felhasználó nem kaphat tisztviselői vagy rendszervizsgálói jogokat.

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

6.1.1.2 A környezet támogatása

Az IT környezet (operációs rendszer szinten) az alábbiak biztosításával támogatja a bizalmi munkakörök kezelését (jogosultság kezelést): a Rendszeradminisztrátor, a Rendszerüzemeltető és a Rendszervizsgáló munkakörök megkülönböztetése, kielégítve ezzel a következő SFR-eket: *FMT_SMF.1 (iteráció 1), FMT_SMR.2 (iteráció 1), FMT_MOF.1 (iteráció 1)* és *FMT_MTD.1 (iteráció 1).*

6.1.2 BF2: Időszinkronizálás

Ennek a biztonsági funkciónak a célja az üzembiztos és pontos idő garantálása az NCA rendszer időkritikus szolgáltatásaihoz.

6.1.2.1 Az NCA időszinkronizálása

Az NCA 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.

Az NCA rendszer ellenőrzi, hogy a maximális eltérés a konfigurálható határon belül van-e. Ha belül van, akkor az NCA rendszer ezt a rendszeridőt elfogadja, s ezt használja minden időfüggő szolgáltatásához. Ellenkező esetben az NCA rendszer ezt naplózza és leállít minden időkritikus hitelesítés-szolgáltatást (tanúsítvány előállítás, időbélyegzés, visszavonás állapot szolgáltatás).

Ez a biztonsági funkció a következő SFR kielégítésére irányul: **FPT_STM.1 (iteráció 2).**

6.1.2.2 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)*

6.1.3 BF3: Azonosítás és hitelesítés

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

Az alábbi biztonsági alfunkciókból áll:

- BF3.1 A felhasználó hitelesítése
- BF3.2 A hitelesítési hiba kezelése
- BF3.3 A titok ellenőrzése

6.1.3.1 A felhasználó hitelesítése

Az NCA rendszer egyes szolgáltatásait azonosítás nélkül mindenki számára elérhetővé teszi. Ezek a szolgáltatások az alábbiak:

- keresés a tanúsítvány tárban,
- CRL letöltés,
- időbélyeg kérés (konfigurációtól függően),
- OCSP kérés (konfigurációtól függően)

Az NCA rendszer a fenti szolgáltatások (függvények) kivételével, minden felhasználótól 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. (Konfigurációtól függően az azonosítás és hitelesítés kötelező elvárása vonatkozik az időbélyeg és OCSP kérésekre is.)

Az NCA rendszer az **Ügyfél** azonosítását és hitelesítését az alábbi módon végzi:

- az azonosítás és hitelesítés kliens oldali parancsokkal valósul meg,
- ncaroot minden ügyfél számára egyedileg beállíthatja a hitelesítés típusát (authtype), az alábbiak szerint:
  - 'd' :letiltott,
  - '0': jogosultság nélkül,
  - 'p': jelszavas,
  - 'c': tanúsítvány alapú,
  - 'a': jelszó és tanúsítvány alapú,
  - 'o': csak jelszócserére jogosító belépés,
- ncaroot az ügyfelek számára közösen beállíthatja a jelszavakra vonatkozó szabályhalmazt (UserPwdType és UserPwdReuse), az alábbiak szerint:
  - hány napig használható a jelszó,
  - hány korábbi jelszóval nem egyezhet meg egy új jelszó,
  - jelszó hosszra és jelkészletre vonatkozó szabályok
- mindig az ügyfél kezdeményezi a kapcsolatfelvételt,
- az ügyfél számára beállított „authtype” értékétől függően:
  - az Ügyfélnek meg kell adnia a regisztráció során kapott azonosítóját és jelszavát, majd meg kell adnia egy új jelszót (authtype: o),
  - az Ügyfélnek meg kell adnia a regisztráció során megadott azonosítóját és az ehhez tartozó érvényes jelszavát: (authtype: p),
  - az Ügyfélnek a szervertől kapott challenge-t, valamint ennek magánkulcsával kódolt képét kell visszaküldenie (authtype: c),
  - az Ügyfél mind jelszó, mind tanúsítvány alapú hitelesítést alkalmazhat (authtype: a),

- az ügyfél számára beállított „authtype” értékétől függően:
    - bejelentkezése sikertelen lesz, függetlenül a hitelesítés eredményétől (authtype: d),

Az NCA rendszer a **Biztonsági adminisztrátor, Rendszeradminisztrátor, Rendszerüzemeltető, Rendszervizsgáló, Tisztviselő** és **GSU** megbízható munkaköröket betöltő személyek azonosítását és hitelesítését az alábbi módon végzi:

- az azonosítás és hitelesítés kliens oldali parancsokkal, vagy szerver oldalon (operációs rendszerből) hívható konzol parancsokkal valósul meg, mindkét esetben az alábbi azonos szabályokkal:
- ncaroot minden érintett privilegizált felhasználó számára egyedileg beállíthatja a hitelesítés lehetőségét (authtype), az alábbiak szerint:
    - 'd' :letiltott,
    - '0': jogosultság nélkül,
    - 'p': jelszavas,
    - 'c': tanúsítvány alapú,
    - 'a': jelszó és tanúsítvány alapú,
    - 'o': csak jelszócserére jogosító belépés.
- ncaroot minden érintett privilegizált felhasználó számára közösen beállíthatja a jelszavakra vonatkozó szabályhalmazt (AdminPwdType és UserPwdReuse), az alábbiak szerint:
    - hány napig használható a jelszó,
    - hány korábbi jelszóval nem egyezhet meg egy új jelszó,
    - jelszó hosszra és jelkészletre vonatkozó szabályok
- mindig az érintett privilegizált felhasználó kezdeményezi a kapcsolatfelvételt,
- az érintett privilegizált felhasználó számára beállított „authtype” értékétől függően:
    - az érintett privilegizált felhasználónak meg kell adnia a regisztráció során kapott azonosítóját és jelszavát, majd meg kell adnia egy új jelszót (authtype: o),
    - az érintett privilegizált felhasználónak meg kell adnia a regisztráció során megadott azonosítóját és az ehhez tartozó érvényes jelszavát: (authtype: p),
    - az érintett privilegizált felhasználónak a szervertől kapott challenge-t, valamint ennek magánkulcsával kódolt képét kell visszaküldenie (authtype: c),
    - az érintett privilegizált felhasználó mind jelszó, mind tanúsítvány alapú hitelesítést alkalmazhat (authtype: a),
- az érintett privilegizált felhasználó számára beállított „authtype” értékétől függően:
    - bejelentkezése sikertelen lesz, függetlenül a hitelesítés eredményétől (authtype: d),

Az NCA rendszerben minden felhasználó számára kötelező az újrahitelesítés kijelentkezése, vagy a session automatikus lezárása után, illetve új szerepkörben való ismételt bejelentkezés esetén.

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

6.1.3.2 A hitelesítési hiba kezelése

Az NCA rendszer megnehezíti a további hitelesítési kísérleteket, ha a sikertelen hitelesítési kísérletek száma elér vagy meghalad egy maximumként meghatározott értéket. ncaroot minden felhasználó számára egységesen beállíthatja a hitelesítésekre vonatkozó alábbi szabályhalmazt:

- (büntetés nélküli) bejelentkezési próbálkozások maximális száma (LoginAttemptNum),
- LoginAttemptNum darab sikertelen kísérlet utáni várakozási idő a bejelentkezések között (LoginAttemptTMO, sec),
- tanúsítvány alapú hitelesítés esetén a válaszra várás maximális ideje, mely után a rendszer sikertelennek nyilvánítja a kísérletet (AuthSessionTMO, sec).

Ez a biztonsági alfunkció a következő SFR-ek kielégítésére irányul: **FIA_AFL.1 (iteráció 2).**

6.1.3.3 A titok ellenőrzése

Az NCA rendszer egy mechanizmust biztosít annak ellenőrzésére, hogy a jelszó alapú hitelesítésben használt titkok (jelszavak) megfelelnek-e az erre meghatározott követelményeknek. ncaroot külön az ügyfelek, illetve külön a bizalmi munkakört betöltő személyek (privilegizált felhasználók) számára beállíthatja a jelszavakra vonatkozó szabályhalmazt (UserPwdType és UserPwdReuse, AdminPwdType és AdminPwdReuse), az alábbiak szerint:

- hány napig használható a jelszó,
- hány korábbi jelszóval nem egyezhet meg egy új jelszó,
- jelszó hosszra és jelkészletre vonatkozó szabályok.

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

6.1.3.4 A környezet támogatása

Az azonosítás és hitelesítés biztonsági funkciót teljes egészében az NCA rendszer valósítja meg (az IT környezet támogatása nélkül).

6.1.4 BF4: Hozzáférés ellenőrzés

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

6.1.4.1 Az NCA rendszer hozzáférés ellenőrzése

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

Nem azonosított felhasználóknak kizárólag az alábbi hozzáféréseket engedélyezi:

- keresés a tanúsítvány tárban,
- időbélyeg kérés,
- CRL lekérések,
- OCSP kérés.

Az azonosított és hitelesített felhasználóknak az általuk betöltött szerepkör alapján kizárólag az alábbi hozzáféréseket engedélyezi:

Munkakör	**Engedélyezett tevékenység**
Biztonsági adminisztrátor (ncasa)	felhasználói account-hoz jogosultságok rendelése, tanúsítvány, CRL, OCSP és TS profil kezelése
Rendszeradminisztrátor (ncaroot)	telepítés, konfigurálás, karbantartás (mentett naplóállományok, naplórekordok, időbélyeg és OCSP kérések/válaszok archiválásának kezdeményezése, mely egyben az archivált adatok rendszerből való törlését is okozza)
Rendszerüzemeltető (ncaop)	NCA rendszer elindítása, leállítása, kézi mentés végrehajtása, helyreállítás végrehajtása
Rendszervizsgáló (ncaau)	Naplóállomány olvasása, Naplóállományban keresések végrehajtása, Napló adatbázis olvasása, Napló adatbázisban keresések végrehajtása
Előkészítő regisztrációs tisztviselő (ncara)	Előtanúsítvány jóváhagyása, Tanúsítvány kérelem elkészítése, felfüggesztés jóváhagyása, visszavonás jóváhagyása
Jóváhagyó regisztrációs tisztviselő (ncaca)	tanúsítvány kiadás jóváhagyása, felfüggesztés jóváhagyása, visszavonás jóváhagyása, manuális CRL kiadás kezdeményezése
Kulcsvisszaállítási tisztviselő (ncakr) /csak PKImod=1 üzemmódban/	titkosító magánkulcs letétbe helyezési kérelmének jóváhagyása és közvetítése, titkosító magánkulcsok visszaállítás kérelmének jóváhagyása, titkosító magánkulcsok visszaállítás végrehajtása, titkosító magánkulcs exportálás végrehajtása
GSU (gsu)	viszontazonosítás válaszok aláírásának kezdeményezése
Ügyfél (ncauser)	tanúsítvány igénylés, felfüggesztési kérelem, visszavonási kérelem, kulcsvisszaállítási kérelem

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)**

6.1.4.2 A környezet támogatása

Az IT környezet (operációs rendszer szinten) az alábbiak biztosításával támogatja a hozzáférés ellenőrzést:

- Az operációs rendszer egy olyan biztonsági tartományt biztosít az NCA rendszer számára, ami megvédi azt a nem megbízható egyedek általi beavatkozástól és hamisítástól (futás közben) /*FPT_SEP.1*/.

