MultiSigno V3 SDK
aláíró alkalmazás fejlesztő készlet
v3.0.1 /r249/

Biztonsági előirányzat

Verzió:	v1.0
Dátum:	2006. május 1.
Megrendelő:	Kopint-Datorg Zrt.
Fájl:	MultiSigno_ST_v1.0.pdf
Minősítés:	Nyilvános
Oldalak:	78

Tartalomjegyzék

Változás kezelés

Verzió	Dátum	Leírás	Készítette
v0.3	2006.02.16.	MultiSigno v3.0.1 Biztonsági előirányzat szerkezet kialakítása	Juhász Judit
v0.5	2006.03.14.	MultiSigno v3.0.1 Biztonsági előirányzat 1-6. fejezeteinek elkészítése	Juhász Judit
v0.9	2006.04.15.	MultiSigno v3.0.1 Biztonsági előirányzat 7-9. fejezeteinek elkészítése, 1-6. fejezetek pontosítása és kiegészítése	Juhász Judit
v1.0	2006.05.01.	MultiSigno v3.0.1 Biztonsági előirányzat módosítások átvezetése a fejlesztői dokumentációk és értékelői észrevételek alapján	Juhász Judit

1. Bevezetés

Ez a fejezet dokumentum-kezelő és áttekintő információkat tartalmaz.
Az "Azonosítás" rész a biztonsági előirányzatok azonosításhoz, katalogizálásához, regisztrációba vételéhez, illetve hivatkozásokhoz szükséges azonosító és leíró információkat tartalmazza.
Az "Áttekintés" rész egy potenciális felhasználó számára ad olyan részletességű áttekintést, melynek alapján eldöntheti a témában való érdekeltségét.

1.1 Azonosítás

Cím:	MultiSigno V3 SDK aláíró alkalmazás fejlesztő készlet v3.0.1 /r249/ - Biztonsági előirányzat
Az értékelés tárgya:	MultiSigno V3 SDK aláíró alkalmazás fejlesztő készlet v3.0.1 /r249/
Az értékelés tárgya rövid neve:	MultiSigno v3.0.1
Értékelési garancia szint:	MIBÉTS kiemelt (EAL4)
Biztonsági funkcióerősség:	SOF-alap
Verzió szám:	3.0.1
Dátum:	2006. május 1.
Szerző:	Juhász Judit
Szponzor szervezet:	KOPINT-DATORG Rt.
Alapot képező védelmi profil:	USMC PKE PP with < Certification Path Validation (CPV) – Basic, PKI Signature Generation, PKI Signature Verification, PKI Encryption using Key Transfer Algorithms, PKI Decryption using Key Transfer Algorithms, Certificate Revocation List (CRL) Validation > at EAL <4> with augmentation
Kiegészítés:	Ebben a biztonsági előirányzat az eredeti PKE PP család választott csomagjain túl kiegészült egy „Időbélyegzés” csomaggal, amely nem része az eredeti PKE PP családnak.

1.2 Áttekintés

Az értékelés tárgya egy olyan fejlesztő készlet, melynek segítségével szabványos (X.509 szabványon alapuló) nyilvános kulcsú szolgáltatásokat biztosító alkalmazások fejleszthetők. A fejlesztő készlet által támogatott nyilvános kulcsú szolgáltatások az alábbiak:

- elektronikus aláírás létrehozása;
- elektronikus aláírás ellenőrzése, a kapcsolódó tanúsítvány útvonal felépítési és érvényesítési szolgáltatásokkal;
- szimmetrikus AES ECB és CBC, 3DES-CBC, RC2 -CBC és aszimmetrikus (RSA, PKCS#1 v1.5) titkosítás és megoldás
- időbélyegzés (kérése és ellenőrzése).

Ennek alapján a MultiSigno v3.0.1 fejlesztői készlet segítségével olyan alkalmazások fejleszthetők, melyek a nyilvános kulcsú technológia alapján bizalmasságot, sértetlenséget, hitelesítést és letagadhatatlanságot biztosító szolgáltatásokat képesek nyújtani.
A biztonsági előirányzat készítője egy csomag koncepcióra épülő, Common Criteria szerint tanúsított védelmi profil családot (PKE PP) használt fel alapul jelen dokumentum követelményrendszerének kialakításához, de megfelelőséget nem vállalt fel ezzel a védelmi profillal. A biztonsági előirányzat kiegészült egy olyan csomaggal is, amely az időbélyegzés kliens oldali követelményeit fogalmazza meg.
A PKE PP védelmi profil családot az USA Védelmi Minisztériuma számára dolgozták ki. A védelmi profil család a csomag koncepció bevezetésével több ezer védelmi profil előállítására alkalmas. A nagyszámú variációk közül ebben a biztonsági előirányzatban egy olyan csomag-összeállítás került kiválasztásra, módosításra és kiegészítésre, mely megfelel a MultiSigno v3.0.1 igényeinek.
Az alábbi táblázat az alapul szolgáló PKE PP védelmi profil családból kiválasztott csomagokat és az időbélyeg kliens csomagot tekinti át, amiket a MultiSigno v3.0.1 megvalósít.

Csomagnév	Funkcionalitás	Függőség
PKE PP védelmi profilból átvett és a MultiSigno v3.0.1-nek megfelelően módosított csomagok		
Tanúsítási útvonal érvényesség ellenőrzése (CPV) - Alap	Végrehajtja az összes X.509 érvényesség ellenőrzést, kivéve a szabályzat és név megszorítás feldolgozását	Nincs
PKI aláírás létrehozás	Magánkulcsot használ az aláírás létrehozására Aláírási információk generálása	Nincs
PKI aláírás ellenőrzés	Feldolgozza az aláírási információkat Nyilvános kulcsot használ az aláírás ellenőrzésére	Tanúsítási útvonal érvényesség ellenőrzése (CPV) – Alap
PKI titkosítás kulcs átviteli algoritmusokkal	Elkészíti a titkosításhoz tartozó kiegészítő információkat (boríték) Nyilvános kulcsot használ a titkosításhoz	Tanúsítási útvonal érvényesség ellenőrzése (CPV) - Alap
PKI titkosítás visszafejtése (dekódolása) kulcs átviteli algoritmusokkal	Feldolgozza a titkosításhoz tartozó kiegészítő információkat Magánkulcsot használ a dekódoláshoz	Nincs
Tanúsítvány visszavonási lista (CRL) érvényesítés	Megszerzi a CRL-t Feldolgozza a CRL-t	Nincs
Kiegészítő csomag		
Időbélyeg kérése és ellenőrzése	Időbélyeget kér és ellenőriz az RFC 3161-nek megfelelően	Tanúsítási útvonal érvényesség ellenőrzése (CPV) – Alap

1.1 táblázat: A PKE –ből felhasznált csomagok

Az 1.1 táblázat az alapul szolgáló védelmi profilból átvett csomagokat és a Kiegészítő csomagot tekinti át. A 2. és további fejezetekben olvasható részletesebb leírás az eredeti csomagokat (elsősorban a Tanúsítási útvonal érvényesség ellenőrzése csomagot) érintő módosításokról.

1.3 Kapcsolódó dokumentumok

- Public Key-Enabled Application Family of Protection Profiles version 2.5 31, October 2002.
- 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
- International Organization for Standards/Internet Electrotechnical Committee (ISO/IEC) 9594-8:"Information Technology- Open Systems Interconnection-The Directory: Public Key and Attribute Certificate Frameworks" (X.509 Standard)
- International Standard ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security
- Common Methodology for Information Security Evaluation (CEM) Version 1.0, August 1999

1.4 A biztonsági előirányzat szerkezete

A 2., 3., és 4. fejezetek a MultiSigno v3.0.1 leírását, a feltételezéseket, fenyegetéseket, illetve a biztonsági célokat adják meg. Ezek az egyes csomagok szerint külön kerültek leírásra.
Az 5.1-5.2 alfejezetek az egyes csomagokra a funkcionális biztonsági követelményeket írják le. Az 5.3 alfejezet a MIBÉTS kiemelt garanciaszint követelményeit írja le.
A 6. fejezet a MultiSigno v3.0.1 által megvalósított biztonsági funkciókat specifikálja.
A 7. fejezet a védelmi profiloknak való megfelelésről nyilatkozik.
A 8. fejezet tartalmazza az indoklásokat.
A 9. fejezet pedig a CC és PKI szakkifejezések magyarázatát és a használt rövidítések listáját tartalmazza.

1.5 Common Criteria (Közös szempontok) megfelelőség

Ez a biztonsági előirányzat a CC 2.3 verziója felhasználásával készült (ISO/IEC 15408 IT biztonság értékelési követelményei, 1. rész: Bevezetés és általános modell, 2. rész: Funkcionális biztonsági követelmények, 3. rész: Garanciális biztonsági követelmények).
A MultiSigno v3.0.1 biztonsági előirányzatra a CC-nek való megfelelőség szempontjából az alábbi nyilatkozat tehető:

- kiterjeszti a 2. részt,
- megfelel a 3. résznek.

A "kiterjeszti a 2. részt" definíciója a CC 1. rész 7.4 szakasza szerint: „Kiterjeszti a 2. részt – Egy PP vagy egy TOE kiterjeszti a 2. részt, ha a funkcionális követelmények olyan funkcionális összetevőket is magukban foglalnak, amelyek nem szerepelnek a 2. részben."
A "megfelel a 3. résznek" definíciója a CC 1. rész 7.4 szakasza szerint:
"Egy PP vagy egy TOE akkor felel meg a 3. résznek, ha a garanciális követelmények csak a 3. részben szereplő garanciális összetevőkön alapulnak."

Az MultiSigno v3.0.1 felhasználja a PKE PP család követelményeit és csomag-filozófiáját, de módosítja, kiegészíti azt, ezért jelen biztonsági előirányzat PP-megfelelőségi nyilatkozatot nem tesz.

2 Az értékelés tárgya (TOE) leírása

2.1 Áttekintés

A MultiSigno v3.0.1 fejlesztői függvénykönyvtár az alábbi nyilvános kulcs szolgáltatásokkal rendelkezik:

- Biztonságosan kezel kulcsokat, megbízható pontokat és tanúsítványokat.
- Elfogad és feldolgoz X509 v3 nyilvános kulcs tanúsítványokat.
- Képes a szükséges visszavonási adatok megszerzésére.
- Ellenőrzi minden tanúsítvány érvényességét, az X.509 szabványban [ISO 9594-8] leírt eljárások felhasználásával, beleértve a visszavonás ellenőrzést is.
- Hozzáfér pontos és megbízható időforráshoz a tanúsítványok, visszavonási adatok és alkalmazási adatok dátumának, idejének ellenőrzése érdekében.
- Minősített aláírás létrehozása esetén együttműködik a magyar jogszabályok által megkövetelt módon minősített aláírás létrehozásához szükséges tanúsított BALE eszközzel, vagy fokozott biztonságú aláírások esetén képes szabványos szoftveres kulcstároló állományok vagy Kriptográfiai hardver eszköz (KHE) biztonságos kezelésére.
- Gyűjti, tárolja és karbantartja a digitális aláírás jövőbeni ellenőrzéséhez szükséges adatokat.
- Képes automatikusan választani több magán rejtjelező kulcsból, ha nyilvános kulcs alapú megoldást végez.

2.2 Megközelítés

Jelen biztonsági előirányzat a PKE PP családon alapul (bár az ennek való megfelelőség nem teljesül), ki lettek választva a TOE funkcionalitásának megfelelő csomagok, illetve ki lettek egészítve egy, az időbélyegzésre vonatkozó csomaggal is.

2.2.1 CC 2. rész és kiterjesztett 2. rész funkcionális biztonsági követelmények

A CC 2. részét felhasználva a biztonsági szempontból fontos követelmények kialakításához a biztonsági előirányzat csak a PKI szolgáltatás biztonsági szempontjaival foglalkozik. A PP, így jelen ST nem tárgyalja például a tanúsítványok és CRL-ek megszerzésének módját, mert ezek biztonsága nem függ attól, hogyan kerültek az alkalmazás birtokába; a biztonságukat a digitális aláírás ellenőrzése biztosítja.
A CC hozzáférés ellenőrzéssel kapcsolatos összetevők nem alkalmasak a tanúsítvány és visszavonási információkat (pl. CRL, OCSP válasz) feldolgozó követelményekként, így a CC 2. részét ki kellett terjeszteni.