A nem-IT környezet (a munkakör beosztások kialakításánál) az alábbiak biztosításával támogatja a hozzáférés ellenőrzést:

- Az NCA rendszer rendszervizsgálója egyúttal az (alapot képező) operációs rendszer naplóinak ellenőrzésére (áttekintésére) és karbantartására (archiválására és ezt követő törlésére) is jogosult.
- Az NCA rendszer rendszervizsgálója egyúttal az (érintett) tűzfalak, és behatolásjelzők naplóinak ellenőrzésére (áttekintésére) és karbantartására (archiválására és ezt követő törlésére) is jogosult.

6.1.5 BF5: Kulcskezelés és kriptográfiai műveletek

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

Az alábbi biztonsági alfunkciókból áll:

- BF5.1: NCA magánkulcs exportálása HSM-ből, helyreállítása (HSM-be)
- BF5.2: Titkosító magánkulcsok exportálása
- BF5.3: Kriptográfiai műveletek végzése
- BF5.4: Nyilvános kulcsok védelme

Az NCA 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 NCA rendszer.
- **infrastrukturális kulcsok** – az NCA rendszer által az alábbi folyamatokhoz használt kulcsok: tanúsítvány állapot válaszok aláírása, napló állományok és naplórekordok aláírása, konfigurációs állományok aláírása, időbélyeg válaszok aláírása, RA-CA kommunikáció titkosítása, titkosító magánkulcsok letétbe helyezése és helyreállítása.
- **rendszervezérlési kulcsok** – az NCA rendszer bizalmas munkakört betöltő felhasználói által használt kulcsok, melyek hitelesítési-, aláírási- vagy bizalmassági szolgáltatásokat biztosítanak.
- **végfelhasználói kulcsok** - az NCA rendszer által (a HSM-ben) az ügyfelek számára előállított titkosító kulcspárok.

6.1.5.1 Az NCA magánkulcs exportálása (HSM-ből), helyreállítása (HSM-be)

Az IT környezet részét képező kriptográfiai hardver eszközben (HSM) tárolt tanúsítvány aláíró magánkulcs exportálása az NCA rendszer aktív közreműködésével történik. Az NCA rendszer (CRYPTO alrendszere) végzi a titkosított formában történő magánkulcs exportálás vezérlését, majd „n-ből m" technika segítségével történő titokmegosztását, intelligens kártyákra töltését. Helyreállítás esetén szintén az NCA rendszer (CRYPTO alrendszere) végzi a titokmegosztással tárolt magánkulcs töredékek beolvasását (m darabot, az intelligens kártyákról), helyreállítását, majd a helyreállított (de a HSM által titkosított) magánkulcs HSM-be töltését.

Ez a biztonsági alfunkció a következő SFR kielégítésére irányul: **FMT_MTD_CIMC.7.**

6.1.5.2 Titkosító magánkulcsok kezelése

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

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

Ez a biztonsági alfunkció a következő SFR-ek kielégítésére irányul: **FMT_MTD_CIMC.4, FMT_MTD_CIMC.5, FDP_ETC_CIMC.5, FDP_ACF_CIMC.2.**

6.1.5.3 Felhasználói titkos kulcsok kezelése

Felhasználói szimmetrikus kulcsok is csak titkosítva kerülhetnek ki a HSM-ből.

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

6.1.5.4 Kriptográfiai műveletek végzése

Az NCA rendszer az alábbi kriptográfiai műveleteket végezheti (az IT környezet támogatása nélküli szoftveres megvalósítással):

- lenyomat számítás (nem igényel kulcsot),
- digitális aláírás ellenőrzése (csak nyilvános kulcs felhasználását igényli),
- a kliens (NCACLI) és a szerver (NCAADM) közötti protokollban továbbított adatok titkosítása a kliens oldalon (SeCh rövidtávú szimmetrikus kulcs felhasználásával).

Az NCA rendszer nem generál titkos vagy magánkulcsot.

Az NCA rendszer végzi viszont a (titkos formában tárolt) titkosító magánkulcsok törlését (PKI üzemmódban).

Ez a biztonsági alfunkció a következő SFR-ek kielégítésére irányul: **FCS_COP.1 (iteráció 2), FCS_CKM_CIMC.5.**

6.1.5.5 A nyilvános kulcsok védelme

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

Az NCA az adatbázisban tárolt minden végfelhasználói nyilvános kulcs sértetlenségét ellenőrzi minden esetben, amikor a szóbanforgó nyilvános kulcs olvasása történik. Ha az ellenőrzés nem sikeres, a hívó függvény hibajelzéssel tér vissza, illetve egy hibajelzés a naplóállományban is rögzítésre kerül.

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

6.1.5.6 A környezet kriptográfiai 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, illetve a megbízható munkaköröket betöltő felhasználók intelligens kártyáik végzik a titkos és magánkulcsok megsemmisítésének döntő többségét /*FCS_CKM.4*/,
- 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 (iteráció 1)*/.

6.1.6 BF6: 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 biztosítása.

Az alábbi biztonsági alfunkciókból áll:

- BF6.1: Napló adatok generálása megfelelő adatokkal
- BF6.2: A napló adatok rendelkezésre állásának biztosítása (az elvesztés megakadályozása)
- BF6.3: A naplózandó adatok kiválasztása
- BF6.4: A napló választható áttekintése
- BF6.5 Korlátozott naplómegtekintés
- BF6.6: Riasztás generálása
- BF6.7 A napló adatok sértetlenségének garantálása

6.1.6.1 Napló adatok generálása megfelelő adatokkal

Az NCA v2.6.0 naplózza mindazokat az eseményeket is, amelyek az 5-4. 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, hogy a valós helyzetek megítéléséhez a szükséges mértékben, a hitelesítés-szolgáltatással kapcsolatos minden eseményt rekonstruálni lehessen.

Minden napló esemény magában foglalja a következő információkat:

- az esemény dátuma /pontosabban minden órában az órajelzés naplózódik, amelyben a dátum (éééé.hh.nn) formátumban, a helyi idő és az UTC idő együtt kerül megadásra (pl. ===== 2005.05.18. 09:00:01 (LOCAL)/2005.05.18. 07:00:01 (UTC) =====), s ebből egyértelműsíthető minden naplóesemény dátuma/,
- az esemény időpontja /[óó:pp:mm]formátumú, helyi időben megadott időjelzéssel/,
- az esemény típusa /(i): információ, (w): figyelmeztetés, (E): hiba, (c): klienstől érkezett naplózandó adatok, (S): aláírás, (D): debug (m): karbantartás /,
- szubjektum azonosító /pontosabban minden olyan naplóbejegyzés esetén, melynek kiváltásában (akár külső, akár privilegizált jogosultságokkal rendelkező belső) felhasználó működött közre, a felhasználó NCA rendszerben használt azonosítója is rögzítésre kerül (pl. (i)[10:53:20]-[14096]-User [lovaszne] authenticated, session [RgIR6KXsYacbh_R4gC] registered)/
- az esemény kimenetele (siker vagy sikertelenség) /pontosabban az esemény típusa „E”-vel jelöli a sikertelenséget, minden más eset sikerességre utal/.

Annak következtében, hogy minden olyan naplóesemény, melynek kiváltásában felhasználó működött közre, egyértelműen össze van kapcsolva ennek a felhasználónak az NCA rendszerben használt azonosítójával, a felhasználók utólag felelősségre vonhatók cselekedeteikért.

Az összes naplóbejegyzés naplófájlokban tárolásra kerül. A gyakran keresett, adatbázisban tárolásra optimalizálható naplóbejegyzések ezen kívül adatbázisba is kerülnek.

A napló (sem a naplóállomány, sem az adatbázisba került naplórekordok) nem tartalmaz nyílt formában magán, vagy titkos kulcsot, illetve olyan egyéb biztonsági paramétert, melynek illetéktelen megismerése biztonságilag kritikus lenne.

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

6.1.6.2 A napló adatok rendelkezésre állásának biztosítása (az elvesztés megakadályozása)

Az NCA rendszerben a napló eseménysor sohasem telik meg, mivel új aktuális naplóállomány kerül létrehozásra minden esetben, amikor az aktuális naplóállomány elér egy (konfigurálható módon) meghatározott méretet.

Az NCA rendszerben a naplóbejegyzések sohasem kerülnek automatikusan felülírásra, mivel az aktuális naplóállomány mindig folyamatosan töltődik, a mentett állományok pedig mindig különböző nevet kapnak.

A lementett naplóállományok automatikusan archiválhatók annak érdekében, hogy a lokális merevlemez ne teljen be.

Ha mégsincs hely az aktuális naplóállománynak akkor a naplózható eseményt létrehozó szolgáltatás leáll, meggátolva ezzel bármely naplózható esemény létrejöttét.

Ez a biztonsági alfunkció a következő SFR kielégítésére irányul: **FAU_STG.4 (iteráció 2)**

6.1.6.3 A napló adatok kiválasztása

Az NCA rendszer nem biztosít lehetőséget a naplózási funkció elindítására és leállítására a hitelesítési szolgáltatástól függetlenül, de a naplózási funkció elindul és leáll minden esetben, amikor az NCA rendszer elindul és leáll, és ez utóbbi két esemény naplózásra kerül.

Az NCA rendszer minden naplózható esemény esetében létrehoz (legalább) egy naplóbejegyzést. Ezenkívül szabályozható, hogy mely szerver oldalon meghívott függvényekről, s ezen belül milyen szerepkörből történő meghívásuk esetén legyen naplóbejegyzés.

Ez a biztonsági alfunkció a következő SFR kielégítésére irányul: **FAU_SEL.1 (iteráció 2).**

6.1.6.4 A napló választható áttekintése

Az NCA rendszer a napló olvasására jogosultak számára áttekinthető és értelmezhető formában megjeleníti a naplóállományokat.

Az NCA rendszer a napló bejegyzések közül a gyakran keresett és adatbázisban tárolásra optimalizálható adatokat adatbázisban is tárolja. Ezek (könnyen áttekinthető és értelmezhető formában történő) megjelenítését, valamint az alábbi szempontok szerinti szűrését lehetővé teszi az erre feljogosított felhasználók számára: keresési lehetőség az esemény időpontja, típusa és/vagy a felhasználó személye szerint.

Ez a biztonsági alfunkció a következő SFR-ek kielégítésére irányul: **FAU_SAR.1 (iteráció 2), FAU_SAR.3 (iteráció 2).**

6.1.6.5 Korlátozott naplómegtekintés

Az NCA rendszer a naplóállományok megtekintését (olvasását), illetve az ebben való keresést a rendszervizsgáló számára teszi csak lehetővé.

Ez a biztonsági alfunkció a következő SFR-ek kielégítésére irányul: **FAU_SAR.1 (iteráció 2), FAU_SAR.3 (iteráció 2)**

6.1.6.6 Riasztás generálása

Az NCA rendszer minősített üzemmódban riasztást generál (a rendszeradminisztrátor számára) a biztonság potenciális megsértésének észlelése esetén, abban az esetben ha az ncasa, ncaroot, ncaop, ncaau, ncara, ncaca vagy ncakr szerepkörökben legalább LoginAttempNUM db egymást követő sikertelen hitelesítési kísérlet történt. A riasztás a következő: az NCA rendszer egy konfigurációban megadható címen, http(s) protokollon meg tud hívni egy olyan eljárást, mely levelet küldhet a megfelelő címzetteknek.

Ez a biztonsági alfunkció a következő SFR-ek kielégítésére irányul: **FAU_SAA.1, FAU_ARP.1.**

6.1.6.7 A napló adatok sértetlenségének garantálása

Az NCA rendszer minden naplóeseményt naplóállományokban tárol. Három különböző naplóállomány különböztethető meg: aktuális, mentett és archivált. Az aktuális az éppen írás alatt lévő, a mentettek azok, melyeket már lezárt a rendszer, de még tárol, az archiváltak pedig azok, melyeket a rendszer már lezárt, külső adathordozóra archivált, tovább már nem tárol.