2.3 A TOE meghatározása

Ez a szakaszban a TOE típusát és struktúráját ismertetjük, bemutatjuk kapcsolatait és határait más összetevők felé.

2.3.1 A TOE típusa és összetevői

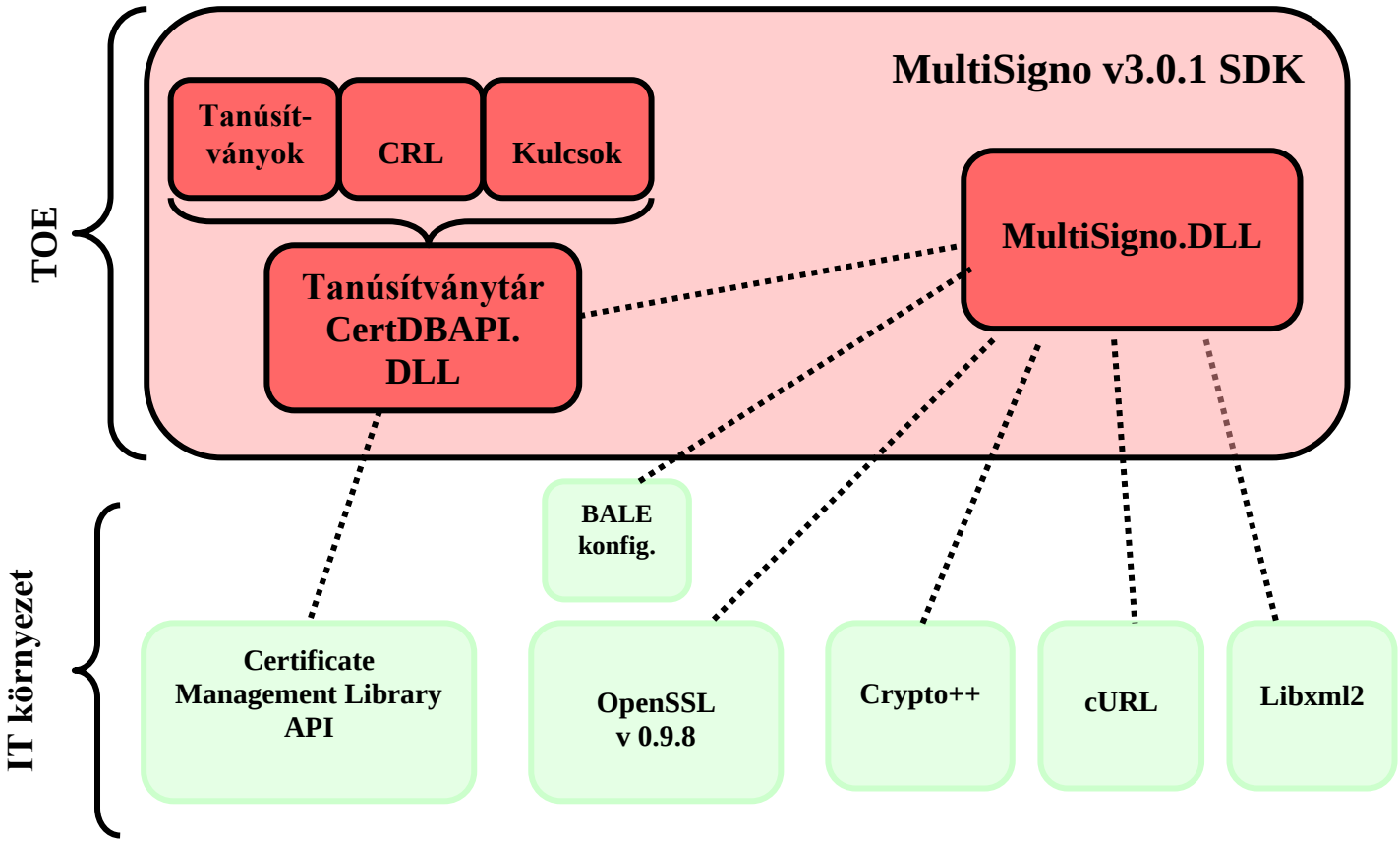
A MultiSigno v3.0.1 szoftverfejlesztők számára készült, C++ felületen elérhető fokozott biztonságú és minősített elektronikus aláírás elkészítésére alkalmas függvénykönyvtár, amely C++ osztályok használatával érhető el. Tartalmazza az aláírás létrehozásával, ellenőrzésével kapcsolatos funkcionalitást. Az alapfunkcionalitás megfelelő működéséhez felhasznál nyílt forrású könyvtárakat, így a kriptográfiai műveleteket az OpenSSL segítségével, a tanúsítási útvonal érvényesség ellenőrzését a Certificate Management Library felhasználásával valósítja meg.

A MultiSigno v3.0.1 képes fokozott biztonságú és minősített elektronikus aláírások létrehozására, az alábbiak szerint:

- Fokozott biztonságú aláírás létrehozása esetén:
    - A TOE-t biztonságos aláírás létrehozó eszköz nélkül használják elektronikus aláírások generálására és ellenőrzésére. Használható KHE (kriptográfiai hardver eszköz) vagy PKCS#12 szoftveres kulcstároló állomány.
- Minősített elektronikus aláírás esetén:
    - Minősített aláírás létrehozása esetén kötelező tanúsított, NHH által nyilvántartásba vett BALE használata. Az aláírás létrehozásához használt tanúsítványnak minősítettnek kell lennie. A BALE-hez való hozzáférés szabványos PKCS#11 interfészen keresztül valósul meg.

A MultiSigno v3.0.1 saját tanúsítványtárat használ a működése során. A függvénykönyvtár által kezelni képes digitális aláírás formátum: Melasz-Ready XAdES.

Az 1. ábra a MultiSigno v3.0.1 összetevőit tekinti át.



1. ábra
A MultiSigno v3.0.1 összetevői és a közöttük lévő alapvető kapcsolatok

A TOE IT környezetéhez tartozó összetevők, melyek nem részei jelen értékelésnek:

- **Crypto ++:** Kriptográfia műveletek végrehajtása (lenyomatolás, szimmetrikus és asszimetrikus titkosítás, kulcsgenerálás).
- **Libxml2:** XML struktúrák értelmezése, előállítása.
- **OpenSLL v0.9.8**: Tanúsítványok értelmezése, http és https kapcsolatok felépítése, aláírás érték létrehozása és ellenőrzése, PKCS 7 és PKCS 12 csomagok értelmezése és létrehozása.
- **cURL v.7.13.1:** Http és https kapcsolatok felépítése (OpenSLL segítségével).
- **Certificate Management Library (CML) v2.5:** Tanúsítványok és visszavonási listák értelmezése és tárolása, valamint tanúsítványok érvényességének vizsgálata
- **BALE konfig**: A MultiSigno v3.0.1 által támogatott BALE eszközök információinak tárolása.

A MultiSigno v3.0.1 értékelés hatáskörébe eső összetevők az alábbiak:

- **MultiSigno SDK CertDBAPI**: A tanúsítványtár szolgáltatásokat végző összetevő.

- **MultiSigno SDK MultiSigno:** Az elektronikus aláírással, kriptográfiával kapcsolatos szolgáltatások.

2.3.2 A MultiSigno v3.0.1 funkcionális csomagjai

A 2.1 táblázat a MultiSigno v3.0.1 által megvalósított csomag-elv alapján szervezett funkciók összegzését adja, a táblázat után pedig a csomagok funkcionalitását találhatjuk.
Jelen csomag összeállítás jelentősen eltér az eredeti PKE PP csomagjaitól, mivel abban a „Tanúsítási útvonal érvényesség ellenőrzése - Alap" csomag a PP-nek megfelelőséget vállaló TOE szerves részét képezte. A MultiSigno v3.0.1 azonban a tanúsítási útvonal érvényesség ellenőrzését az értékelés hatáskörén kívül eső függvénykönyvtárral valósítja meg.
Ezen kívül a biztonsági előirányzat tartalmaz az eredetihez képest új csomagot, ami az időbélyeg kérések és válaszok kezelésére vonatkozik.

Az említett Certificate Management könyvtár magas szintű hozzáférést biztosít a nyilvános kulcsokhoz és X.509 tanúsítványokhoz. A Certfiicate Management könyvtár egyszerűbbé teszi a nyilvános kulcs kriptográfia használatát azáltal, hogy végrehajtja az X.509 tanúsítványokra vonatkozó összes feldolgozást az alkalmazás számára. Teljes mértékben megfelel a mértékadó szabványoknak (X.509 2000 és IETF RFC 3280).
A MultiSigno v3.0.1 feldolgozza a Certificate Management által szolgáltatott eredményeket.

Csomag neve	**Funkcionalitás**	**Függések**	**Megjegyzés**
Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése	Végrehajtja az összes X.509 érvényesség ellenőrzést, kivéve a szabályzat és név megszorítás feldolgozását	Nincs	**Értékelés hatáskörén kívüli csomag,** ebben a fejezetben a teljesség miatt szerepel, követelményeket a MultiSigno v3.0.1 mint TOE nem fogalmaz meg erre.
PKI aláírás létrehozás	Magánkulcs használata aláírás létrehozására Aláírási információk generálása	Nincs	
PKI aláírás ellenőrzés	Feldolgozza az aláírási információkat Nyilvános kulcsot használ az aláírás ellenőrzésére	Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése	Lásd táblázat 1. sorának megjegyzését.

PKI titkosítás kulcs átviteli algoritmusok használatával	Rejtjelezési boríték információkat generálja Nyilvános kulcsot használ a rejtjelezéshez	Tanúsítási útvonal érvényesség ellenőrzése és tanúsítvány ok kezelése	Lásd táblázat 1. sorának megjegyzését.
PKI megoldás kulcs átviteli algoritmusok használatával	Rejtjelezési boríték információkat feldolgozza Magánkulcsot használ a megoldáshoz	Nincs	
CRL érvényesség ellenőrzés	CRL lehívása CRL feldolgozása	Nincs	

Kiegészítő csomag

Időbélyeg kérése és ellenőrzése	Időbélyeget kér és ellenőriz az RFC 3161-nek megfelelően	Tanúsítási útvonal érvényesség ellenőrzése és tanúsítvány ok kezelése	Lásd táblázat 1. sorának megjegyzését.

2.1 táblázat – A MultiSigno v3.0.1 PKI csomagok áttekintése

2.3.2.1 Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése csomag

Az alapul szolgáló védelmi profilban a „**Tanúsítási útvonal érvényesség ellenőrzése – Alap**” csomag (CPV - Alap) gondoskodik az X.509 érvényesség ellenőrzésről. Ez a csomag a tanúsítási útvonal érvényességének ellenőrzésével és a tanúsítási útvonal felépítésével foglalkozik. A feldolgozás megfelel a X.509 és PKIX szabványoknak.
Háromféle nyilvános kulcs tanúsítványt különböztetünk meg:

- **Megbízható pontok**: Ezek önaláírt tanúsítványok, melyek nem igényelnek semmilyen érvényesség ellenőrzést. A megbízható pont (önaláírt tanúsítvány) általában tanúsítvány formában jelenik meg. A megbízható pont elsődleges célja a megkülönböztető név (Distinguished Name), a nyilvános kulcs, az algoritmus azonosító és a nyilvános kulcs paraméterek (ha vannak ilyenek) megállapítása.
- **Közbenső tanúsítványok:** Ezek a CA-k számára kibocsátott tanúsítványok. Egy tanúsítási útvonal minden tanúsítványa ennek tekintendő, kivéve az utolsót.
- **Végtanúsítvány:** A tanúsítási útvonal legutolsó tanúsítványa, melyet a szóban forgó egyed (aláíró) részére bocsátottak ki.

A 2.3.2-ben írtaknak megfelelően a MultiSigno v3.0.1 értékelés hatókörének nem része a CML csomag. Ennek megfelelően ezt a MultiSigno v3.0.1 környezeteként tekintjük. Szerepeltetjük a rá vonatkozó veszélyeket, biztonsági célokat, de a konkrét követelményeket nem.