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

- Minden naplóállomány (a naplóeseményeken kívül) tartalmaz egy napló fejlécet is, amely információkat tartalmaz a fájlban található naplóadatokról.
- Az NCA rendszer az aktuális naplóállomány integritását folyamatos, memóriában tárolt lenyomat értékkel biztosítja, az integritást konfigurációban megadható (CheckLogFileTMO) paraméter által meghatározott időközönként automatikusan ellenőrzi. Az aktuális naplóállomány integritásának sérülése esetén a rendszer leáll.
- Az NCA rendszer új naplóállomány megkezdése előtt, illetve szabályos leálláskor az éppen befejezett aktuális fájl integritásának ellenőrzése után a naplófájlt időjelzéssel látja el, majd infrastrukturális kulccsal aláírja.
- Az NCA rendszer a mentett naplóállományok integritását az elektronikus aláírásaik alapján a konfigurációban megadható (CheckLogArchTMO) paraméter által meghatározott időközönként automatikusan ellenőrzi. Egy mentett naplóállomány integritásának sérülése esetén a rendszer a sérülés tényéről naplóbejegyzést készít az aktuális naplóállományba.
- Az NCA rendszer a napló adatbázis táblát (a még nem archivált, adatbázisba szervezett naplórekordok összességét) rekordonként infrastrukturális kulccsal aláírja, s ezeket az aláírásokat, tehát a rekordok sértetlenségét külön-külön ellenőrzi.
- A kezelt (még nem archivált) naplóállományokat az NCA rendszer nyilvántartja a logarch.hea állományban, s a rendszeres ellenőrzések során a hiányzókról, valamint a nem nyilvántartottakról naplóbejegyzést készít az aktuális naplófájlba.

Ez a biztonsági alfunkció a következő SFR-ek kielégítésére irányul: **FAU_STG.1 (iteráció 2), FPT_CIMC_TSP.1.**

6.1.6.8 A környezet támogatása

Az IT környezet (operációs rendszer szinten) az alábbiak biztosításával támogatja a naplózást:

- a TOE napló (operációs rendszer szinten megvalósított) törlése is naplózásra kerül /*FAU_GEN.1 (iteráció 1)*/,
- a TOE napló (operációs rendszer szinten megvalósított) esetleges törlésének naplóeseményéből egyértelműen következtetni lehet a törlést kiváltó felhasználóra /*FAU_GEN.2 (iteráció 1*)/,
- a rendszervizsgálók a naplórekordokból kikereshetik és kiolvashatják a TOE (naplófájlban és adatbázisban tárolt) naplóbejegyzéseinek az esetleges törlésére vonatkozó információkat /*FAU_SEL.1 (iteráció 1), FAU_SAR.1 (iteráció 1)* **és** *FAU_SAR.3 (iteráció 1)*/,
- az IT környezet független időforrások biztosításával támogatja a megbízható időpont előállítását /*FPT_STM.1 (1. iteráció*)/.

6.1.7 BF7: Mentés és helyreállítás

Ennek az összetett biztonsági funkciónak a célja az üzemmenet folytonosságának és az adatvesztés elkerülésének a biztosítása, rendszeres mentések elvégezhetőségével, illetve az informatikai rendszer egészének szükség esetén megvalósítható helyreállításával.

Az alábbi biztonsági alfunkciókból áll:

- BF7.1 Mentés generálása
- BF7.2 A mentési információ sértetlenségének és bizalmasságának biztosítása
- BF7.3 Helyreállítás

6.1.7.1 Mentés generálása

Az NCA rendszer egy mentési funkciót biztosít, mely:

- konfigurálható időpontban (BUConfig) automatikus mentést végez,
- konfigurálható időközönként (BUConfig) automatikus mentést végez,
- a mentési állományokat konfigurálható (BUConfig) helyre teszi,
- lehetőséget biztosít az erre jogosult rendszerüzemeltetőnek, hogy konzol parancs segítségével szükség esetén mentést végezhessen.

Az NCA rendszer mentésében tárolt adatok elegendőek a rendszer állapotának visszaállítására:

- az összes adatbázistábla, konfigurációs, futtatható és egyéb rendszervezérlési állományok kerülnek mentésre, a mentési pillanatban érvényes állapotukban,
- mentésre kerül az összes kiadott időbélyeg, OCSP-válasz, tanúsítványkérés-válasz és CRL is.

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

6.1.7.2 A mentési információ sértetlenségének és bizalmasságának biztosítása

Az NCA rendszer digitális aláírás alkalmazásával védi a mentést.

Az NCA rendszer mentése nem tartalmaz nyílt formában kritikus biztonsági paramétereket.

Ez a biztonsági alfunkció a következő SFR kielégítésére irányul: **FDP_CIMC_BKP.2.**

6.1.7.3 Helyreállítás

Az NCA rendszer egy helyreállítási funkciót biztosít, mely képes egy mentésből helyreállítani a rendszert. A visszaállítási funkció segítségével az NCA rendszer egy olyan, a mentés időpontja alattival "egyenértékű" állapota áll elő, mely kezelni képes az NCA rendszer valamennyi lényeges tranzakciójára vonatkozó információt is.

A helyreállítási funkciót az erre feljogosított, rendszerüzemeltető szerepkört betöltő felhasználó hívhatja meg.

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

6.1.7.4 A környezet támogatása

A mentés és helyreállítás biztonsági funkciót teljes egészében az NCA rendszer valósítja meg (a környezet támogatása nélkül).

6.1.8 BF8: Archiválás

Ennek az összetett biztonsági funkciónak a célja annak biztosítása, hogy a hosszú távon megőrzendő, de a napi működéshez nem feltétlenül szükséges információk ne terheljék feleslegesen az erőforrásokat, ám bármikor visszakereshetőek legyenek a rendszer felügyelete alól kivett (archivált) adatállományokban tárolt adatok, egyúttal az archivált adatok sértetlensége, s ahol ez szükséges, a bizalmassága is védve legyen.

Az alábbi biztonsági alfunkciókból áll:

- BF8.1 Archív adatok generálása
- BF8.2 Szelektálható keresés az archivált adatok között
- BF8.3 Az archivált adatok sértetlenségének és bizalmasságának biztosítása

6.1.8.1 Archív adatok generálása

Az NCA rendszer egy archiválási funkciót biztosít, mely az alábbi adatok archiválására használható:

- minden tanúsítvány,
- minden CRL,
- minden időbélyeg token (kiadott időbélyeg válasz),
- minden OCSP válasz,
- minden GSU által kért aláírás (köztük a viszontazonosítás válaszok),
- minden naplóállomány (A rendszer automatikusan elmenti a befejezett naplóállományokat, ha a konfigurációban ez így van beállítva /ArchivateLogFile/. A befejezett naplóállományok mentési helye szabadon konfigurálható /LogArea/.)

Minden archivált bejegyzés tartalmazza az esemény előfordulásának időpontját.

Az archívum nem tartalmaz védtelen formában kritikus biztonsági paramétereket (jelszavakat, titkos és magánkulcsokat).

A fenti archiválási funkciót az NCA rendszer a naplóállományokra egy közvetlen funkcióval (a befejezett naplóállományok exportálásával és az éles rendszerből való törlésével), míg a tanúsítványok, időbélyeg és OCSP válaszokra és a napló adatbázis egyes elemeire egy másik közvetlen funkcióval valósítja meg (a permanens mentések automatikus készítése mellett).

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

6.1.8.2 Szelektálható kereshetőség az archivált adatok között

Az NCA rendszer az archívumra vonatkozóan az események típusa szerinti keresés lehetőségét a rendszer saját adatbázisára megvalósított keresési mechanizmusokkal valósítja meg:

- az archivált naplóállományok, időbélyeg válaszok és OCSP válaszok éles rendszerbe való visszatöltésével, illetve
- a tanúsítványok és CRL-ek folyamatos éles rendszerben tartásával.

Ez a biztonsági alfunkció a következő SFR kielégítésére irányul: **FDP_CWA_ARC.2.**

6.1.8.3 Az archivált adatok sértetlenségének és bizalmasságának biztosítása

Az NCA rendszer az archívum minden egyes bejegyzését védi a módosítástól, azzal, hogy:

- a naplóállományok elektronikusan aláírva kerülnek archiválásra, illetve
- a tanúsítványok, CRL-ek, valamint az időbélyeg és OCSP válaszok eleve alá vannak írva.

Az NCA rendszer archívuma nem tartalmaz nyílt formában kritikus biztonsági paramétereket.

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

6.1.8.4 A környezet támogatása

Az archiválás biztonsági funkciót teljes egészében az NCA rendszer valósítja meg (a környezet támogatása nélkül).

6.1.9 BF9: Távoli adatbevitel és export

Ennek az összetett biztonsági funkciónak a célja az NCA rendszernek (pontosabban az NCAADM alrendszernek) távolról beküldött adatok, valamint az innen kikerülő adatok sértetlenségének, hitelességének és bizalmasságának a biztosítása.

Az alábbi biztonsági alfunkciókból áll:

- BF9.1 Eredet bizonyítás és eredet ellenőrzés
- BF9.2 A belső adatkommunikáció védelme

6.1.9.1 Eredet bizonyítás és eredet ellenőrzés

Az NCA minden általa kibocsájtott tanúsítványt, CRL-t, időbélyeg tokent, illetve OCSP választ digitális aláírással lát el, ezzel biztosítva az eredet bizonyíthatóságát.

Az NCA kezdeti tanúsítvány regisztrálási kérést csak akkor fogad el egy tanúsítvány alanytól, ha az helyesen megad egy hitelesítési kódot (a regisztráció során kapott jelszót).

Az NCA minden egyéb biztonság-kritikus információt csak erre külön feljogosított belső felhasználótól fogad el, azt is csa akkor, ha az információ digitálisan alá lett írva (pl. regisztrációs tisztviselő tanúsítványkérelme) vagy ha a felhasználó helyesen megad egy hitelesítési kódot (pl. Rendszeradminisztrátor által megadott konfigurációs paraméterek).

Ez a biztonsági alfunkció a következő SFR kielégítésére irányul: **FCO_NRO_CIMC.3** és **FCO_NRO_CIMC.4**

6.1.9.2 A belső adatkommunikáció védelme

Az NCA fizikailag elkülönülő részei között lebonyolított teljes belső kommunikációja (vagyis az NCAADM és az NCACLI USR, illetve az NCAADM és az NCACLI ADM közöttti adatforgalom) titkosított és hitelesített (a 2. ábrán a COMM alrendszer, illetve a SeCh kulccsal titkosított kapcsolat). A titkosítás véd a továbbított adatok illetéktelen felfedése ellen, míg a megvalósított hitelesítés véd a továbbított adatok illetéktelen módosítása ellen.

Ez a biztonsági alfunkció a következő SFR kielégítésére irányul: **FDP_ITT.1 (iteráció 3 és 4)** és **FPT_ITT.1 (iteráció 3 és 4).**

6.1.9.3 A környezet támogatása

Távoli adatbevitel és export esetén az IT környezet a következő fontos támogatást biztosítja: (a 2. ábrán jelölt webszerver és az egyéb alkalmazások hozzáférése között) kikényszeríti a az SSL kapcsolat kiépítését, mely megbízható csatornát biztosít a távoli felhasználók és az NCA rendszer között.

Az IT környezet (az SSL kapcsolat kiépítésének kikényszerítésével a következő SFR-ek kielégítésére irányul: **FDP_ITT.1 (iteráció 1 és 2), FDP_UCT.1, FPT_ITC.1** és **FPT_ITT.1 (iteráció 1 és 2).**

6.1.10 BF10: Tanúsítvány előállítás

Ennek az összetett biztonsági funkciónak a célja annak biztosítása, hogy az NCA rendszer alap szolgáltatásai közé tartozó tanúsítvány előállítási, illetve megújítási, felülhitelesítési kérelmek biztonságos módon hajtódjanak végre.

Az NCA rendszerben nincs külön RA és CA rendszer, melyek kommunikálnak egymással. Egy rendszer van, aminek adatbázisában státusz állapotok állításával „kommunikálnak" a különböző szolgáltatások.

Az NCA rendszer tanúsítványok kezelésével kapcsolatos biztonsági funkciói (BF10: Tanúsítvány előállítás, BF11: Visszavonás kezelés, valamint BF12: Visszavonás állapot) egységes szemléletben kezelik a tanúsítványok életciklusát.

Egy tanúsítvány életciklusa az NCA rendszeren belül úgynevezett státusz állapotokon keresztül követhető. Kétféle státuszállapotot különböztet meg a rendszer:

- főstátuszokat (f0: beadva, f1: elutasítva, f2: előtanúsítvány, f3: tanúsítvány, f4: előkérelem) és
- alstátuszokat melyeket 0-99 jelöl.

Az NCA rendszer csak a főstátuszokat értelmezi logikailag. Értékei 0 vagy 1 lehetnek. Jelentésük az alábbi:

- f0=1, ha be van adva a tanúsítványkérelem,
- f1=1, ha a kérelem elutasításra került. /Amíg a kérelemből nem lesz tanúsítvány (f3=1), addig bármely fázisban a regisztrációs tisztviselők elutasíthatják, mely után semmilyen további művelet végrehajtását nem engedélyezi az NCA rendszer.
- f2=1, ha az ncara regisztrációs tisztviselő kiadhatónak minősíti a tanúsítványkérelmet, miután az összes előírt regisztrációs műveletet végrehajtotta. Ezután ncara további műveletet nem végezhet a tanúsítványkérelmen. /f2=1 akkor lehet, ha f0=1 és f1=0/.
- f3=1, ha az ncaca regisztrációs tisztviselő jóváhagyta a tanúsítvány kiadását. Ezután további státusz művelet a kérelemmel vagy a tanúsítvánnyal nem végezhető. / f3=1 akkor lehet, ha f0=1, f1=0 és f2=1/.
- f4=1 olyan tanúsítványkérelem bejegyzést jelöl, amelyhez még nem tartozik kulcs, viszont e-mail, lakcímkártya, stb. ellenőrizhető, nyilvántartható. /A tanúsítvány kérelem csatolása után f0 állapotba kerül./

Az alstátuszokat csak tárolja és visszaadja az NCA rendszer függvényeit meghívó környezetnek (template rendszernek). Az alstátuszok értéke egy nyomtatható karakter lehet, melyeket a template rendszer saját hatáskörében használ. A státusz átmenetek logikáját a minden egyes CA-hoz egyedileg tartozó stats.cnf állomány írja le. A stats.cnf állományban tanúsítvány típusonként különböző bejegyzések kerülhetnek.

Az alstátuszok és a stats.cnf állomány segítségével a környezetben működő program a tanúsítványkezelés feltételeit tág határok között tovább finomíthatja, megoldva például az alábbiakat:

- az egyes státusz váltásokra jogosult szerepkörök meghatározása,
- az egyes státusz váltásokra együttesen feljogosított privilegizált felhasználók száma,
- az adott státusz váltáskor a művelet aláírását is ellenőrizni kell,
- az adott státusz váltáshoz ellenőrizni kell: személy azonosító igazolvány és/vagy lakcímkártyát és/vagy egyéb igazolványt és/vagy e-mail címet,
- az adott státusz váltáshoz on-line adategyeztetés szükséges,

További konfigurációs állomány a precert.cnf. Segítségével széles határok között szabályozhatók az alábbiak:

- a tanúsítványkérelemben szereplő mezők elfogadható (lehetséges) értékei (kötelezően vagy opcionálisan kitöltött, illetve tiltott mezők),
- a tanúsítvány életciklusát befolyásoló paraméterek:
    - duration (alapértelmezett érvényességi hossz napokban),
    - holditoncrl (kiadáskor azonnal felfüggesztésre kerüljön-e a tanúsítvány),
    - notbeforeop (ennyi másodperccel eltolódik a tanúsítvány érvényessé válása a kiadás pillanatához képest),
    - certlifeflags (melynek értékei a következők:
        - a hosszabbított tanúsítvány élettartama beágyazható-e az előzőbe
        - a hosszabbított tanúsítvány érvényessége között lehet-e hézag
        - legfeljebb az előző élettartamra hosszabbítható
        - ismétlések, hosszabbítások maximális darabszáma
        - érvényesség hossza napokban
        - maximális élettartam hossza napokban)
    - reqsubjchange (az ncara megadhatja-e, hogy a tanúsítvány subject-jébe a kérelemtől eltérő adatok kerülhessenek bele. A tanúsítvány kiadásakor az NCA rendszer ellenőrzi a csere bejegyzés meglétét.)

További konfigurációs állomány a v3exts.cnf. Segítségével azok az x509-es kiterjesztések adhatók meg, melyek kiadáskor a tanúsítványba kerülnek.

A regisztrálás biztonsági funkció segítségével az NCA rendszer képes az alábbi szabványos tanúsítvány kérelmek fogadására és feldolgozására:

- PKCS#10,
- x509-es tanúsítvány

A tanúsítvány kérelemben megadott adatok körének és érvényességének ellenőrzését az NCA rendszeren kívül végzik.

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

A jóváhagyást, illetve elutasítást (pontosabban az ezt jelző főstátusz állapot változtatását) a regisztrációs tisztviselő digitálisan aláírja.

A regisztrálás során a kérelmező választása alapján a tanúsítványba kerülő adatok publikussá válnak, vagy ellenkezőleg, bizalmasan kezelendőnek. E választástól függően fogja az NCA rendszer az érintett felek (anonymous) számára elérhetővé, kereshetővé tenni a tanúsítvány alanyok adatait.

A tanúsítvány előállításon belül az alábbiak különböztethetők meg:

- Kezdeti tanúsítvány előállítás
- Tanúsítvány megújítás
- Felülhitelesítés

6.1.10.1 (Kezdeti) tanúsítvány előállítás

Amennyiben a regisztrációs tisztviselő (ncaca) jóváhagyta a tanúsítvány kiadását /f3=1, amellett, hogy f0=1, f1=0 és f2=1/, az NCA rendszer képes különböző (konfigurálható) profiloknak megfelelő, szabványos x509-es tanúsítványok előállítására.

A kezdeti tanúsítvány előállítást (a tanúsítvány alany kérelme és e kérelem ncara általi elfogadása után) az ncaca regisztrációs tisztviselő kérheti, azonosítás és hitelesítés után.

6.1.10.2 Tanúsítvány megújítás

Az NCA rendszer támogatja a tanúsítvány megújítás azon formáját, amikor egy új tanúsítvány készül a már létező és még érvényes nyilvános kulcs felhasználásával (azt a másik megújítási formát nem támogatja, amikor új nyilvános kulcsra készül tanúsítvány, az előző tanúsítvány előállításához felhasznált regisztrációs adatok felhasználásával).

A tanúsítvány megújítást a tanúsítvány alanya (a magánkulcs birtokosa), illetve a (mindkét típusú) regisztrációs tisztviselő kérheti, azonosítás és hitelesítés után.

6.1.10.3 Felülhitelesítés

Az NCA rendszer támogatja a felülhitelesítést is, melynél az NCA rendszer egy kereszt-tanúsítványt biztosít a kérelmező másik megbízható rendszer számára, mely megadta saját nyilvános kulcsát a tanúsítványhoz. Ennek alapján az NCA rendszerhez tartozó előfizetők is megbízhatnak a másik hitelesítés-szolgáltatóban.

A felülhitelesítést a (ncara és ncaca) regisztrációs tisztviselő kérheti, azonosítás és hitelesítés után.

Mindhárom fenti esetben az NCA rendszer tanúsítvány aláírására használt magánkulcsait kizárólag a tanúsítványok és a megfelelő visszavonás állapot adatok aláírására használja fel. Az NCA rendszer azt is biztosítja, hogy csak érvényes (nem lejárt, és nem is visszavont) tanúsítványhoz tartozó magánkulccsal ír alá tanúsítványt, CRL-t.

A tanúsítvány előállítás mindhárom esete (kezdeti tanúsítvány előállítás, tanúsítvány megújítás, felülhitelesítés) tanúsítvány profilokon alapul, s az NCA rendszer biztosítja, hogy a kiadott tanúsítványok megfelelnek valamelyik profilnak.

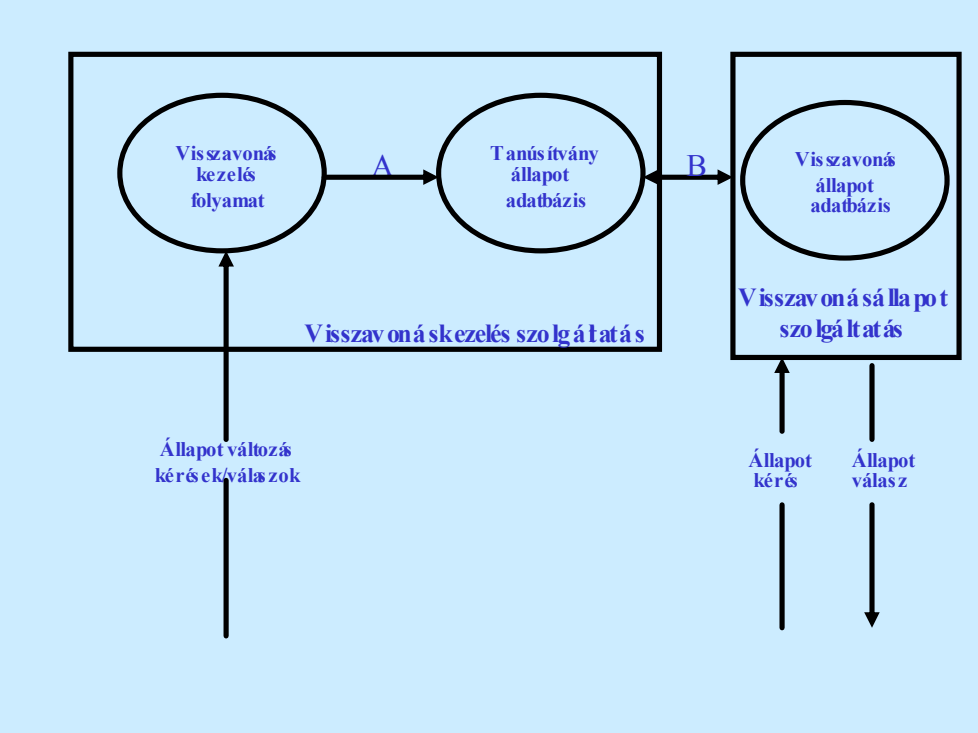
Ez a biztonsági funkció a következő SFR-ek kielégítésére irányul: **FDP_CIMC_CER.1** és **FMT_MOF_CIMC.3.**

6.1.10.4 A környezet támogatása

A tanúsítvány előállítás biztonsági funkcióhoz az (IT és nem IT) környezet az alábbi támogatást nyújtja: az egyes tanúsítvány kérelmekben megadott adatok ellenőrzése.

6.1.11 BF11: Visszavonás kezelés

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

Az 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).