2.3.2.2 PKI aláírás létrehozás csomag

A **PKI aláírás létrehozás** csomag aláírás létrehozáskor a magánkulcs biztonságos használatára és aláírási információk generálására tartalmaz funkciókat.

A TOE az aláírás létrehozás és ellenőrzést az alábbi digitális aláírás sémák szerint valósítja meg:

- RSA algoritmus 1024 bit kulcshossz,
- SHA-1, SHA-256, SHA-386, SHA-512 lenyomatoló algoritmus.

A MultiSigno v3.0.1 minősített elektronikus aláírás létrehozása esetén kezeli a magánkulcs műveletekhez szükséges külső biztonságos aláírás létrehozó eszközt (tanúsított, NHH által nyilvántartásba vett BALE), amely eszközt a magánkulcs az életciklusa során nem hagy el, és az aláírás létrehozása szigorúan az eszközön belül történik.

2.3.2.3 PKI aláírás ellenőrzés csomag

A PKI aláírás ellenőrzés csomag az aláírás ellenőrzéséhez felhasznált tanúsítvány tanúsítási útvonal érvényességének ellenőrzésétől függ, amit a CML, értékelés hatókörén kívül eső könyvtár hajt végre. Aláírási információk, az elektronikus aláírás feldolgozására és a nyilvános kulcs használatára tartalmaz funkciókat.

2.3.2.4 PKI titkosítás kulcs átviteli algoritmusok használatával csomag

A **PKI titkosítás kulcs átviteli algoritmusok használatával** csomag a CPV – Alap csomagtól, azaz a CML által szolgáltatott eredménytől függ. Kulcs átviteli algoritmusokat alkalmazó (pl. RSA) nyilvános kulcsú titkosítás végrehajtására tartalmaz funkciókat.

A MultiSigno v3.0.1 a titkosító-megoldó funkcionalitása részeként adatok rejtjelezésére és megoldására alkalmazható algoritmusokat valósít meg. A kulcsok kezelésének problémaköre kívül esik a MultiSigno v3.0.1határain. A MultiSigno v3.0.1 funkciókat hívó alkalmazás gondoskodik a kulcsok MultiSigno v3.0.1 felé juttatásáról. A MultiSigno v3.0.1 nem módosítja az alkalmazástól kapott kulcsokat, és biztosítja, hogy a kulcsok védve legyenek más alkalmazások és egyedek elől.

A MultiSigno v3.0.1 a következő aszimmetrikus titkosító algoritmusokat valósítja meg:

- RSA algoritmus 1024 bit kulcshossz,
- lenyomatoló algoritmus: SHA-1, SHA-256, SHA-384, SHA-512.

A MultiSigno v3.0.1 az alábbi blokkos rejtjelezési algoritmusokat valósítja meg:

- AES 256 bit [FIPS PUB 197] ECB és CBC mód;
- 3DES CBC mód;
- RC2 CBC mód.

2.3.2.5 PKI megoldás kulcs átviteli algoritmusok használatával csomag

Ez a csomag kulcs átviteli algoritmusokat alkalmazó (pl. RSA) nyilvános kulcsú megoldás végrehajtására tartalmaz funkciókat. Mivel csak a megoldó fél magánkulcsa használt, ez a csomag nem követeli meg a tanúsítvány útvonal feldolgozásának funkcióit.

2.3.2.6 Tanúsítvány visszavonási lista (CRL) érvényesség ellenőrzése csomag

A CRL érvényesség ellenőrzése csomag lehetővé teszi, hogy a MultiSigno v3.0.1 ellenőrizzen egy CRL-t. A csomag használható olyan CRL feldolgozására, amelyre egy CRL szétosztó pont (CRLDP) kiterjesztés mutat egy tanúsítványban, amennyiben a CRL teljes CRL, melyet jelez az IDP és deltaCRLIndicator kiterjesztések hiánya.

2.3.2.7 Időbélyeg kérése és ellenőrzése csomag

Az „Időbélyeg kérése és ellenőrzése” csomag lehetővé teszi, hogy a MultiSigno v3.0.1 Időbélyeget kérjen egy időbélyegzés-szolgáltatótól, illetve ellenőrizze a kapott választ az RFC 3161-nek megfelelően.

2.4 Garanciális követelmények

A TOE értékelésre vonatkozó garanciakövetelménye: MIBÉTS kiemelt (EAL4).

3 A TOE biztonsági környezete

3.1 A biztonságos használattal kapcsolatos feltételezések

3.1 táblázat – Feltételezések az IT környezetre

Sor-szám	Feltételezés megnevezése	Leírás
1	**AE.Authorized_Users**	Az engedéllyel rendelkező felhasználók megbízhatók a tekintetben, hogy a számukra kijelölt funkciókat megfelelően hajtják végre.
2	**AE.Configuration**	A TOE-t megfelelően telepítik és konfigurálják.
3	**AE.Crypto_Module**	A TOE által meghívott kriptográfiai funkciókról feltételezés, hogy TOE hatáskörén kívüli modulok hajtják végre, melyek megbízhatónak tekinthetők a TOE által hívott, kriptográfiai funkciók megvalósítása terén. Minősített elektronikus aláírás létrehozása esetén a TOE környezetéről feltételezés, hogy tartalmaz egy vagy több NHH által nyilvántartott, tanúsított BALE-t, mely(ek) tárolják és védik az aláíró magánkulcsát, illetve végrehajtják a digitális aláírást.
4	**AE.Low**	A TOE-val szembeni támadási potenciált alacsonynak tételezzük fel.
5	**AE.Physical_Protection**	A környezetről feltételezzük, hogy fizikailag véd. A TOE szoftverről feltételezzük, hogy védett a jogosulatlan fizikai hozzáféréssel szemben.
6	**AE.PKI_Info**	A tanúsítvány és tanúsítvány visszavonási információk a TOE rendelkezésére állnak.
7	**AE.Time**	A környezetről feltételezzük, hogy GMT formában és a megkívánt pontossággal gondoskodik a pontos rendszeridőről.
8	**AE.TimeStamp**	A környezetről feltételezzük, hogy biztosítja az időbélyegzés szolgáltatóhoz való hozzáférést.

3.2 Általános biztonsági fenyegetések

Ez az alfejezet a MultiSigno v3.0.1-t fenyegető általános veszélyeket, a 3.3 alfejezet pedig a PKI-specifikus, csomagokra vonatkozó veszélyeket azonosítja. A támadott érték az értékelés tárgyán valamilyen formában áthaladó információ. Általánosságban, a veszély forrásai lehetnek (de nem kizárólagosan)
1) a MultiSigno-hoz hozzáférő olyan egyének, akik „átlagos" szakértelemmel, kevés erőforrással bírnak és közepes motiváció jellemzi őket (alacsony támadási potenciállal rendelkező támadók); vagy
2) a MultiSigno v3.0.1 hibája.

3.2 táblázat – Alapvető biztonsági fenyegetések

Sor-szám	Veszély megnevezése	Veszély leírása
1	**T.Attack**	A TOE értékek észrevétlen kompromittálódása következhet be egy (külső vagy belső) támadó jogosulatlan tevékenység végzésének kísérlete miatt.
2	**T.Bypass**	Jogosulatlan egyed vagy felhasználó meghamisíthatja a biztonsági tulajdonságokat vagy más adatokat a TOE biztonsági funkcióinak kikerülése és a TOE értékekhez való jogosulatlan hozzáférés megszerzése érdekében.
3	**T.Imperson**	Jogosulatlan egyed megszemélyesíthet egy jogosult TOE felhasználót, és ezáltal hozzáféréshez jut a TOE adatokhoz, kulcsokhoz és műveletekhez.
4	**T. Modify**	Egy támadó módosíthatja a TSF-et vagy más adatokat, például a tárolt biztonsági beállításokat vagy kulcsokat, hogy hozzáférést szerezzen a TOE-hoz és annak adataihoz.
5	**T.Object_Init**	Egy támadó jogosulatlanul hozzáférhet egy objektumhoz annak létrehozása során, ha a biztonsági tulajdonságokat nem állítják be, vagy bárki megadhatja azokat az objektum létrehozás során.
6	**T.Private_key**	Egy támadó egy felhasználónak adja ki magát a felhasználó magánkulcsának használata által.
7	**T.Role**	Egy felhasználó magasabb szintű jogosultságú szerepben jelenhet meg, mint amekkora neki megengedett, és ezt az emelt szintű jogosultságot használhatja fel jogosulatlan tevékenységekhez.
8	**T.Secure_attributes**	Egy felhasználó módosíthatja egy objektum biztonsági tulajdonságait, ami által jogosulatlanul hozzáfér az objektumhoz.
9	**T.Shoulder_Surf**	Egy jogosulatlan felhasználó a jogosult felhasználó válla fölötti kémleléssel megismeri a hitelesítési információkat a hitelesítési folyamat során.
10	**T.Tries**	Egy jogosulatlan egyed próbálgatás és hiba következtében kitalálhatja a hitelesítési információt.

3.3 PKI-specifikus biztonsági fenyegetések

3.3.1 Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése csomag

3.3 táblázat– A „ Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése” csomagot érintő veszélyek

Sorszám	Veszély megnevezése	Veszély leírása
1	**T.Certificate_Modi**	Egy jogosulatlan felhasználó módosíthat egy tanúsítványt, és ezáltal rossz nyilvános kulcs kerül felhasználásra.
2	**T.Expired_Certificate**	Lejárt (és feltehetően visszavont) tanúsítványt aláírás ellenőrzésre használnak.
3	**T.Masquarade**	Nem megbízható egyed (CA) tanúsítványokat bocsáthat ki álegyedeknek, miáltal ezek más jogosult felhasználónak adhatják ki magukat.
4	**T.No_Crypto**	A felhasználó nyilvános kulcsa és kapcsolódó információk nem állnak rendelkezésre a kriptográfiai funkció elvégzéséhez.
5	**T.Path_Not_Found**	Egy érvényes tanúsítási útvonal nem található valamely rendszerfunkció hiánya miatt.
6	**T.Revoked_Certificate**	Egy visszavont tanúsítvány érvényesként való használata a biztonság megsértését vonja maga után.
7	**T.User_CA**	Egy felhasználó CA-ként lép fel, és jogosulatlan tanúsítványokat bocsát ki.

3.3.2 PKI aláírás létrehozás csomag

Az alábbi veszélyek a „PKI aláírás létrehozás” csomagot jellemzik.

3.4 táblázat – A PKI aláírás létrehozás csomaggal kapcsolatos veszélyek

Sorszám	Veszély megnevezése	Veszély leírása
1	**T.Clueless_PKI_Sig**	A felhasználó jelzés hiányában csak helytelen tanúsítványokat próbál ki az aláírás során.
2	**T.Key_Leakage_Sig**	Az aláírás létrehozás után magán vagy titkos kulcsok válnak más folyamatok számára hozzáférhetővé.

3.3.3 PKI aláírás ellenőrzés csomag

Az alábbi veszélyek a "PKI aláírás ellenőrzés" csomagot jellemzik.

3.5 táblázat – A "PKI aláírás ellenőrzés" csomaggal kapcsolatos veszélyek

Sorszám	Veszély megnevezése	Veszély leírása
1	**T.Assumed_Identity_PKI_Ver**	Egy felhasználó az aláíró személyére mást feltételez egy PKI aláírás ellenőrzése során.
2	**T.Clueless_PKI_Ver**	A felhasználó jelzés hiányában csak helytelen tanúsítványokkal próbál ellenőrizni.

3.3.4 PKI titkosítás kulcs átviteli algoritmusok használatával csomag

Az alábbi veszélyek a "PKI titkosítás kulcs átviteli algoritmusok használatával" csomagot jellemzik.

3.6 táblázat – A "PKI titkosítás kulcs átviteli algoritmus használatával" csomaggal kapcsolatos veszélyek

Sorszám	Veszély megnevezése	Veszély leírása
1	**T.Assumed_Identity_WO_En**	Egy felhasználó a címzett személyére mást feltételez egy kulcs átviteli algoritmussal végrehajtott titkosítás során.
2	**T.Clueless_WO_En**	A felhasználó jelzés hiányában csak helytelen tanúsítványokkal próbál titkosítani, kulcs átviteli algoritmust használva.