6.1.11.1 Az NCA rendszer visszavonás kezelése

Az NCA rendszer architekturális felépítése miatt más filozófiát juttat érvényre. Mindkét szolgáltatás ugyanazon adatbázishoz fér hozzá (az első módosíthatja az állapotokat, míg a másik csak olvashat, kereshet benne). A jogosultságellenőrzésen keresztül az NCA rendszer is biztosítja az adatbázis hitelességét és sértetlenségét, egyúttal a változások késlekedés nélkül, külön üzenetközvetítés nélkül is elérhetők a többi szolgáltatás (OCSP, CRL) számára.

Az NCA rendszer minden felfüggesztésre, felfüggesztés megszüntetésére és visszavonásra vonatkozó kérelmet megfelelő módon hitelesít és érvényesít.

Állapot változtatását csak a következők kezdeményezhetik:

- az infrastrukturális tanúsítványokra a rendszeradminisztrátor (ncaroot),
- a rendszervezérlési tanúsítványokra az adott tanúsítvány (bizalmi munkakört betöltő) alanya (ncaroot, ncara, ncaca, ncasecadm, ncaau),
- az alanyok tanúsítványaira a regisztrációs tisztviselők (ncara és ncara).

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

Ezt követően a valós idejű visszavonás állapot (OCSP) szolgáltatás késleltetés nélkül az aktuális állapotokat mutatja.

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

Az OCSP szolgáltatás által kibocsátott OCSP válaszok egy OCSP profilon alapulnak, s az NCA rendszer biztosítja, hogy a kibocsátott OCSP válaszok megfelelnek az OCSP profilnak.

Ez a biztonsági funkció a következő SFR-ek kielégítésére irányul: **FMT_MOF_CIMC.5** és **FMT_MOF_CIMC.6**.

6.1.11.2 A környezet támogatása

A visszavonás kezelés biztonsági funkcióhoz az (IT és nem IT) környezet az alábbi támogatást nyújtja: az egyes vissazavonási kérelmekben megadott adatok ellenőrzése.

6.1.12 BF12: Visszavonás állapot (CRL, OCSP)

Ennek a biztonsági funkciónak a célja a Visszavonás kezelés biztonsági funkció által módosított állapotok lekérdezése.

6.1.12.1 Az NCA rendszer visszavonás állapot szolgáltatása

Az NCA rendszer kétféle vissszavonás állapot szolgáltatást támogat:

- OCSP, melyet az alábbiak jellemeznek:
  - bárki kérhet (azonosítás nélkül),
  - kérés feldolgozása és a válasz elkészítése megfelel az RFC 2560 előírásainak,
  - a kérés elvárt szerkezete konfigurálható (az RFC 2560 keretszabvány lehetőségein belül),
  - a tanúsítvány állapot adatbázis aktuális tartalma alapján válaszol.
- CRL, melyet az alábbiak jellemeznek:
  - bárki kérhet (azonosítás nélkül),
  - a CRL szerkezete és tartalma megfelel az RFC 3280 előírásainak (v2),
  - kibocsátásakor a tanúsítvány állapot adatbázis aktuális tartalma a meghatározó,
  - mindig két CRL készül párhuzamosan, kétféle adattartalommal:
    - az egyik a CA által valaha kibocsátott tanúsítványok közül tartalmazza a visszavontak és felfüggesztettek azonosítóit,
    - a másik a CA által kibocsátott, még le nem járt tanúsítványok közül tartalmazza a visszavontak és felfüggesztettek azonosítóit.
  - a CRL kibocsátás az alábbi módokon valósulhat meg:
    - konfigurálható időközönként, automatikusan,
    - ncaca kiadási parancs alapján azonnal,
    - változás (visszavonás, felfüggesztés, felfüggesztés visszavonása) után azonnal és automatikusan.

Az NCA rendszerben a visszavonás állapot szolgáltatás közvetlenül az éles tanúsítvány állapot adatbázis alapján működik.
Minden OCSP kérés megválaszolása előtt, az NCA rendszer ellenőrzi a tanúsítvány állapot adatbázis érintett rekordjának sértetlenségét (a rekord aláírásának ellenőrzésével). Az NCA rendszer minden OCSP kérés esetén garantáltan a kérésben azonosított tanúsítványra vonatkozóan kér információt a tanúsítvány állapot adatbázisból.
Az NCA rendszerben a visszavonás állapot szolgáltatás minden válaszát digitálisan aláírja, (különböző CRL és OCSP) infrastrukturális kulcsával.
A digitális aláírásra használt aláíró algoritmusok és kulcsok megfelelnek a "Biztonságos algoritmusok"-ra vonatkozó NHH elvárásoknak.
A válasz üzenetek tartalmazzák azt az időt, amikor a visszavonás állapot szolgáltatás aláírta a választ.

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

6.1.12.2 A környezet támogatása

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

6.1.13 BF13: Időbélyegzés

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

6.1.13.1 Az NCA rendszer időbélyegzés szolgáltatása

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

Az NCA rendszer konfigurálástól függően:

- nem ellenőrzi az időbélyeg kérések eredetét (azaz azonosítás és hitelesítés nélkül bárkinek elérhetővé teszi ezt a szolgáltatását), vagy
- promóciós kód használatával eredet vizsgálatot végez (azaz azonosításhoz és hitelesítéshez köti ezt a szolgáltatását).

Az NCA rendszer ellenőrzi az időbélyeg kérésekben alkalmazott lenyomatkészítő algoritmust, s csak a következőt fogadja el: SHA1

Miután az NCA rendszer IT környezete szinkronizálja független időforrásait és meghatározza az UTC-től való eltérés maximális eltérését, az NCA rendszer ellenőrzi, hogy a maximális eltérés egy konfigurálható határon belül van-e. Az NCA 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 NCA 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 NCA rendszer biztosítja, hogy az időbélyeg válasz ugyanazokat az adatokat tartalmazza, mint amit a kérésben küldtek.

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

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

6.1.13.2 A környezet támogatása

Az NCA rendszer a z informatikai környezetétől az alábbi védelmi mechanizmusokat várja el:

- független és pontos időforrások biztosítása,
- a független időforrások szinkronizálása (egy NTPv4 protokoll alapú ntpd programmal),

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 NCA v2.6.0 egyedül a BF3 biztonsági funkciójához használ ilyen mechanizmust, nevezetesen az alábbit:

- hitelesítésre használt jelszó alapú hitelesítés.

Az NCA v2.6.0 biztonsági funkcióerősségre vonatkozó elvárása: SOF-alap (SOF-basic).

6.3 Garanciális intézkedések

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

6.3.1 Konfiguráció kezelés

Az NCA v2.6.0 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;
- felhasználói és adminisztrátori útmutatók;
- konfiguráció kezelés dokumentáció;
- (feltárt és javított) biztonsági hibák;
- teszt dokumentáció és teszt szoftver.

Az NCA v2.6.0 fejlesztése során biztosítva volt, hogy csak engedélyezett módosítások történhessenek a fejlesztés alatt álló szoftveren. Az NCA v2.6.0 termékhez verziószámot rendelnek (2.6.0.buildszám), az értékelés során egyértelműen látható, hogy mely verzió értékelését végzik az értékelők.
A konfiguráció kezelési tervről készült leírás: "NCA v2.6.0 – A konfiguráció kezelés dokumentációja".

6.3.2 Szállítás és üzembe helyezés

Az NCA rendszer szállítását és telepítését kizárólag a termék gyártója végzi.

6.3.3 Fejlesztés

Az "NCA v2.6.0 – Biztonsági szabályzat modell” című dokumentum leírja az NCA rendszer valamennyi modellezhető szabályzatának jellemzőit és szabályait.
A funkcionális specifikáció meghatározza az NCA v2.6.0 fő biztonsági funkcióit, a külső interfészeket, ezek használatának célját és módját, teljesen részletezve valamennyi hatást, kivételt és hibaüzenetet. /”NCA v2.6.0 - Funkcionális specifikáció”/.
A magas szintű terv leírja az NCA rendszer fő elemeit (alrendszereit), a közöttük lévő kapcsolatokat. /”NCA v2.6.0 - - Magas szintű terv”/.
Az alacsony szintű terv az NCA v2.6.0 szerkezetét modulok (kliens oldali függvények és kozolparancsok) szerint tárgyalja, leírva minden modul célját, a modulok közötti belső kapcsolatokat, a modulokhoz csatlakozó valamennyi interfészt. /"NCA v2.6.0 - Alacsony szintű terv"/
Az értékelés vizsgálta a megvalósítási reprezentáció egy részhalmazát is (a biztonság-kritikus forráskódok).
Az "NCA v2.6.0 – Megfeleltetés elemzések" 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 NCA rendszer különböző felhasználóinak (adminisztrátorok és alkalmazás (template) fejlesztők) számára készült dokumentumok leírják az NCA rendszer biztonságos adminisztrálásának és felhasználásának módját. /"NCA v2.6.0 – Konfigurációs állományok", "NCA v2.6.0 – Kliens oldali függvények és konzolparancsok"

6.3.5 Az életciklus támogatása

A tervezés és fejlesztés során az NCA 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.
Az "NCA v2.6.0 – A fejlesztési biztonság dokumentációja" leírja a fejlesztők által az NCA rendszer fejlesztése során alkalmazott szabályokat.
Az NCA rendszer fejlesztői környezetében a teljes fejlesztési és karbantartási folyamatot ellenőrzés alatt tartják. Az NCA rendszer fejlesztéséhez és karbantartáshoz felállított és használt életciklus modell leírását az "NCA v2.6.0 – Az életciklust meghatározó dokumentáció" című anyag tartalmazza.
Az "NCA v2.6.0 –Hibajelentési eljárások dokumentációja" 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 az "NCA v2.6.0 – A fejlesztő eszközök dokumentációja " című anyag meghatározza NCA rendszer megvalósításához és vizsgálatához használt fejlesztő eszközöket, és ezen eszközök megvalósítástól függő tulajdonságait (opcióit).

6.3.6 Tesztelés

Az NCA rendszer teszteléséhez az alábbi, teszteléssel kapcsolatos dokumentumok készültek:
" NCA v2.6.0 – Tesztelési dokumentáció", " NCA v2.6.0 – Teszt lefedettség elemzés", " NCA v2.6.0 – Teszt mélység elemzés".

6.3.7 Sebezhetőségek felmérése

Az "NCA v2.6.0 – Az útmutatók helytelen használhatóságának elemzése" című anyag azt mutatja ki, hogy a különböző (telepítési, adminisztrátori, felhasználói) útmutató dokumentumok nem tartalmaznak félrevezető, értelmetlen és ellentmondásos útmutatásokat, valamint hogy valamennyi üzemmódban tárgyalják a biztonságos eljárásokat.
Az "NCA v2.6.0 – Sebezhetőség elemzés" című dokumentum az NCA rendszer potenciális sebezhetőségere kimutatni, hogy az adott sebezhetőség miért nem használható ki az NCA rendszer működési környezetében.
Végül az "NCA v2.6.0 – Biztonsági funkcióerősség elemzés" című dokumentum a jelszó alapú hitelesítés funkció erősségének elemzését tartalmazza.

7. Védelmi profil megfelelőségi nyilatkozat

Jelen biztonsági előirányzat megfelel a következő védelmi profilnak:
Certificate Issuing and Management Components Family of Protection Profiles (CIMC-PP) Version 1.0 /Security Level 3, 3-as biztonsági szint/ (2003. október 31.)

A 3-as biztonsági szintű CIMC PP védelmi profil minden feltételezése, veszélye, szabályzata, biztonsági célja és biztonsági követelménye újraszerepel jelen ST-ben. Ezen kívül ezen biztonsági előirányzat definiálja a P.Archiving és P.TimeStampToken szervezeti biztonsági szabályzatot és az O.Archiving és O.TimeStampToken biztonsági célt.
Az IT biztonsági követelményeken végrehajtott minden művelet a 3-as biztonsági szintű CIMC PP által meghatározott határokon belül van. Az értékadás és kiválasztás műveleteit tipográfiai megkülönböztetés jelzi, ahogyan az az 5. fejezet elején szerepel.

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
O.Control unknown source communication traffic	T.Hacker gains access
O.Non-repudiation	T.Sender denies sending information
O.Preservation/trusted recovery of secure state	T.Critical system component fails
O.Sufficient backup storage and effective restoration	T.Critical system component fails T.User error makes data inaccessible

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.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.Repair identified security flaws	T.Flawed code T.Critical system component fails
OE.Social Engineering Training	T.Social engineering
OE.Trusted Path	T.Hacker gains access T.Message content modification
OE.Validation of security function	T.Malicious code exploitation T.Administrators, Operators, Officers and Auditors commit errors or hostile actions

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).Cryptographic functions	T.Disclosure of private and secret keys T.Modification of private/secret keys
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	O(E).Cryptographic functions
P.Archiving	O.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:

O.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.

Rendszer

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.
>
> **O.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.
>
> **O.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.

O(E).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:

O(E).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.

T.Sender denies sending information arra az esetre irányul, amikor egy üzenet küldője letagadja az üzenet elküldését, hogy elkerülje az üzenet küldéséért és az ezt követő cselekvés vagy nem cselekvés miatti felelősségre vonhatóságot. Ezt a veszélyt az alábbiak védik ki:

> **O.Non-repudiation** biztosítja, hogy egy üzenet küldője/készítője sikeresen nem tagadhatja le az üzenet küldését a fogadónak.

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.Control unknown source communication traffic** biztosítja az ismeretlen forrásból származó kommunikációs forgalom ellenőrzését (pl. átirányítással vagy eldobással) a lehetséges károk elkerülésére. A támadásnak feltételezett forgalom átirányításával vagy eldobásával különböző támadások észlelhetők vagy akadályozhatók meg.
>
> **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 **O(E).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 **O.Archiving** biztonsági cél irányul.

P.TimeStampToken előírja az RFC 3161 szabványnak megfelelő időbélyeg kérésekre adott időbélyeg válaszok RFC 3161-nek megfelleő 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 a rész 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 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_GEN.1 Napló adatok generálása (iteráció 1,2)	O(E).Individual accountability and audit records
FAU_GEN.2 A felhasználói azonosítóval való összekapcsolás (iteráció 1,2)	O(E).Individual accountability and audit records
FAU_SAR.1 Napló áttekintés (iteráció 1,2)	O(E).Individual accountability and audit records
FAU_SAR.3 Kiválogatható napló áttekintés (iteráció 1,2)	O(E).Individual accountability and audit records
FAU_SEL.1 Kiválasztható napló (iteráció 1,2)	O(E).Individual accountability and audit records
FAU_STG.1 A naplóesemények védett tárolása (iteráció 1,2)	O(E).Protect stored audit records
FAU_STG.4 A napló adatok elvesztésének meggátolása (iteráció 1,2)	O(E).Respond to possible loss of stored audit records
FCO_NRO_CIMC.3 Kötelező eredet bizonyítás és eredet ellenőrzés	O.Non-repudiation O.Control unknown source communication traffic
FCO_NRO_CIMC.4 Az eredet fokozott ellenőrzése	O.Non-repudiation
FCS_CKM.1 A kriptográfiai kulcsok generálása	O(E).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 (iteráció 1,2)	O(E).Cryptographic functions
FDP_ACC.1 Részleges hozzáférés ellenőrzés (iteráció 1,2)	O(E).Limitation of administrative access
FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés (iteráció 1,2)	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_BKP.1 CIMC mentés és visszaállítás	O(E).Object and data recovery free from malicious code O.Preservation/trusted recovery of secure state O.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_CWA_ARC.1 Archiválás	**O.Archiving**
FDP_CWA_ARC.2 Szelektálható keresés az archívumban	**O.Archiving**
FDP_CWA_ARC.3 Kiterjesztett archiválás	**O.Archiving**
FDP_CIMC CER.1 Tanúsítvány előállítás	O.Certificates
FDP_CIMC CRL.1 Tanúsítvány visszavonási lista érvényesítés	O.Certificates

Funkcionális biztonsági követelmény	Biztonsági cél
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 1,3)	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 2,4)	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
FDP_UCT.1 Alapszintű adatcsere bizalmasság	O(E).Data import/export
FIA_AFL.1 Hitelesítési hibák kezelése (iteráció 1,2)	O(E).React to detected attacks
FIA_ATD.1 Felhasználói tulajdonságok megadása (iteráció 1,2)	O(E).Maintain user attributes
FIA_SOS.1 A titkok ellenőrzése	O(E).Manage behavior of security functions
FIA_UAU.1 A hitelesítés időzítése (iteráció 1,2)	O(E).Limitation of administrative access O(E).Restrict actions before authentication
FIA_UID.1 Az azonosítás időzítése (iteráció 1,2)	O(E).Individual accountability and audit records O(E).Limitation of administrative access
FIA_USB.1 Felhasználó - szubjektum összerendelése (iteráció 1,2)	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_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
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	O(E).Maintain user attributes O(E).User authorization management
FMT_MSA.2 Biztonságos biztonsági tulajdonságok	O(E).Security-relevant configuration management
FMT_MSA.3 Statikus tulajdonságok kezdeti értékadása	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.5 A TSF titkos kulcs 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 1,2)	O(E).Manage behavior of security functions

Funkcionális biztonsági követelmény	Biztonsági cél
FMT_SMR.2 Megszorítások a biztonsági szerepkörökre (iteráció 1,2)	O(E).Security roles
FPT_AMT.1 Az absztrakt gép tesztelése	OE.Periodically check integrity OE.Validation of security function
FPT_CIMC_TSP.1 Napló lista aláírása	O(E).Protect stored audit records
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 1,2,3,4)	O(E).Protect user and TSF data during internal transfer
FPT_RVM.1 A TSP megkerülhetetlensége (iteráció 1)	OE.Operating System
FPT_RVM.1 A TSP megkerülhetetlensége (iteráció 2)	O(E).Limitation of administrative access
FPT_SEP.1 TSF tartomány szétválasztás	OE.Operating System
FPT_STM.1 Megbízható időbélyegzés (iteráció 1,2)	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

8-7. 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 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

garanciális biztonsági követelmény	biztonsági cél
ATE_IND.2 Független tesztelés - mintán	EAL4 választás
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

Jogosult felhasználók

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 (OCSP alap-válasz érvényesítés),** amelyek azt garantálják, hogy a tanúsítvány visszavonási listák és a tanúsítvány állapot információk érvényesek. Abban az esetben, amikor a TOE *(kizárólag PKI üzemmódjában)* 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 az időbélyeg válaszok érvényesek.

Rendszer

O.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.

O.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.

O.Archiving teljesülését az alábbiak biztosítják: **FDP_CWA_ARC.1 (Archiválás)**, mely egy olyan archiválási funkciót követel meg, amely lehetővé teszi a TOE által előállított minden tanúsítvány, CRL, napló állomány és *időbélyeg token* archiválását**, FDP_CWA_ARC.2 (Szelektálható keresés az archívumban)**, amely az archívumra vonatkozóan egy keresési lehetőséget követel meg az események típusa szerint, illetve **FDP_CWA_ARC.3 (Kiterjesztett archiválás)**, mely az archivált adatok sértetlenségének biztosítását várja el.

Kriptográfia

O.Non-repudiation teljesülését az alábbiak biztosítják: **FCO_NRO_CIMC.3 (Kötelező eredet bizonyítás és eredet ellenőrzés)**, mely arra vonatkozó követelmény, hogy biztonság-kritikus üzenetet a TOE csak az eredet bizonyítása esetén fogadjon, **FCO_NRO_CIMC.4 (Az eredet fokozott ellenőrzése),** mely arra vonatkozó követelmény, hogy az eredet bizonyítását (a kezdeti tanúsítvány regisztrálási üzenetek kivételével) digitális aláírással kell teljesíteni.

Külső támadások

O.Control unknown source communication traffic teljesülését biztosítja: **FCO_NRO_CIMC.3 (Kötelező eredet bizonyítás és eredet ellenőrzés)**, mely arra vonatkozó követelmény, hogy a TOE dobjon el minden olyan ismeretlen forrásból származó üzenetet, mely biztonság-kritikus információt tartalmaz.

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.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.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),** 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), FMT_MOF_CWA.1 (Időbélyeg profil menedzsment),** melyek megkövetelik, hogy a rendszeradminisztrátorok ellenőrizhessék a TOE által generált tanúsítványokba, tanúsítvány visszavonási listákba, OCSP válaszokba, illetve időbélyeg válaszokba (időbélyeg tokenekbe) 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).Cryptographic functions teljesülését biztosítja: **FCS_CKM.1 (A kriptográfiai kulcsok generálása)** és **FCS_COP.1 (Kriptográfiai eljárás, iteráció 1),** melyek arra vonatkozó követelmények, hogy jóváhagyott kriptográfiai algoritmusokat kell megvalósítani a titkosításra/dekódolásra, hitelesítésre és aláírás létrehozására/ellenőrzésére, valamint jóváhagyott kulcsgenerálási technikákat kell alkalmazni.

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, kulcsolt lenyomatot vagy hitelesítési kódot használ a módosítások észlelésére, ezért **FMT_MTD_CIMC.4 (A TSF magánkulcs bizalmasságának védelme)** és **FMT_MTD_CIMC.5 (A TSF titkos kulcs bizalmasságának védelme)** követelményekre is szükség van annak garantálására, hogy egy szoftvert, förmvert vagy mentett adatokat módosító támadó ne tudja megakadályozni a módosítás észlelését új digitális aláírás, kulcsolt lenyomat vagy hitelesítési kód 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, iteráció 1,2)** és **FAU_SEL.1 (Kiválasztható napló, iteráció 1,2)** azt követelik meg, hogy a biztonság-kritikus eseményeket naplózzák, **FAU_GEN.2 (A felhasználói azonosítóval való összekapcsolás, iteráció 1,2)** és **FPT_STM.1 (Megbízható időbélyegzés, iteráció 1,2)** 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)** azt követeli meg, hogy a naplóadatokat a rendszervizsgáló átvizsgálhassa, s rajta kívül egyetlen felhasználó se törölhesse ezeket. Végül **FAU_SAR.1 (Napló áttekintés, iteráció 1,2)** és **FAU_SAR.3 (Kiválogatható napló áttekintés, iteráció 1,2)** 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 1,3)** 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 kriptográfia alkalmazásával védik meg, **FMT_MTD_CIMC.4 (A TSF magánkulcs bizalmasságának védelme)** és **FMT_MTD_CIMC.5 (A TSF titkos kulcs bizalmasságának védelme)** követelményekre is szükség van, hogy az adatok és szoftverek védelméhez használt magán és titkos kulcsok 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)** és **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)** 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),** mely arra vonatkozó követelmény, hogy a jogosult felhasználók konfigurálhassák, működtethessék és kezelhessék a biztonsági mechanizmusokat, illetve a **FIA_SOS.1 (A titkok ellenőrzése),** ami biztosítja, hogy a felhasználói jelszavak megfeleljenek egy konfigurálható biztonságos követelményhalmaznak, továbbá az **FMT_SMF.1 (Menedzsment funkciók megadása)**, 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, iteráció 1,2),** 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 védeni kell a jogosulatlan hozzáférésekkel szemben. Mivel 3-as szint esetében a rosszindulatú tevékenységek nagyobb mértéke tételezhető fel, ezért **FPT_CIMC_TSP.1 (Napló lista aláírása)** is követelmény, mely alapján a naplórekordok módosítása 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, iteráció 1,2),** 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)** és **FMT_MSA.2 (Biztonságos biztonsági tulajdonságok),** melyek arra vonatkozó követelmények, hogy a biztonsági tulajdonságok biztonságos értékeket vegyenek fel. **FMT_MOF.1 (A biztonsági funkciók viselkedésének kezelése, iteráció 1,2)** 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, iteráció 1,2),** mely arra vonatkozó követelmény, hogy az időpont megbízható.