3.3.5 PKI megoldás kulcs átviteli algoritmusok használatával csomag

Az alábbi veszélyek a "PKI dekódolás kulcs átviteli algoritmusok használatával" csomagot jellemzik.

3.7 táblázat – A "PKI dekódolás kulcs átviteli algoritmus használatával" csomaggal kapcsolatos veszélyek

Sorszám	Veszély megnevezése	Veszély leírása
1	**T.Garble_WO_De**	A felhasználó nem a megfelelő kulcs átviteli algoritmust vagy nem a megfelelő magánkulcsot alkalmazza, ami az adatok összekeveredését okozza.
2	**T.Key_Leakage_De**	A dekódolás után magán vagy titkos kulcsok válnak más folyamatok számára hozzáférhetővé.

3.3.6 Tanúsítvány visszavonási lista ellenőrzése (érvényesítése)csomag

Az alábbi veszélyek a „Tanúsítvány visszavonási lista (CRL) ellenőrzése” csomagra vonatkoznak.

3.8 táblázat – A CRL érvényességi csomaggal kapcsolatos veszélyek

Sorszám	Veszély megnevezése	Veszély leírása
1	**T.Replay_Revoc_Info_CRL**	A felhasználó elfogad egy régi CRL-t, mely következtében a TOE visszavont tanúsítványt érvényesnek fogad el.
2	**T.Wrong_Revoc_Info_CRL**	A felhasználó egy rossz CRL miatt elfogad egy visszavont tanúsítványt, vagy elutasít egy érvényeset.

3.3.7 Időbélyeg kérése és ellenőrzése csomag

Az alábbi veszélyek az „Időbélyeg kérése és ellenőrzése” csomagra vonatkoznak.

3.9 táblázat – Az időbélyeg kéréssel és ellenőrzéssel kapcsolatos veszélyek

Sorszám	Veszély megnevezése	Veszély leírása
1	**T.Replay_TimeStamp**	A felhasználó elfogad egy régi időbélyeg választ, mely következtében a TOE visszavont tanúsítványt érvényesnek fogad el.
2	**T.Wrong_TimeStamp_Info**	A felhasználó rossz időbélyeg válasz miatt elfogad egy visszavont tanúsítványt vagy visszautasít egy érvényeset.

3.4 Szervezeti biztonsági szabályok

Ezen biztonsági előirányzat nem tartalmaz szervezeti biztonsági szabályokat.

4 Biztonsági célok

Ez a fejezet azonosítja a MultiSigno v3.0.1 (4.2 alfejezet), illetve annak informatikai környezete (4.1 alfejezet) által teljesítendő biztonsági célokat
„OE" előtag jelöli a környezet által, „O" előtag pedig az értékelés tárgya által teljesítendő célokat.

4.1 A MultiSigno informatikai környezetére vonatkozó általános biztonsági célok

Az alábbiakban felsorolt biztonsági célok jelen biztonsági előirányzat alapját képező PKE PP-ből származnak, és minden, a PP-n családon alapuló ST-ben szerepeltetni kell ezeket. Azonban az alapul szolgáló védelmi profil család megengedi ezen biztonsági célok IT környezet általi kielégítését is, ezért ezeket „OE." Előtaggal jelöljük.
Ezen biztonsági célok IT környezeti célként való felvételét indokolja a termék (MultiSigno v3.0.1) típusa, a fejlesztői könyvtár-jelleg. A MultiSigno v3.0.1 az alá, illetve a fölé épülő IT környezetre alapoz (lásd 1. ábrát) az alábbi általános biztonsági célok teljesítése érdekében.

4.1 táblázat – A MultiSigno informatikai környezete által teljesítendő biztonsági célok

Sor-szám	Cél megnevezése	Cél leírása
1	OE.DAC	Az IT környezet TSF-nek ellenőriznie és korlátoznia kell a felhasználók hozzáféréseit a TOE értékekhez, egy megadott hozzáférés ellenőrzési szabályzatnak megfelelően.
2	OE.I&A	Az IT környezet TSF-nek egyedi módon azonosítania kell minden felhasználót, és hitelesíteni kell azok állítólagos azonosságát, mielőtt egy felhasználónak hozzáférést ad a TOE szolgáltatásokhoz.
3	OE.Init_Secure_Attr	Az IT környezet TSF-nek érvényes és helyes alapértelmezett biztonsági tulajdonságokról kell gondoskodnia egy objektum inicializálásakor.
4	OE.Invoke	Az IT környezet TSF-nek minden tevékenység esetén meg kell hívódnia.
5	OE.Limit_Actions_Auth	Az IT környezet TSF-nek korlátoznia kell azon tevékenységeket, melyeket egy felhasználó végrehajthat, mielőtt a TSF ellenőrzi a felhasználó kilétét.
6	OE.Limit_Tries	Az IT környezet TSF-nek korlátoznia kell az egymás utáni sikertelen hitelesítések számát.
7	OE.No_Echo	Az IT környezet TSF-nek nem szabad kijeleznie a hitelesítési információkat.
8	OE.Protect_I&A_Data	Az IT környezet TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie az I&A adatok módosítását.
9	OE.Secure_Attributes	Az IT környezet TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie a biztonsági tulajdonságok módosítását.
10	OE.Security_Roles	Az IT környezet TSF-nek karban kell tartania a biztonsági szempontból lényeges szerepköröket és a felhasználók ezen szerepkörökhöz való rendelését.
11	OE.Self_Protect	Az IT környezet TSF-nek a saját futásához egy

		tartományt kell kezelnie, melyet és melynek értékeit védi a külső beavatkozástól, hamisítástól vagy jogosulatlan felfedéstől.

12	OE.Trust_Anchor	Az IT környezet TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie a megbízható pontok karbantartását.
13	OE.TSF_Data	Az IT környezet TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie a TSF adatok módosítását.
14	OE.Authorized_Users	Az engedéllyel rendelkező felhasználók megbízhatók a tekintetben, hogy a számukra kijelölt feladatokat biztonsági szempontból korrekt módon hajtják végre.
15	OE.Configuration	A MultiSigno-t úgy kell telepíteni és konfigurálni, hogy biztonságos állapotban kezdjen el üzemelni.
16	OE.Crypto	A MultiSigno által meghívott kriptográfiai funkciókat a MultiSigno hatáskörén kívüli modulok hajtják végre, melyek megbízhatónak tekinthetők a MultiSigno által hívott, kriptográfiai funkciók megvalósítása terén. Minősített elektronikus aláírás létrehozása esetén a MultiSigno v3.0.1 környezetnek tartalmaznia kell egy vagy több NHH által nyilvántartott, tanúsított BALE-t, mely(ek) tárolják és védik az aláíró magánkulcsát, illetve végrehajtják a digitális aláírást.
17	OE.Low	A MultiSigno azonosítási és hitelesítési funkcióit egy minimális támadási potenciállal rendelkező támadás kivédésére tervezték, melyet a sebezhetőségi elemzés és a funkcióerősségi elemzések ellenőriztek.
18	OE.Physical_Security	A környezetnek elfogadható szinten kell fizikai védelemről gondoskodnia, hogy a MultiSigno-t ne lehessen hamisítani, illetve ne lehessen célpontja olyan rejtett csatorna támadásoknak, mint például áramingadozás elemzés és időzítés elemzés különböző formái.
19	OE.PKI_Info	Az IT környezetnek biztosítania kell a TOE számára a tanúsítvány és tanúsítvány visszavonási információkat, valamint az időbélyegzés szolgáltatóhoz való hozzáférést.
20	OE.Time	Az IT környezetnek hozzáférést kell biztosítania a pontos időhöz, megkívánt pontossággal, GMT formára alakítva.

4.2 A MultiSigno v3.0.1 által teljesítendő biztonsági célok

4.2.1 Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése csomag

Ezt a csomagot a MultiSigno 3.0.1 megvalósítás jellemzői miatt környezeti összetevő CL, Certificate Management Library v2.5) valósítja meg. A MultiSigno 3.0.1 közvetlen interfészeinek feladata, hogy megfelelően előkészítsék a tanúsítási útvonal érvényesség ellenőrzését. A CML által visszaadott eredményeket a MultiSigno v3.0.1 értelmezi, és továbbítja a hívó alkalmazásnak.

4.2 táblázat – Biztonsági célok a Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése csomag esetén

Sorszám	Cél megnevezése	Cél leírása
1	O.Correct_Time	A TSF-nek gondoskodnia kell érvényes pontos időről.
2	O.Current_Certificate	A TSF-nek csak nem lejárt tanúsítványokat szabad elfogadnia.
3	O.Get_KeyInfo	A TSF-nek gondoskodnia kell a felhasználó nyilvános kulcsáról és az ahhoz kapcsolódó információkról a kriptográfiai műveletek elvégzése céljából.
4	O.Path_Find	A TSF-nek képesnek kell lennie a tanúsítási útvonal felépítésére az aláírótól egy megbízható pontig.
5	O.Trusted_Keys	A TSF-nek megbízható nyilvános kulcsokat kell használnia a tanúsítási útvonal érvényességének ellenőrzése során.
6	O.User	A TSF-nek csak CA által kibocsátott tanúsítványokat szabad elfogadnia.
7	O.Verified_Certificate	A TSF-nek csak ellenőrizhető aláírással bíró tanúsítványokat szabad elfogadnia.
8	O.Valid_Certificate	A TSF-nek érvényes, azaz nem visszavont tanúsítványokat kell használnia.

4.2.2 PKI aláírás létrehozási csomag

4.3 táblázat – Biztonsági célok PKI aláírás létrehozási csomag esetén

Sorszám	Cél megnevezése	Cél leírása
1	O.Give_Sig_Hints	A TSF-nek utalni kell arra, hogy melyik tanúsítványt vagy kulcsot kell kiválasztani az aláírás ellenőrzéséhez.
2	O.Delete_Key_Sig	A TSF-nek törölnie kell a felhasználó által megadott titkos kulcsot vagy az aláíráshoz használt magánkulcsot a memóriából azok felhasználása után.

4.2.3 PKI aláírás ellenőrzési csomag

4.4 táblázat– Biztonsági célok a PKI aláírás ellenőrzési csomag esetén

Sorszám	Cél megnevezése	Cél leírása
1	O.Use_Sig_Hints	A TSF-nek használnia kell azt az információt, mely arra utal, hogy melyik tanúsítványt vagy kulcsot kell kiválasztani az aláírás ellenőrzéshez.
2	O.Linkage_Sig_Ver	A TSF-nek a megfelelő felhasználói nyilvános kulcsot kell használnia az aláírás ellenőrzéséhez.

4.2.4 PKI titkosítás kulcs átviteli algoritmusok használatával csomag

4.5 táblázat – Biztonsági célok a PKI titkosítás kulcs átviteli algoritmusok használatával csomag esetén

Sorszám	Cél megnevezése	Cél leírása
1	O.Hints_Enc_WO	A TSF-nek utalni kell arra, hogy mely tanúsítványokat vagy kulcsokat kell kiválasztani a kulcs átviteli algoritmusok használatával történő PKI titkosításhoz.
2	O.Linkage_Enc_WO	A TSF-nek a megfelelő felhasználói nyilvános kulcsot kell használnia a kulcs átvitelhez.

4.2.5 PKI megoldás kulcs átviteli algoritmusok használatával csomag

4.6 táblázat – Biztonsági célok a PKI megoldás kulcs átviteli algoritmusok használatával csomag esetén

Sorszám	Cél megnevezése	Cél leírása
1	O.Correct_KT	A TSF-nek a megfelelő magánkulcsot és kulcs átviteli algoritmust kell használnia.
2	O.Delete_Key_De	A TSF-nek törölnie kell a felhasználó által megadott titkos kulcsot vagy a megoldáshoz használt magánkulcsot a memóriából azok felhasználása után.

4.2.6 Tanúsítvány visszavonási lista ellenőrzése (érvényesítése)csomag

4.7 táblázat – Biztonsági célok a CRL érvényesség ellenőrzés csomag esetén

Sorszám	Cél megnevezése	Cél leírása
1	O.Accurate_Rev_Info	A TSF-nek csak pontos visszavonási információkat szabad elfogadnia.
2	O.Auth_Rev_Info	A TSF-nek csak jogosult CRL forrásból szabad visszavonási információkat elfogadnia.
3	O.Fresh_Rev_Info	A TSF-nek csak aktuális (friss) CRL-t szabad elfogadnia.

4.2.7 Időbélyeg kérése és ellenőrzése csomag

4.8 táblázat – Biztonsági célok a CRL érvényesség ellenőrzés csomag esetén

Sorszám	**Cél megnevezése**	**Cél leírása**
1	O.Accurate_TimeStamp_Info	A TSF-nek csak pontos időbélyeg választ szabad elfogadnia.
2	O.Auth_TimeStamp_Info	A TSF-nek csak jogosult időbélyeg szolgáltatótól (időbélyeg forrásból) szabad időbélyeg választ elfogadnia.
3	O.Fresh_TimeStamp_Info	A TSF-nek csak friss időbélyeg válaszokkal szabad dolgoznia, azaz minden időbélyeg feldolgozásnál új kérést kell kiküldenie, és az arra adott választ kell feldolgoznia.

5 IT biztonsági követelmények

Ez a fejezet a MultiSigno v3.0.1 funkcionális és garanciális biztonsági követelményeit írja le. A követelmények a CC 2. és 3. részéből származnak, illetve a 2. rész kiterjesztései.
A CC összetevők nem alkalmasak a tanúsítvány és visszavonási információkat leíró követelményekként, így a CC 2. részét ki kellett terjeszteni. A kiterjesztett követelmények jelölései megfelelnek a CC-nek.
A fejezet nem tartalmazza a környezet hatáskörébe tartozó funkciókra vonatkozó követelményeket.

5.1 táblázat – Kiterjesztett 2. vagy 3. rész követelmények

Követelmény	**2. részből származó vagy kiterjesztett**
FMT_SMF.1	2. rész
FDP_RIP.1	2. rész
FDP_CPD.1	Kiterjesztett 2. rész
FDP_DAU_CPV_OUT.1	Kiterjesztett 2. rész
FDP_DAU_CRL.1	Kiterjesztett 2. rész
FDP_DAU_ENC.1	Kiterjesztett 2. rész
FDP_DAU_SIG.1	Kiterjesztett 2. rész
FDP_ETC_ENC.1	Kiterjesztett 2. rész
FDP_ETC_SIG.1	Kiterjesztett 2. rész
FDP_ITC_ENC.1	Kiterjesztett 2. rész
FDP_ITC_SIG.1	Kiterjesztett 2. rész
FDP_DAU_TS.1	Kiterjesztett 2. rész

5.1. A MultiSigno v3.0.1 által teljesítendő funkcionális biztonsági követelmények

Az alábbi alfejezetek az egyes csomagokra vonatkozó funkcionális követelményeket írják le. A csomagok közötti függések:

- Tanúsítási útvonal érvényesség ellenőrzése csomag az alábbi más csomagokkal van függő viszonyban: (azaz amikor az alábbiakban felsorolt csomagokat szerepeltetjük a védelmi profilban, akkor a Tanúsítási útvonal érvényesség ellenőrzése – Alap csomagot szintén ki kell választani)
    - PKI titkosítás kulcs átviteli algoritmusok használatával
    - PKI aláírás ellenőrzés

5.2 táblázat – A MultiSigno v3.0.1 által megvalósított csomagokban szereplő funkcionális biztonsági követelmények összegzése

Csomag neve	**Funkcionális követelmény**	**Megjegyzés**
Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése	FDP_CPD.1	A konkrét érvényesség ellenőrzésre vonatkozó szabályokat az IT környezet Certificiate Management API biztosítja.
	FDP_DAU_CPV_OUT.1	
	FMT_SMF.1	
PKI aláírás létrehozás	FDP_ETC_SIG.1	Nincs
	FDP_RIP.1	
PKI aláírás ellenőrzés	FDP_ITC_SIG.1	A Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése csomagtól függ.
	FDP_DAU_SIG.1	
PKI titkosítás kulcs átviteli algoritmusokkal	FDP_ETC_ENC.1	Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése csomagtól függ
	FDP_DAU_ENC.1	
PKI megoldás kulcs átviteli algoritmusokkal	FDP_ITC_ENC.1	Nincs
	FDP_RIP.1	
Tanúsítvány visszavonási lista érvényesség ellenőrzése	FDP_DAU_CRL.1	Nincs
Kiegészítő csomag		
Időbélyeg kérése és ellenőrzése	FDP_DAU_TS.1	Az IT környezethez tartozó Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése csomagtól függ.

5.1.1 „Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése” csomag

5.1.1.1 FDP osztály – Felhasználói adatok védelme

FDP_CPD.1 Tanúsítási útvonal felépítése

Hierarchia szerint alárendelt-e más komponensnek: nem.

FDP_CPD.1.1 A TSF-nek fel kell építenie egy tanúsítási útvonalat a végtanúsítványtól ***a használt/betöltött tanúsítványtár tanúsítványai alapján*** a megbízható pontig, a következő tanúsítvány mezők vagy kiterjesztésekre vonatkozó illesztési szabályok felhasználásával:

a) a tanúsítvány kibocsátó (issuer mezője) megegyezik az aláíráshoz használt tanúsítvány alany megkülönböztető nevével (subject DN).

FDP_CPD.1.2 A TSF-nek fel kell építenie a tanúsítási útvonalat az alábbiakban leírt egyéb szabályok segítségével:

a) RFC 3280 szabályainak való megfelelés.

FDP_CPD.1.3 A TSF-nek fel kell építenie a tanúsítási útvonalat az alábbiakban leírt egyéb szabályok segítségével:

a) a `pathLenConstraint` megszorítás valóban teljesül.

Függések: nincsenek.

FDP_DAU_CPV_OUT.1 Tanúsítási útvonal kimenet – alapelemek

Hierarchia szerint alárendelt-e más komponensnek: nem.

FDP_DAU_CPV_OUT.1.1 A TSF-nek vissza kell adnia a tanúsítási útvonal érvényesség ellenőrzésének sikertelenségét, ha a tanúsítási útvonal bármelyik tanúsítványa érvénytelen.

FDP_DAU_CPV_OUT.1.2 A TSF-nek vissza kell adnia a végtanúsítvány következő változóit:

a) alany megkülönböztető neve,

b) `keyUsage` kiterjesztés.

FDP_DAU_CPV_OUT.1.3 A TSF-nek vissza kell adnia továbbá a következő változókat a végtanúsítványból:

a) tanúsítvány.

FDP_DAU_CPV_OUT.1.4 A TSF-nek az alany nyilvános kulcs paramétereit a tanúsítási útvonal paraméter állapotgép alapján kell visszaadnia.

Függések: nincsenek.

Alkalmazási megjegyzés:

Az ellenőrzési szabályok megvalósítását a CML v2.5 függvényei végzik, ami az értékelés hatókörén kívül esik, ezért ebben a fejezetben nem szerepelnek erre vonatkozóan további részletes követelmények.

FMT_SMF.1 Menedzsment funkciók megadása –Tanúsítványok kezelése
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FMT_SMF.1.1 A **TOE-nek** képesnek kell lennie a következő biztonsági menedzsment funkciók végrehajtására:

- **tanúsítványtár létrehozása;**
- **megbízható pontok karbantartása (hozzáadása, listázása, törlése);**
- **közbenső tanúsítványok karbantartása (hozzáadása, listázása, törlése);**
- **végtanúsítványok karbantartása (hozzáadása, listázása, törlése);**
- **CRL-ek karbantartása (CRL tárolása, források megadása,listázása, hozzáadása, törlése);**
- **végtanúsítvány exportálása**
- **PKCS#12 formátumú magánkulcs tárolása.**

Függések: nincsenek.

5.1.2 PKI aláírás létrehozás csomag

A PKI aláírás létrehozási csomag a magánkulcsot használja az aláírás létrehozására és lehetővé teszi az aláírási információk generálását.

5.1.2.1 FDP osztály – Felhasználói adatok védelme

FDP_ETC_SIG.1 PKI aláírás exportálása
Hierarchia szerint alárendelt-e más komponensnek: nem.
FDP_ETC_SIG.1.1 A TSF-nek a magánkulcs felhasználásával kell létrehoznia a digitális aláírást.
FDP_ETC_SIG.1.2 A TSF-nek az alábbi információkat kell belefoglalnia a digitális aláírásba:

- ***hash algoritmus,***
- ***aláíró megkülönböztető neve (DN),***
- ***aláíró nyilvános kulcs tanúsítványa,***
- ***aláírás időpontja,***
- ***aláírás helye.***

FDP_ETC_SIG.1.3 A TSF-nek explicit módon le kell tiltania az aláírás létrehozását az alábbi feltételek esetén:

- **aláírói hitelesítő adat sikertelen megadása;**
- **nulla hosszúságú dokumentum megadása aláírásra.**

Függések:
FCS_COP.1 Kriptográfiai műveletek – Az IT környezet végzi a kriptográfiai műveleteket

FDP_RIP.1 Részleges maradvány információ védelem – Aláírás létrehozás
FDP_RIP.1.1 A TSF-nek biztosítania kell, hogy egy erőforrás korábbi információtartalma hozzáférhetetlenné válik az **erőforrás használat utáni közvetlen deallokációja** után az alábbi objektumokra: **magánkulcs, aláíró hitelesítő adat**.

Függések: nincsenek.

Alkalmazási megjegyzés:
Az eredeti PKE PP ezen csomagja a MultiSigno v3.0.1-ben kiegészül a felhasználói adatok védelmét biztosító követelménnyel (FDP_RIP.1).

5.1.3 PKI aláírás ellenőrzési csomag

A **PKI aláírás ellenőrzési csomag** dolgozza fel az aláírási információkat és a nyilvános kulcsot használja az aláírás ellenőrzéséhez. Ez a csomag a „**Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése**" csomagtól függ. Az aláírás ellenőrzési csomag a „**Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése**" csomagot használja fel bemenetként.

5.1.3.1 FDP osztály – Felhasználói adatok védelme

FDP_ITC_SIG.1 PKI aláírás importálása
Hierarchia szerint alárendelt-e más komponensnek: nem.

FDP_ITC_SIG.1.1 A TSF-nek a következő információkat kell használnia az aláírt adatok közül:
- ***hash algoritmus,***
- ***aláíró megkülönböztető neve (DN),***
- ***aláíró nyilvános kulcs tanúsítványa,***
- ***aláírás időpontja,***
- ***aláírás helye.***

Függések: nincsenek

FDP_DAU_SIG.1 Digitális aláírás érték ellenőrzése
Hierarchia szerint alárendelt-e más komponensnek: nem.

FDP_DAU_SIG.1.1 A TSF-nek a **Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése** csomagból az alábbi információkat kell használnia az aláírt adatok digitális aláírásának ellenőrzéséhez:
alany nyilvános kulcs algoritmusa, alany nyilvános kulcsa, alany nyilvános kulcs paraméterei.
FDP_DAU_SIG.1.2 A TSF-nek vissza kell tudni adnia az alábbi értékeket:

a) **A Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése csomagból *kapott `keyUsage` kiterjesztés milyen értéket tartalmaz;***

b) ***Tanúsítvány kiterjesztések.***

FDP_DAU_SIG.1.3 A TSF-nek az alábbiakban felsorolt ellenőrzéseket kell még végrehajtania:

a) ***az alany DN-je a tanúsítási útvonal ellenőrzéséből megegyezik-e az aláírt adatban lévővel.***

Függések:
FCS_COP.1 Kriptográfiai műveletek – PP kiveszi függőségekből, mert az IT környezet végzi a kriptográfiai műveleteket

FDP_DAU_CPV_OUT.1 Tanúsítási útvonal kimenet – alapelemek

Alkalmazási megjegyzés:

A MultiSigno v3.0.1 függvénykönyvtárat hívó alkalmazás feladata a keyUsage kiterjesztésben található értékek ellenőrzése. Minősített elektronikus aláírás esetén a keyUsage kiterjesztésben csak a nonRepudiation bit lehet beállítva, fokozott biztonságú elektronikus aláírás esetén pedig emellett csak a digitalSignature bit lehet opcionálisan beállítva.. Minősített elektronikus aláírás esetén az aláíró tanúsítványában a kötelező qcStatements kiterjesztés meglétének ellenőrzése is szükséges.