O(E).User authorization management teljesülését biztosítja: **FMT_MSA.1 (Biztonsági tulajdonságok kezelése),** mely arra vonatkozó követelmény, hogy a rendszeradminisztrátorok kezelik és frissítik a felhasználók biztonsági tulajdonságait. 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

Az alábbi táblázat összefoglalja a funkcionális biztonsági követelmények között végzett függőség elemzés eredményeit.

8-8. táblázat:
A TOE-ra vonatkozó 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_SEL.1 Kiválasztható napló	FAU_GEN.1 Napló adatok generálása	Igen
	FMT_MTD.1TSF adatok kezelése	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
FCO_NRO_CIMC.3 Kötelező eredet bizonyítás és eredet ellenőrzés	FIA_UID.1 Az azonosítás időzítése	Igen
FCO_NRO_CIMC.4 Az eredet fokozott ellenőrzése	FCO_NRO_CIMC.3 Kötelező eredet bizonyítás és eredet ellenőrzés	Igen
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_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_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_TS.1 Időbélyeg előállítás	---	---
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	---	---
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_SOS.1 A titkok ellenőrzése	---	---
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)
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)

Követelmény összetevő	függőség	teljesülés
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.1TSF adatok kezelése	FMT_SMR.1 Biztonsági szerepkörök	Igen (FMT_SMR.2)
FMT_MTD_CIMC.4 A TSF magánkulcs bizalmasságának védelme	---	---
FMT_MTD_CIMC.5 A TSF titkos kulcs 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_CIMC_TSP.1 Napló lista aláírása	FAU_GEN.1 Napló adatok generálása	Igen
	FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése	Igen
FPT_ITT.1 A belső adatátvitel alapszintű védelme	---	---
FPT_RVM.1 A TSP megkerülhetetlensége	---	---
FPT_STM.1 Megbízható időbélyegzés	---	---
FTP_TRP.1 Megbízható útvonal	---	---

8.3.1.2 A garanciális biztonsági követelmények függőségei

A 8-9 táblázat a garanciális biztonsági követelmények között végzett függőség elemzés eredményeit foglalja össze.

8-9. 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 tesztelése	(közvetett) ADV_HLD.2	Igen (ADV_HLD.2)
	ATE_FUN.1	Igen

Követelmény összetevő	függőség	teljesülés
	(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, FAU_GEN.2 és FAU_SEL.1, 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. A fentiekből következően jelen biztonsági előirányzatban egyedül a (jelszó alapú) hitelesítési mechanizmusra lehet és kell funkcióerősségre vonatkozó elvárást megfogalmazni.

A hitelesítés funkcióerősségére az alap (SOF-alap) az elvárt szint, mely a jelenleg kereskedelmi forgalomban beszerezhető termékekkel általában elérhető. A SOF-alap funkcióerősség a FIA_UAU.1 (iteráció 1,2) által meghatározott hitelesítési mechanizmusra vonatkozik, s a következőket várja el:

- A hitelesítési mechanizmus minden alkalmazása esetén annak a valószínűségnek, hogy egy véletlen kísérlet sikerrel jár, kisebbnek kell lennie, mint 1/1000000.
- A hitelesítési mechanizmus egy percen belüli többszöri alkalmazása esetén annak a valószínűségnek, hogy a véletlen kísérletek egyike sikerrel jár, kisebbnek kell lennie, mint 1/100000.

A SOF-alap elvárás összhangban van a CIMC védelmi profil SOF elvárásával, valamint a 3-as biztonsági szint AVA_VLA.2 sebezhetőség vizsgálat követelményével is (mely alacsony támadási képességű támadó által végrehajtott áthatolási támadásnak való ellenállást vár el).

8.5 Az értékelési garanciaszint indoklása

8.5.1 A CIMC védelmi profil 3-as biztonsági szintjének indoklása

A CIMC védelmi profil alapján tervezett rendszerek a legkülönbözőbb környezetekben működhetnek, a zárt, biztonságos létesítményektől egészen az ellenséges környezetben működő nyílt hozzáférésű létesítményekig. A környezet és a velejáró veszélyek és sebezhetőségek kockázatának tehát eltérő szintjei lehetségesek. A CIMC védelmi profil a biztonsági

követelményeket a biztonság négy, növekvő szintjére határozza meg: 1-es 2-es , 3-as és 4-es biztonsági szint.

Az 1-es biztonsági szint nyújtja a legkisebb mértékű biztonságot. Az 1-es biztonsági szint biztonsági követelményeinek kielégítésére tervezett rendszereket csak olyan környezetekben helyes alkalmazni, amelyekben a rosszindulatú tevékenységek veszélyét alacsonynak tartják. Az 1-es biztonsági szintű rendszerek nem nyújtanak védelmet a rosszindulatú jogosult vagy jogosulatlan felhasználók általi jogosulatlan felfedéssel szemben.

A 2-es biztonsági szint követelményeinek kielégítésére tervezett rendszerek olyan környezetekben megfelelők, ahol a kockázatok és az adatfelfedés következményei nem jelentősek. A 2-es biztonsági szintű rendszereknek védelmet kell nyújtaniuk a legtöbb, hálózaton keresztül kezdeményezett támadással szemben. Ezen a biztonsági szinten feltételezik, hogy a PKI felhasználói nem rosszindulatúak. A 2-es biztonsági szint legalább két szerepkört ír elő (az egyik szerepkör lesz felelős a felhasználói fiókok adminisztrálásáért, a kulcsgenerálásokért és a napló konfigurálásáért; míg a másik szerepkör lesz a felelős a tanúsítványok kibocsátásáért és visszavonásáért). A 2-es biztonsági szint növeli azoknak az eseményeknek a számát, amelyeket naplózni kell, és a napló fájlokra és rendszer mentésekre fokozottabb kriptográfiai védelmet ír elő. Ezeken túlmenően a magánkulcsok védelmére FIPS 140-1 2-es szinten értékelt és tanúsított kriptográfiai modul van megkövetelve.

A 3-as biztonsági szint követelményeinek kielégítésére tervezett rendszerek olyan környezetekben megfelelőek, ahol a kockázatok és az adatfelfedések és adat sértetlenség elvesztésének következményei közepesek. A 3-as biztonsági szint védelmet tartalmaz olyan személyekkel szemben is, akik fizikai hozzáféréssel rendelkeznek a komponensekhez, és további garancia követelményeket tartalmaz annak biztosítására, hogy a rendszer biztonságosan működik. Ez a biztonsági szint bizonyos védelmet nyújt a rosszindulatú jogosult felhasználókkal szemben is azáltal, hogy legalább három elkülönített szerepkört ír elő (az egyik szerepkör lesz felelős a felhasználói fiókok adminisztrálásáért, a kulcsgenerálásokért és a napló konfigurálásáért; egy másik szerepkör lesz felelős a tanúsítványok kibocsátásáért és visszavonásáért; és egy harmadik szerepkör lesz felelős a naplóbejegyzések kezeléséért). A 3-as biztonsági szint kétszemélyes ellenőrzést ír elő a magánkulcs exportálására, további naplózást ír elő a titkos és magánkulcsok importálására és exportálására, valamint az információ kérelmekre. A hosszú távú magánkulcsok védelméért és a tanúsítványok és tanúsítvány állapot információk aláírásáért felelős kriptográfiai modulokat a FIPS 140-1 3-as biztonsági szintjének megfelelően kell értékelni és tanúsítani. Végül elvárás van a nyilvános kulcsok fokozott védelmére és minden üzenet digitális aláírására.

A 4-es biztonsági szint követelményeinek kielégítésére tervezett rendszerek olyan környezetekben megfelelőek, ahol az adat felfedés és az adatsértetlenség elvesztésének veszélye és ennek következményei jelentősek. A környezet és a felhasználók egyaránt ellenségesek lehetnek.

A 4-es biztonsági szint védelmet kíván nyújtani a rosszindulatú jogosult és jogosulatlan felhasználókkal szemben. Ez részben megvalósítható legalább négy elkülönített szerepkör megkövetelésével (az egyik szerepkör lesz felelős a felhasználói fiókok adminisztrálásáért és a kulcsgenerálásokért; egy másik szerepkör lesz felelős a naplóbejegyzések kezeléséért; egy harmadik szerepkör lesz felelős a tanúsítvány kibocsátásért és visszavonásért; végül egy negyedik szerepkör lesz felelős a mentések végrehajtásáért). A 4-es biztonsági szint megnöveli a naplóbejegyzések sértetlenségét azzal, hogy harmadik fél általi, aláírt időbélyegzést ír elő. A hosszú távú magánkulcsok védelméért és a tanúsítványok és tanúsítvány állapot információk

aláírásáért felelős kriptográfiai modulokat a FIPS 140-1 4-es biztonsági szintjének megfelelően kell értékelni és tanúsítani.

Jelen biztonsági előirányzat a CIMC védelmi profil 3-as biztonsági szintjét várja el.

Ennek egyik oka az, hogy a TOE működtetési környezetére, valamint a jogosult és jogosulatlan felhasználókra vonatkozó feltételezések megegyeznek a védelmi profil 3-as biztonsági szintjén megfogalmazottakkal.

A másik indok, hogy a jelen biztonsági előirányzat egyúttal az MSZ CWA 14167-1 (Elektronikus aláírások tanúsítványait kezelő megbízható rendszerek biztonsági követelményei) mértékadó dokumentum informatikai eszközökkel megvalósítható követelményeinek is meg kíván felelni. A CWA 14167-1 elvárásait a 2-es biztonsági szint még nem teljesíti (pl. a két szerepkör nem elég, a HSM modulra a FIPS 140 szerinti 2-es szint is kevés), viszont a 4-es biztonsági szint felesleges, esetenként csak igen drágán kielégíthető követelményeket támaszt (pl. a HSM modulra vonatkozó FIPS 140 szerinti 4-es szint a CWA elvárásait meghaladja, a harmadik féltől származó napló időbélyegzés is felesleges költségeket okozna).

8.5.2 A CC EAL4 értékelési garanciaszintjének indoklása

A CIMC védelmi profil 3-as biztonsági szintjének garanciális elvárásai nagyon közel állnak a CC EAL4-es garanciaszintjéhez. Ezért kézenfekvő volt a választás: a TOE általános értékelési garanciaszintje EAL4 legyen. (Pontosabban a CIMC védelmi profil 3-as biztonsági szintjén elvárt ALC_FLR.2 (Hibajelentési eljárások) követelménnyel megemelt EAL4.)