5.1.4 PKI titkosítás kulcs átviteli algoritmusok használatával csomag

Ez a csomag a kulcs átviteli algoritmusokkal (pl. RSA) végrehajtott nyilvános kulcsú titkosítással kapcsolatban fogalmaz meg követelményeket. A tanúsítási útvonal érvényessége azt biztosítja, hogy a megoldó fél helyes, megfelelő nyilvános kulcsát alkalmazzák a titkosítás során. A csomag a „**Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése”**csomagtól függ.

5.1.4.1 FDP osztály – Felhasználói adatok védelme

FDP_ETC_ENC.1 PKI titkosítás exportálása – Kulcs átviteli algoritmusok
Hierarchia szerint alárendelt-e más komponensnek: nem.

FDP_ETC_ENC.1.1 A TSF-nek tartalmaznia kell a rejtjeles adatokkal együtt a következő információkat:

- ***címzett nyilvános kulcs tanúsítványa***
- ***adat rejtjelezési algoritmus,***
- ***RSA-val csomagolt titkos kulcs***

FDP_ETC_ENC.1.2 A TSF-nek használnia kell az alábbi információkat „**Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése**” csomagból a rejtjeles adatok létrehozásához:
alany nyilvános kulcs algoritmusa, alany nyilvános kulcsa, alany nyilvános kulcs paraméterek.

Függések:
FCS_COP.1 Kriptográfiai műveletek – Az IT környezet végzi a kriptográfiai műveleteket
FDP_DAU_CPV_OUT.1 Tanúsítási útvonal kimenet – alapelemek

FDP_DAU_ENC.1 PKI titkosítás ellenőrzés – Kulcs átvitel
Hierarchia szerint alárendelt-e más komponensnek: nem.

FDP_DAU_ENC.1.1 A TSF-nek vissza kell tudni adnia az alábbi értékeket:

a) A Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése csomagból kapott `keyUsage` kiterjesztés milyen értéket tartalmaz.

FDP_DAU_ENC.1.2 A TSF-nek a következő egyéb ellenőrzéseket kell végrehajtania:
a) Össze kell hasonlítania a „Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése***" kimenetének alany DN-jét a kérdéses alany DN-jével.***

Függések: FDP_DAU_CPV_OUT.1 Tanúsítási útvonal kimenet – alapelemek

Alkalmazási megjegyzés:
Ez az összetevő annak ellenőrzésére szolgál, hogy a rejtjelezés során a megfelelő nyilvános kulcsot alkalmazzák-e. Titkosítás esetén a tanúsítvány keyUsage-ében a keyEncipherment bitnek kell beállítva lenni.

5.1.5 PKI megoldás kulcs átviteli algoritmusok használatával csomag

Ez a csomag a kulcs átviteli algoritmusokkal végrehajtott nyilvános kulcsú megoldással kapcsolatban fogalmaz meg követelményeket. Mivel csak a megoldó fél magánkulcsa használt, ez a csomag nem függ a tanúsítási útvonal feldolgozástól.

5.1.5.1 FDP osztály – Felhasználói adatok védelme

FDP_ITC_ENC.1 PKI titkosítás importálása – Kulcs átviteli algoritmusok
Hierarchia szerint alárendelt-e más komponensnek: nem.

FDP_ITC_ENC.1.1 A TSF-nek a rejtjeles adatokból a következő információkat kell felhasználnia a megoldás során:
- ***kulcs rejtjelezési algoritmus,***
- ***adat rejtjelezési algoritmus,***
- ***megoldó kulcs azonosítója***
- ***RSA-val csomagolt titkos kulcs***

Függések:
FCS_COP.1 Kriptográfiai műveletek – Az IT környezet végzi a kriptográfiai műveleteket

FDP_RIP.1 Részleges maradvány információ védelem – Kulcs átvitel
FDP_RIP.1.1 A TSF-nek biztosítania kell, hogy egy erőforrás korábbi információtartalma hozzáférhetetlenné válik az **erőforrás használat utáni közvetlen deallokációja** után az alábbi objektumokra: **magánkulcs, aláíró hitelesítő adat**.

Függések: nincsenek.

Alkalmazási megjegyzés:
Az eredeti PKE PP ezen csomagja a MultiSigno v3.0.1-ben kiegészül a felhasználói adatok védelmét biztosító követelménnyel (FDP_RIP.1).

5.1.6 Tanúsítvány visszavonási lista (CRL) érvényesség ellenőrzés csomag

5.1.6.1 FDP osztály – Felhasználói adatok védelme

FDP_DAU_CRL.1 Alap CRL ellenőrzés

Hierarchia szerint alárendelt-e más komponensnek: nem.

FDP_DAU_CRL.1.1 A TSF-nek meg kell kapnia a CRL-t az alábbi helyek valamelyikéről:
- ***helyi tároló,***
- ***a használt nyilvános kulcs tanúsítványban szereplő CRL DP által mutatott pont.***

FDP_DAU_CRL.1.2 A TSF-nek meg kell kapnia a CRL kibocsátójára vonatkozóan a ***megbízható nyilvános kulcsot, algoritmust és nyilvános kulcs paramétereket***.
FDP_DAU_CRL.1.3 A TSF-nek ellenőriznie kell a CRL-en az aláírást a CRL kibocsátójának ***megbízható nyilvános kulcsa, az algoritmus és a nyilvános kulcs paramétereinek*** ismeretében.
FDP_DAU_CRL.1.4 A TSF-nek vissza kell tudni adnia az alábbi értékeket:
- ***a `keyUsage` kiterjesztés értéke.***

FDP_DAU_CRL.1.5 A TSF-nek egyeztetnie kell a CRL-ben lévő kibocsátó mezőt a CRL feltételezett kibocsátójával.
FDP_DAU_CRL.1.6 A TSF-nek az alábbi szabályok teljesülése esetén kell elfogadnia aktuálisként a CRL-t:
- ***„aktuális idő" <= thisUpdate + x ahol x-et az ellenőrző fél által reprezentált folyamat adja meg.***

FDP_DAU_CRL.1.7 A TSF-nek csak akkor szabad érvényesnek elfogadnia a CRL-t, ha fennáll az alábbi szabály:
- ***„aktuális idő" <= nextUpdate + x ahol x-et az ellenőrző fél által reprezentált folyamat adja meg.***

FDP_DAU_CRL.1.8 A TSF-nek nem szabad elfogadnia a CRL-t, ha a CRL olyan „kritikus" kiterjesztéseket tartalmaz, melyeket a TSF nem tud feldolgozni.
FDP_DAU_CRL.1.10 A TSF-nek a következő további ellenőrzéseket kell elvégeznie:
- ***a) CRL formátuma X.509 v2.***

Függések: FCS_COP.1,
FCS_COP.1 Kriptográfiai műveletek – PP kiveszi függőségekből, mert az IT környezet végzi a kriptográfiai műveleteket
FPT_STM.1 Megbízható időbélyegek

Alkalmazási megjegyzések:
A CRL kibocsátó megbízható nyilvános kulcsának, algoritmusnak és nyilvános kulcs paramétereinek normál esetben ugyanannak kell lennie, mint amiket a visszavonás szempontjából ellenőrzött tanúsítványok aláírásának ellenőrzésére használnak.

A MultiSigno v3.0.1 függvénykönyvtárat hívó alkalmazás feladata a keyUsage kiterjesztésben található értékek ellenőrzése (cRLSign bit be van-e állítva a CRL kibocsátó tanúsítványban).

5.1.7 Időbélyeg kérése és ellenőrzése csomag

Az időbélyeg kérése és ellenőrzése csomag fogalmazza meg az időbélyeg kérésre és a válaszra vonatkozó biztonsági követelményeket. Ez a csomag a „**Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése**” csomagtól függ.

FDP_DAU_TS.1 Időbélyeg kérés és ellenőrzés
Hierarchikus kapcsolat: nincs más komponenshez.

FDP_DAU_TS.1.1 A TSF-nek időbélyeg kérést kell összeállítania az alábbi mértékadó útmutatóban specifikált:

PKIX RFC 3161

alábbi formátumnak megfelelően:

TimeStampReq

FDP_DAU_TS.1.2 A TSF-nek az időbélyeg kérést ***az ellenőrző fél által reprezentált folyamat által*** megadott ***időbélyeg szolgáltató*** felé kell kibocsátania.

FDP_DAU_TS.1.3 Az időbélyeg kérésnek az alábbi adatokat kell tartalmaznia:

- ***verzió***
- ***messageImprint: hash algoritmus OID-je és az időbélyeggel ellátandó adat lenyomata;***
- ***certReq.***

FDP_DAU_TS.1.4 A TSF-nek ellenőriznie kell, hogy az időbélyeg válasz megfelel-e az alábbi mértékadó útmutatóban definiált:

PKIX RFC 3161

alábbi formátumnak:

TimeStampResp.

FDP_DAU_TS.1.5 A TSF-nek az időbélyeg válaszban a következő alap ellenőrzéseket kell elvégeznie:

a) ***ha a státusz nem granted vagy grantedWithMods, akkor nem szerepelhet a válaszban TimeStampToken;***
b) ***ha a státusz nem granted vagy grantedWithMods, akkor a válaszban szerepelnie kell PKIFailureInfo hiba információnak;***
c) ***ha a státusz granted vagy grantedWithMods, akkor a válaszban szerepelnie kell TimeStampToken objektumnak.***

FDP_DAU_TS.1.6 A TSF-nek az időbélyeg aláíráshoz használt tanúsítványt az időbélyeg válaszból meg kell ismernie.

FDP_DAU_TS.1.7 A TSF-nek a **TSA megbízhatóságának megállapítására** tanúsítási útvonal érvényesség ellenőrzést kell végrehajtania a **Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése** csomag felhasználásával.

FDP_DAU_TS.1.9 A TSF-nek a **Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése** csomagból az alábbi információkat kell használnia az időbélyeg válasz aláírásának ellenőrzéséhez: ***aláíró nyilvános kulcsa.***

FDP_DAU_TS.1.10 A TSF-nek az időbélyeg válasz ellenőrzésekor az alábbi egyéb szabályokat kell figyelembe vennie:

a) *messageImprint azonosságát az időbélyeg kérés messageImprint értékkel.*

FDP_DAU_TS.1.11 A TSF-nek nem szabad elfogadnia az időbélyeg választ, ha a válasz olyan **kritikus** kiterjesztéseket tartalmaz, melyeket a TSF nem tud feldolgozni.

Függések:
FCS_COP.1 Kriptográfiai műveletek – Az IT környezet végzi a kriptográfiai műveleteket

5.1.8 Funkcióerősségre vonatkozó követelmény

A funkcionális biztonsági követelményekre vonatkozó minimális funkcióerősségi szint: SOF-alap, de a MultiSigno v3.0.1 hatáskörén belül nincsenek valószínűségi vagy permutációs mechanizmusok.

5.2 A MIBÉTS kiemelt garanciaszint

Jelen biztonsági előirányzat (összhangban a minősített aláírásokra vonatkozó igen szigorú elvárásokkal) a MIBÉTS kiemelt (EAL4) garanciaszintet követeli meg. Valamennyi garanciaösszetevő a CC 3. részéből származik, s az 5.3 táblázat felsorolja ezeket.

Garanciaösszetevő azonosító	garanciaösszetevő cím
ACM_AUT.1	Részleges konfiguráció menedzselés automatizálás
ACM_CAP.4	A generálás támogatása és elfogadási eljárások
ACM_SCP.2	A biztonsági hibákat követő konfiguráció menedzselés
ADO_DEL.2	A módosítás kimutatása
ADO_IGS.1	Hardver telepítés, szoftver telepítés, a beindítás eljárásai
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
AGD_ADM.1	Adminisztrátori útmutató
AGD_USR.1	Felhasználói útmutató
ALC_DVS.1	A biztonsági intézkedések azonosítása
ALC_LCD.1	A fejlesztő által meghatározott életciklus modell
ALC_TAT.1	Jól meghatározott fejlesztő eszközök
ATE_COV.2	A lefedettség elemzése
ATE_DPT.1	A magas szintű terv vizsgálata
ATE_FUN.1	Funkcionális tesztelés
ATE_IND.2	Független tesztelés – mintavételezés
AVA_MSU.2	A vizsgálatok megerősítése
AVA_SOF.1	A TOE biztonsági funkciónak erősségértékelése
AVA_VLA.2	Független sebezhetőség vizsgálat

5.3 táblázat – A MIBÉTS kiemelt szint garanciális követelményei

*Az ADV_SPM.1 garanciaösszetevő által meghatározott értékelői tevékenységet a MIBÉTS séma nem követeli meg.

5.2.1 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 t 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.

5.2.2 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.

5.2.3 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 (ellentmondásmentesnek) 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-et.

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.

5.2.4 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.

5.2.5 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.

5.2.6 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.

5.2.7 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.

Alkalmazási megjegyzés: Jelen biztonsági előirányzat nem tartalmaz olyan biztonsági funkciót, melyre a funkcióerősség értelmezhető, ezért ez a garanciális követelmény nem alkalmazandó.

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 a MultiSigno v3.0.1 által teljesítendő biztonsági követelményeket teljesítő biztonsági funkciókat tartalmazza. Leírja a MultiSigno v3.0.1 összes biztonsági funkcióját és garanciális intézkedését, amelyek a MultiSigno v3.0.1 biztonsági követelményeinek a kielégítéséhez járulnak hozzá.

6.1 Biztonsági funkciók

A MultiSigno v3.0.1 az alábbi biztonsági funkciókat valósítja meg:

BF1 Aláírás létrehozása
BF2 Elektronikus aláírás ellenőrzése
BF3 Időbélyeg kérések és válaszok kezelése
BF4 Tanúsítási útvonal felépítése és érvényesség ellenőrzése
BF5 Tanúsítványtár kezelés
BF6 Titkosítás és megoldás

BF1 Aláírás létrehozása

A **BF1 Aláírás létrehozása** biztonsági funkció végzi el a fokozott biztonságú vagy minősített elektronikus aláírás létrehozását. Előkészíti az aláírás létrehozást (fájl hozzáadása, magánkulcs kiválasztása, aláírással kapcsolatos adatszerkezetek létrehozása), majd az előkészített információk alapján elkészíti a lenyomatot és az elektronikus aláírást.
A funkció képes az aláírói dokumentum mimeType-jának tárolására, amit a hívó alkalmazás ellenőrizhet.

Az aláírás létrehozás biztonsági funkció az aláírás létrehozási funkció részeként létrehozza a titkosítandó lenyomatot. Az alkalmazható lenyomatoló algoritmusok: SHA-1, SHA-256, SHA-384, SHA-512 [FIPS 180-1], [FIPS 180-2].

A MultiSigno v3.0.1 lehetőséget biztosít fokozott biztonságú és minősített elektronikus aláírások létrehozására. ***Fokozott biztonságú aláírások esetén*** az alábbi kulcstároló eszközöket képes kezelni:

- Saját tanúsítványtárba betöltött PKCS#12-es formátumú kulcstároló fájl,
- kriptográfiai hardver eszköz (saját tanúsítványtáron keresztül).

A biztonsági funkció közvetlenül nem ellenőrzi a **`keyUsage`** kiterjesztést (a kötelezően beállított **`nonRepudiation`** bit mellett opcionálisan a **`digitalSignature`** bit lehet beállítva), a függvénykönyvtár használójának kell ellenőrizni a funkció által visszaadott értéket.

Minősített elektronikus aláírás létrehozása esetén az aláíráshoz használt tanúsítványnak minősített tanúsítványnak (QCStatement kiterjesztés használata) kell lennie. A MultiSigno 3.0.1 képes minősített tanúsítványokhoz tartozó, hardvereszközön (BALE-n) tárolt magánkulcsot használni. A minősített aláírás létrehozásához használt magánkulcshoz tartozó tanúsítványban a **`keyUsage`** kiterjesztésben csak a **`nonRepudiation`** bit lehet beállítva, amit a függvénykönyvtárat használó alkalmazásfejlesztőnek kell ellenőriznie.

A funkció által létrehozott elektronikus aláírás formátuma: Melasz-Ready XadES-C formátum.
A MultiSigno v3.0.1 az aláírás létrehozását akkor tekinti sikeresnek, ha az aláírás ellenőrzését is végre tudja hajtani.

BF2 Elektronikus aláírás ellenőrzése

Ez a funkció valósítja meg a bemenetként kapott elektronikus aláírás ellenőrzését. A funkciónak átadott elektronikus aláírás ellenőrzés után a hívó alkalmazásnak meg kell vizsgálni az ellenőrzés által visszaadott információkat, amelyek jelzik, hogy az aláírás megfelel-e a hívó alkalmazás által kezdeményezett kezdeti vagy utólagos ellenőrzésnek, illetve további részletek ad az ellenőrzés státuszról.

BF3 Időbélyeg kérések és válaszok kezelése

A MultiSigno v3.0.1 képes időbélyeg kérést kibocsátani az aláírás adott időben való meglétének igazolása céljából. Az RFC 3161-ben specifikáltaknak megfelelően összeállítja az időbélyeg kérést a lenyomattal, és elküldi a kérés paramétereként megadott külső időbélyeg szolgáltatóhoz.

A MultiSigno v3.0.1 az időbélyeg szolgáltatótól kapott időbélyeg válaszra végrehajtja a szükséges szintaktikai és szemantikai ellenőrzéseket, azaz ellenőrzi az időbélyeg válasz elemeit és aláírását.

BF4 Tanúsítási útvonal felépítése és érvényesség ellenőrzése

Ez a biztonsági funkció végzi az aláíró tanúsítványtól a gyökértanúsítványig tartó tanúsítvány lánc elemeinek összegyűjtését és ellenőrzését. A MultiSigno v3.0.1 saját tanúsítványtárából dolgozik, ezt adja át az útvonal tényleges ellenőrzését végző nyílt kódú függvénykönyvtárnak (Certificate Management Library API), melynek feladata a tanúsítványok és visszavonási listák értelmezése és tárolása, tanúsítványok érvényességének vizsgálata.
A biztonsági funkció meghívását a MultiSigno v3.0.1 végzi, de a tényleges útvonal érvényesség ellenőrzést a CML-ben megvalósított függvények végzik (MultiSigno értékelés hatáskörén kívüli összetevőként), melyek az ellenőrzés eredményét visszaadják a hívó MultiSigno v3.0.1 függvénynek, ami értelmezi az érvényesség ellenőrzés eredményét.

BF5 Tanúsítványtár kezelés

A MultiSigno v3.0.1 saját tanúsítványtárat használ a működése során, amihez az alábbi tanúsítványtár funkciókat biztosítja:

- Gyökér tanúsítvány hozzáadása
- Gyökér tanúsítvány eltávolítás
- Gyökér tanúsítvány listázása
- közbenső tanúsítvány hozzáadása
- közbenső tanúsítvány eltávolítás

- közbenső tanúsítvány listázása
- végfelhasználói tanúsítvány hozzáadása
- végfelhasználói tanúsítvány eltávolítás
- végfelhasználói tanúsítvány listázása
- végfelhasználói tanúsítvány exportálása
- PKCS#12 formátumú magánkulcs tárolása
- CRL források megadása
- CRL források törlése
- CRL források listázása
- CRL tárolása

BF6 Titkosítás és megoldás

A MultiSigno v3.0.1 titkosítás és kapcsolódó megoldás biztonsági funkciókat is támogat.
A támogatott aszimmetrikus algoritmusok:

- RSA, PKCS#1 v1.5.

Támogatott szimmetrikus titkosítási algoritmusok:

- AES/ECB és CBC mód,
- 3DES/CBC,
- RC2/CBC.

6.2 Garanciális intézkedések

A **garanciális intézkedések**ről szóló nyilatkozat az értékelés tárgya azon garanciális intézkedéseit határozza meg, amelyekről kijelentették, hogy eleget tesznek a kinyilvánított garanciális követelményeknek. A garanciális intézkedéseket a garanciális követelményekre úgy kell visszavezetni, hogy láthatóvá váljon, melyik intézkedés melyik követelmény kielégítéséhez járul hozzá.
A garanciális intézkedések megadhatók a fontosabb tervdokumentációkra, életciklus tervekre, vagy menedzseri tervekre való utalással. Ezen dokumentációk összesítését tartalmazza a 6.1 táblázat.

Cím	**verzió**	**fájl név**
Biztonsági előirányzat	v1.0	MultiSigno_ST_v10.pdf
Funkcionális specifikáció	v1.0	MultiSigno_FS_v10.doc
Magas szintű terv	v1.0	MultiSigno_HLD_v10.doc
Alacsony szintű terv (MultiSigno SDK Dokumentáció)	v3.0.1	„htlm_060428” alkönyvtár
megvalósítás	v3.0.1	„include_060428, „src_060428” és „bin_060428” alkönyvtárak
Megfeleltetés elemzések	v1.0	MultiSigno_RCR_v10.doc
Tesztelési dokumentáció	v1.0	MultiSigno_Test_Documentation.doc
Teszt lefedettség elemzés	v1.0	MultiSigno_Test_Cov_v10.doc
Teszt mélység elemzés	v1.0	MultiSigno_Test_Depth_v10.doc
Útmutató (MultiSigno 3.0 Manual)	2006.04.28	MultiSigno_SDK_man.rtf
A konfiguráció menedzselés dokumentációja	v1.0	MultiSigno_Conf_Mgmt_v10.doc
A fejlesztési biztonság dokumentációja	v1.0	MultiSigno_DVS_v10.doc
Az életciklust meghatározó dokumentáció	v1.0	MultiSigno_LCDf_v10.doc
A fejlesztő eszközök dokumentációja	v1.0	MultiSigno_TAT_v10.doc
Az útmutató helytelen használhatóságának elemzése	v1.0	MultiSigno_Misuse_v10.doc
Sebezhetőség elemzés	v1.0	MultiSigno_Vulnerability_Analysis.doc
Folyamatábrák	v.1.0.0	„Folyamatábrák” alkönyvtár
MultiSigno 3 – Rendszerterv – Implementációs modell	2006.01.06	MS3-Komponensmodell.pdf
MultiSigno 3 – Rendszerterv – Felhasználási esetek megvalósításai	2006.01.06	MS3-Kovetelmenyrealizaciok.pdf
Logikai architektúra a MultiSigno 3 rendszertervhez	2006.01.06	MS3-Logikai_Architektura.pdf
MultiSigno 3.0 Specifikáció	v2.0	MS3-specifikacio_v2.pdf
MultiSigno 3.0 Manual	2006.04.28	MultiSigno_SDK_man.rtf

7 PP megfelelőség

Jelen biztonsági előirányzat a PKE PP alapján készült, de a MultiSigno v3.0.1 biztonsági jellemzői miatt PP megfelelőségi nyilatkozatot nem tesz.

8 Indoklások

Ez a fejezet tartalmazza azon indoklásokat, melyek megmutatják, hogy a MultiSigno v3.0.1 valóban kivédi a számításba vett veszélyeket és teljesíti a biztonsági céljait. Mivel a MultiSigno v3.0.1 nem önálló alkalmazás, hanem egy fejlesztői függvénykönyvtár, ezért a PKE PP család által általános követelményként értelmezett biztonsági követelményeket a TOE IT környezetének kell kielégítenie. A MultiSigno v3.0.1 IT környezetébe tartoznak a TOE által használt programcsomagok és az operációs rendszer, a tanúsítási útvonal tényleges érvényesség ellenőrzését végző Certificate Management Library, továbbá minősített elektronikus aláírás esetén a BALE eszköz és annak biztonságos használatát biztosító programok, vagy KHE eszköz és annak meghajtó programjai.

8.1 A biztonsági célok indoklása

8.1.1 A környezeti biztonsági célok indoklása

A 8.1 táblázat az általános feltételezéseket és veszélyeket képezi le a IT környezet biztonsági céljaira, megmutatva, hogy minden veszélyhez és feltételezéshez tartozik legalább egy biztonsági cél. A 8.2 táblázat az általános biztonsági célokat rendeli veszélyekhez és feltételezésekhez, bizonyítván, hogy minden biztonsági célhoz tartozik legalább egy veszély vagy feltételezés.