Az alábbi érvek megerősítik, hogy miért érdemes a CIMC 3-as biztonsági szintjén hiányzó, de a CC EAL4-ben megjelenő garanciális biztonsági követelményeket is felvállalni:

- ACM_AUT.1 Részleges konfiguráció kezelés automatizálás
  A konfiguráció kezelés rendszer (részleges) automatizálása segíti az emberi hibákból vagy figyelmetlenségekből bekövetkező kockázatok csökkentését.
- ACM_CAP.4 A generálás támogatása és elfogadási eljárások
  Igen fontos, hogy a TOE változásait megfelelően ellenőrizzék. Az ACM_CAP.4 annyival szigorúbb elvárásokat fogalmaz meg a CIMC védelmi profil 3-as biztonsági szintjének ACM_CAP.3 követelményéhez képest, hogy egy elfogadási eljárás kidolgozásának és betartásának megkövetelésével garantálja, hogy a módosított vagy újra generált konfiguráció tételeket csak megfelelő ellenőrzés után fogadják el a TOE generálása során.
- ALC_LCD.1 A fejlesztő által meghatározott életciklus modell
  Ez a követelmény (a fejlesztésre és a karbantartásra vonatkozó életciklus modell megfogalmazásával) hozzájárul a fejlesztés és karbantartás megfelelő kezeléséhez és ellenőrzéséhez.

8.5.3 A CC EAL4 értékelési garanciaszint megemelésének az indoklása

A CIMC védelmi profil 3-as biztonsági szintjén elvárja az ALC_FLR.2 (Hibajelentési eljárások) követelmény teljesítését, mely sem az EAL3, sem az EAL értékelési garanciaszintnek nem képezi részét. Tehát a CIMC védelmi profil 3-as biztonsági szintjének való megfelelés célkitűzése indokolja a ALC_FLR.2 követelménnyel való megemelést.

8.6 Az összefoglaló előírás indoklása

A 8-10. táblázat visszavezeti az informatikai biztonsági funkciókat a TOE funkcionális biztonsági követelményeire. Ennek alapján látható, hogy melyik informatikai biztonsági funkció mely TOE funkcionális biztonsági követelményeket elégíti ki, és hogy minden informatikai biztonsági funkció hozzájárul a TOE legalább egy funkcionális biztonsági követelményének a kielégítéséhez (minden biztonsági funkció szükséges).

A 8-11. táblázat a TOE funkcionális biztonsági követelményeit vezeti vissza a biztonsági funkciókra. Ebből az látható, hogy a TOE egyes funkcionális biztonsági követelményeit melyik informatikai biztonsági funkció elégíti ki, és hogy minden funkcionális biztonsági követelményt kielégít egy biztonsági funkció (a biztonsági funkciók elégségesek).

8-10. táblázat:
A biztonsági funkciók visszavezetése a funkcionális biztonsági követelményekre

Biztonsági funkció	Biztonsági alfunkció	funkcionális biztonsági követelmény (melynek teljesítéséhez az adott BF hozzájárul)
BF1 Bizalmi munkakörök kezelése		FMT_SMF.1 (iteráció 2), FMT_SMR.2 (iteráció 2), FMT_MOF.1 (iteráció 2), FMT_MSA.1, FMT_MSA.2, FMT_MSA.3 FMT_MTD.1 (iteráció 2)
BF2 Időszinkronizálás		FPT_STM.1 (iteráció 2).
BF3 Azonosítás és hitelesítés	BF3.1 A felhasználó hitelesítése	FIA_ATD.1 (iteráció 2), FIA_UID.1 (iteráció 2), FIA_UAU.1 (iteráció 2), FIA_USB.1 (iteráció 2)
	BF3.2 A hitelesítési hiba kezelése	FIA_AFL.1 (iteráció 2)
	BF3.3 A titok ellenőrzése	FIA_SOS.1.
BF4 Hozzáférés ellenőrzés		FDP_ACC.1 (iteráció 2), FDP_ACF.1 (iteráció 2), FPT_RVM.1 (iteráció 2)
BF5 Kulcskezelés és kriptográfiai műveletek	BF5.1: NCA magánkulcs exportálása HSM-ből, helyreállítása (HSM-be)	FMT_MTD_CIMC.7
	BF5.2: Titkosító magánkulcsok kezelése	FMT_MTD_CIMC.4, FMT_MTD_CIMC.5, FDP_ACF_CIMC.2, FDP_ETC_CIMC.5
	BF5.3: Felhasználói titkos kulcsok kezelése	FDP_ACF_CIMC.3
	BF5.4: Kriptográfiai műveletek végzése	FCS_COP.1 (iteráció 2), FCS_CKM_CIMC.5
	BF5.5: Nyilvános kulcsok védelme	FDP_SDI_CIMC.3

BF6 Biztonsági naplózás	BF6.1: Napló adatok generálása megfelelő adatokkal	FAU_GEN.1 (2. iteráció), FAU_GEN.2 (2. iteráció)
	BF6.2: A napló adatok rendelkezésre állásának biztosítása (az elvesztés megakadályozása)	FAU_STG.4 (iteráció 2)
	BF6.3: A naplózandó adatok kiválasztása	FAU_SEL.1 (iteráció 2)
	BF6.4: A napló választható áttekintése	FAU_SAR.1 (iteráció 2), FAU_SAR.3 (iteráció 2)
	BF6.5 Korlátozott naplómegtekintés	FAU_SAR.1 (iteráció 2), FAU_SAR.3 (iteráció 2)
	BF6.6: Riasztás generálása	FAU_SAA.1, FAU_ARP.1
	BF6.7 A napló adatok sértetlenségének garantálása	FAU_STG.1 (iteráció 2), FPT_CIMC_TSP.1
BF7 Mentés és helyreállítás	BF7.1 Mentés generálása	FDP_CIMC_BKP.1
	BF7.2 A mentési információ sértetlenségének és bizalmasságának biztosítása	FDP_CIMC_BKP.2
	BF7.3 Helyreállítás	FDP_CIMC_BKP.1
BF8 Archiválás	BF8.1 Archív adatok generálása	FDP_CWA_ARC.1
	BF8.2 Szelektálható keresés az archivált adatok között	FDP_CWA_ARC.2
	BF8.3 Az archivált adatok sértetlenségének és bizalmasságának biztosítása	FDP_CWA_ARC.3
BF9 Adat export	BF9.1 Eredet bizonyítás és eredet ellenőrzés	FCO_NRO_CIMC.3, FCO_NRO_CIMC.4
	BF9.2 A belső adatkommunikáció védelme	FDP_ITT.1 (iteráció 3,4), FPT_ITT.1 (iteráció 3,4)
BF10 Tanúsítvány előállítás		FDP_CIMC_CER.1 FMT_MOF_CIMC.3
BF11 Visszavonás kezelés		FMT_MOF_CIMC.5, FMT_MOF_CIMC.6
BF12 Visszavonás állapot		FDP_CIMC_CRL.1, FDP_CIMC_OCSP.1 FDP_CIMC_CSE.1
BF13 Időbélyegzés		FDP_CWA_TS.1, FMT_MOF_CWA.1

8-11. táblázat:
A funkcionális biztonsági követelmények visszavezetése a biztonsági funkciókra

funkcionális biztonsági követelmény		Biztonsági funkció
FAU_ARP.1	Biztonsági riasztások	6
FAU_GEN.1	Napló adatok generálása (iteráció 2)	6
FAU_GEN.2	A felhasználói azonosítóval való összekapcsolás (iteráció 2)	6
FAU_SAA.1	A biztonság potenciális megsértésének vizsgálata	6
FAU_SAR.1	Napló áttekintés (iteráció 2)	6
FAU_SAR.3	Kiválogatható napló áttekintés (iteráció 2)	6
FAU_SEL.1	Kiválasztható napló (iteráció 2)	6
FAU_STG.1	A naplóesemények védett tárolása (iteráció 2)	6
FAU_STG.4	A napló adatok elvesztésének meggátolása (iteráció 2)	6
FCO_NRO_CIMC.3	Kötelező eredet bizonyítás és eredet ellenőrzés	9
FCO_NRO_CIMC.4	Az eredet fokozott ellenőrzése	9
FCS_COP.1	Kriptográfiai műveletek (iteráció 2)	5
FCS_CKM_CIMC.5	A TOE magán és titkos kulcsának nullázása	5
FDP_ACC.1	Részleges hozzáférés ellenőrzés (iteráció 2)	4
FDP_ACF.1	Biztonsági tulajdonság alapú hozzáférés ellenőrzés (iteráció 2)	4
FDP_ACF_CIMC.2	A felhasználói magánkulcs bizalmasságának védelme	5
FDP_ACF_CIMC.3	A felhasználói titkos kulcs bizalmasságának védelme	5
FDP_CIMC_BKP.1	CIMC mentés és visszaállítás	7
FDP_CIMC_BKP.2	Kiterjesztett CIMC mentések és visszaállítások	7
FDP_CWA_ARC.1	Archiválás	8
FDP_CWA_ARC.2	Szelektálható keresés az archívumban	8
FDP_CWA_ARC.3	Kiterjesztett archiválás	8
FDP_CIMC CER.1	Tanúsítvány előállítás	10
FDP_CIMC CRL.1	Tanúsítvány visszavonási lista érvényesítés	12
FDP_CIMC CSE.1	Tanúsítvány állapot export	12
FDP_CIMC_OCSP.1	OCSP alap-válasz érvényesítés	12
FDP_CWA_TS.1	Időbélyeg előállítás	13
FDP_ETC_CIMC.5	Kiterjesztett felhasználói magán és titkos kulcs export	5
FDP_ITT.1	A belső adatátvitel alapszintű védelme (iteráció 3 és 4)	9
FDP_SDI CIMC.3	A tárolt nyilvános kulcs sértetlenségének figyelése és reagálás	5
FIA_AFL.1	Hitelesítési hibák kezelése (iteráció 2)	3
FIA_ATD.1	Felhasználói tulajdonságok megadása (iteráció 2)	3
FIA_SOS.1	A titkok ellenőrzése	3
FIA_UAU.1	A hitelesítés időzítése (iteráció 2)	3
FIA_UID.1	Az azonosítás időzítése (iteráció 2)	3
FIA_USB.1	Felhasználó - szubjektum összerendelése (iteráció 2)	3
FMT_MOF.1	A biztonsági funkciók viselkedésének kezelése (iteráció 2)	1
FMT_MOF_CIMC.3	Kiterjesztett tanúsítvány profil menedzsment	10
FMT_MOF_CIMC.5	Kiterjesztett tanúsítvány visszavonási lista profil menedzsment	11
FMT_MOF_CIMC.6	OCSP profil menedzsment	11
FMT_MOF_CWA.1	Időbélyeg profil menedzsment	13
FMT_MSA.1	Biztonsági tulajdonságok kezelése	1
FMT_MSA.2	Biztonságos biztonsági tulajdonságok	1
FMT_MSA.3	Statikus tulajdonságok kezdeti értékadása	1
FMT_MTD.1	TSF adatok kezelése (iteráció 2)	1
FMT_MTD_CIMC.4	A TSF magánkulcs bizalmasságának védelme	5
FMT_MTD_CIMC.5	A TSF titkos kulcs bizalmasságának védelme	5
FMT_MTD CIMC.7	Kiterjesztett TSF magán és titkos kulcs export	5
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	6
FPT_RVM.1	A TSP megkerülhetetlensége (iteráció 2)	4
FPT_ITT.1	A belső adatátvitel alapszintű védelme (iteráció 3 és 4)	9
FPT_STM.1	Megbízható időbélyegzés (iteráció 2)	2

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**
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./
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
IIS	**Internet Information Server**	/A Microsoft cég webszerver terméke./
NHH		**Nemzeti Hírközlési Hatóság**
ODBC	**Open Database Connectivity**	/Szabványos adatbázis interfész./
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./
SAR	**Security Assurance Requirement**	**Garanciális biztonsági követelmény** /A TOE által kielégítendő garanciális biztonsági követelmény, melyeket az 5.3 alfejezet határoz meg./
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./

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
SSL	**Secure Socket Layer**	Bizalmasságot és hitelesítést biztosító protokoll.
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./
TLS	**Transport Layer Security**	Bizalmasságot és hitelesítést biztosító protokoll (az SSL legújabb verziója).
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./
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./