8.1. táblázat – A TOE-re vonatkozó feltételezések és veszélyek leképezése a célokra

Feltételezés/veszély	**Célok**
AE.Authorized_Users	OE.Authorized_Users
AE.Configuration	OE.Configuration
AE.Crypto_Module	OE.Crypto
AE.Low	OE.Low
AE.PKI_Info	OE.PKI_Info
AE.Physical_Protection	OE.Physical_Security
AE.Time	OE.Time
AE.TimeStamp	OE.PKI_Info
T.Attack	OE.DAC
T.Bypass	OE.Invoke
T.Imperson	OE.I&A, OE.Limit_Actions_Auth
T.Modify	OE.Self_Protect, OE.DAC, OE.Protect_I&A_Data, OE.Trust_Anchor, OE.TSF_Data
T.Object_Init	OE.Init_Secure_Attr
T.Private_key	OE.DAC
T.Role	OE.Security_Roles
T.Secure_Attributes	OE.Secure_Attributes
T.Shoulder_Surf	OE.No_Echo

T.Tries	OE.Limit_Tries

AE.Authorized_Users: az engedéllyel rendelkező felhasználók megbízhatók, hogy a számukra kijelölt funkciókat végrehajtsák. A feltételezésből származtatott biztonsági cél:

- **OE.Authorized_Users**: az engedéllyel rendelkező felhasználók megbízhatók a tekintetben, hogy a számukra kijelölt feladatokat végrehajtják.

AE.Configuration: a TOE-t megfelelően telepítik és konfigurálják. A feltételezésből származtatott biztonsági cél:

- **OE.Configuration:** a TOE-t úgy kell telepíteni és konfigurálni, hogy a TOE biztonságos állapotban kezdjen el üzemelni.

AE.Crypto_Module: A TOE által meghívott kriptográfiai funkciókról feltételezés, hogy TOE hatáskörén kívüli modulok hajtják végre (OpenSSL), melyek megbízhatónak tekinthetők a TOE által hívott, kriptográfiai funkciók megvalósítása terén.
Minősített elektronikus aláírás létrehozása esetén a TOE környezetéről feltételezés, hogy tartalmaz egy vagy több NHH által nyilvántartott, tanúsított BALE-t, mely(ek) tárolják és védik az aláíró magánkulcsát, illetve végrehajtják a digitális aláírást. A feltételezésből származtatott biztonsági cél:

- **OE.Crypto**: A TOE által meghívott kriptográfiai funkciókat TOE hatáskörén kívüli modulok hajtják végre (OpenSSL), melyek megbízhatónak tekinthetők a TOE által hívott, kriptográfiai funkciók megvalósítása terén. Minősített elektronikus aláírás létrehozása esetén a TOE környezetnek tartalmaznia kell egy vagy több NHH által nyilvántartott, tanúsított BALE-t, mely(ek) tárolják és védik az aláíró magánkulcsát, illetve végrehajtják a digitális aláírást.

AE.Low: a TOE-val szembeni támadási potenciált alacsonynak tételezzük fel. A feltételezésből származtatott biztonsági cél:

- **OE.Low:** kimondja, hogy a TOE azonosítási és hitelesítési funkcióit egy minimális támadási potenciállal rendelkező támadás kivédésére tervezték, melyet a sebezhetőségi elemzés és a funkcióerősségi elemzések ellenőriztek.

AE.PKI_Info: a tanúsítvány és tanúsítvány visszavonási információk a TOE rendelkezésére állnak. A feltételezésből származtatott biztonsági cél:

- **OE.PKI_Info**: az IT környezetnek biztosítania kell a TOE számára a tanúsítvány és tanúsítvány visszavonási információkat, valamint az időbélyegzés szolgáltatóhoz való hozzáférést.

AE.Physical_Protection: a környezetről feltételezzük, hogy fizikailag véd. A TOE szoftverről feltételezzük, hogy védett a jogosulatlan fizikai hozzáféréssel szemben. A feltételezésből származtatott biztonsági cél:

- **OE.Physical_Security**: a környezetnek elfogadható szinten kell fizikai védelemről gondoskodnia, hogy a TOE-t ne lehessen hamisítani, illetve ne lehessen célpontja olyan rejtett csatorna támadásoknak, mint például áramingadozás elemzés és időzítés elemzés különböző formái.

AE.Time: a környezetről feltételezzük, hogy GMT formában és a megkívánt pontossággal gondoskodik a pontos rendszeridőről. A feltételezésből származtatott biztonsági cél:

- **OE.Time**: a környezetnek hozzáférést kell biztosítania a pontos időhöz, megkívánt pontossággal, GMT formára alakítva.

AE.TimeStamp: a környezetről feltételezzük, hogy biztosítja az időbélyegzés szolgáltatóhoz való hozzáférést. A feltételezésből származtatott biztonsági cél:

- **OE.PKI_Info**: az IT környezetnek biztosítania kell a TOE számára a tanúsítvány és tanúsítvány visszavonási információkat, valamint az időbélyegzés szolgáltatóhoz való hozzáférést.

T.Attack: a TOE értékek nem észlelt kompromittálódás következhet be egy (külső vagy belső) támadó olyan tevékenysége révén, mely tevékenységet nincs joga végezni. A veszélyből származtatott biztonsági cél:

- **OE.DAC**: a TSF-nek ellenőriznie és korlátoznia kell a felhasználók hozzáféréseit a TOE értékekhez, egy megadott hozzáférés ellenőrzési szabályzatnak megfelelően.

T.Bypass: egy jogosulatlan egyed vagy felhasználó meghamisíthatja a biztonsági tulajdonságokat vagy más adatokat a TOE biztonsági funkcióinak megkerülése és a TOE értékekhez való jogosulatlan hozzáférés megszerzése érdekében. A veszélyből származtatott biztonsági cél:

- **OE.Invoke:** a TSF-nek minden tevékenység esetén meg kell hívódnia.

T.Imperson: egy jogosulatlan egyed megszemélyesíthet egy jogosult TOE felhasználót, miáltal hozzáférést szerez a TOE adatokhoz, kulcsokhoz és műveletekhez. A veszélyből származtatott biztonsági célok:

- **OE.I&A**: a TSF-nek egyedi módon azonosítania kell minden felhasználót, és hitelesíteni kell azok állítólagos azonosságát, mielőtt egy felhasználónak hozzáférést ad a TOE szolgáltatásokhoz.
- **OE.Limit_Actions_Auth**: a TSF-nek korlátoznia kell azon tevékenységeket, melyeket egy felhasználó végrehajthat, mielőtt a TSF ellenőrzi a felhasználó kilétét.

T.Modify: egy támadó módosíthatja a TSF-et vagy felhasználói adatokat, például a tárolt biztonsági tulajdonságokat vagy kulcsokat, annak érdekében, hogy hozzáférést szerezzen a TOE-hez és annak értékeihez. A veszélyből származtatott biztonsági célok:

- **OE.Self_Protect:** a TSF-nek a saját futásához egy tartományt kell kezelnie, melyet és melynek értékeit védi a külső beavatkozástól, hamisítástól vagy jogosulatlan felfedéstől.
- **OE.DAC**: a TSF-nek ellenőriznie és korlátoznia kell a felhasználók hozzáféréseit a TOE értékekhez, egy megadott hozzáférés ellenőrzési szabályzatnak megfelelően.
- **OE.Protect_I&A_Data**: a TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie az I&A adatok módosítását.
- **OE.Trust_Anchor**: a TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie a megbízható pontok karbantartását.
- **OE.TSF_Data**: a TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie a TSF adatok módosítását.

T.Object_Init: egy támadó jogosulatlan hozzáférést szerez egy objektumhoz annak létrehozása során, ha a biztonsági tulajdonságokat nem rendelik hozzá az objektumhoz, vagy az objektum létrehozásakor ezt bárki megteheti. A veszélyből származtatott biztonsági cél:

- **OE.Init_Secure_Attr**: a TSF-nek érvényes és helyes alapértelmezett biztonsági tulajdonságokról kell gondoskodnia egy objektum inicializálásakor.

T.Private_key: egy támadó felveheti egy felhasználó azonosságát a felhasználó magánkulcsának generálása vagy használata által. A veszélyből a következő biztonsági célok származnak:

- **OE.DAC**: kimondja, hogy a TSF-nek ellenőriznie és korlátoznia kell a felhasználók hozzáféréseit a TOE értékekhez, egy megadott hozzáférés ellenőrzési szabályzatnak megfelelően.

T.Role: egy felhasználó a számára megengedettnél magasabb jogosultságot vehet fel és használhat számára egyébként nem megengedett tevékenységek elvégzése céljából. A veszélyből származtatott biztonsági cél:

- **OE.Security_Roles**: a TSF-nek karban kell tartania a biztonsági szempontból lényeges szerepköröket és a felhasználók ezen szerepkörökhöz való rendelését.

T.Secure_Attributes: egy felhasználó képes lehet egy objektum biztonsági tulajdonságainak megváltoztatására és így az objektumhoz való jogosulatlan hozzáférés megszerzésére. A veszélyből származtatott biztonsági cél:

- **OE.Secure_Attributes**: a TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie a biztonsági tulajdonságok módosítását.

T.Shoulder_Surf: egy jogosulatlan felhasználó a jogosult felhasználó válla fölött meglátja a hitelesítési információkat a hitelesítési folyamat közben. A veszélyből származtatott biztonsági cél:

- **OE.No_Echo**: a TSF-nek nem szabad kijeleznie a hitelesítési információkat.

T.Tries: egy jogosulatlan egyed kitalálhatja a hitelesítési információt próbálgatás és hibák révén. A veszélyből származtatott biztonsági cél:

- **OE.Limit_Tries**: a TSF-nek korlátoznia kell az egymás utáni sikertelen hitelesítések számát.

A 8.2 táblázat az általános környezeti biztonsági célokat vezeti vissza a veszélyekre és feltételezésekre, ami azt mutatja meg, hogy minden cél visszavezethető egy feltételezésre vagy veszélyre. Az indoklás az előző, itt már nem ismételjük meg.

8.2 táblázat – A környezeti célok leképezése veszélyekre és feltételezésekre

Cél	**Feltételezés/veszély**
OE.Authorized_Users	AE.Authorized_Users
OE.Configuration	AE.Configuration
OE.Crypto	AE.Crypto_Module
OE.Low	AE.Low
OE.PKI_Info	AE.PKI_Info OE.TimeStamp
OE.Physical_Security	AE.Physical_Protection
OE.Time	AE.Time
OE.DAC	T.Attack, T.Modify, T.Private_key
OE.Invoke	T.Bypass
OE.I&A	T.Imperson
OE.Limit_Actions_Auth	T.Imperson
OE.Protect_I&A_Data	T.Modify
OE.Init_Secure_Attr fg	T.Object_Init

OE.DAC	T.Private_key
OE.Security_Roles	T.Role
OE.Secure_Attributes	T.Secure_Attributes
OE.No_Echo	T.Shoulder_Surf
OE.Limit_Tries	T.Tries
OE.Self_Protect	T.Modify
OE.Trust_Anchor	T.Modify
OE.TSF_Data	T.Modify

8.1.2 A MultiSigno v3.0.1 által teljesítendő biztonsági célok indoklása

Az itt szereplő biztonsági célok mind az értékelés tárgya, azaz a MultiSigno v3.0.1 hatáskörén belül teljesítendőek.

8.1.2.1 Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése csomag biztonsági céljainak indoklása

A csomag veszélyei és céljai közötti hozzárendeléseket mutatja az alábbi táblázat, a táblázat után pedig az indoklás olvasható.

8.3 táblázat – A veszélyek leképezése célokra a „Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése" csomag esetén

Sorszám	Veszély	Célok
1	T.Certificate_Modi	O.Verfied_Certificate
2	T.Expired_Certificate	O.Correct_Time O.Current_Certificate
3	T.Masquarade	O.trusted_Keys
4	T.No_Crypto	O.Get_KeyInfo
5	T.Path_Not_Found	O.Path_Find
6	T.Revoked_Certificate	O.Valid_Certificate
7	T.User_CA	O.User

T.Certificate_Modi: egy nem megbízható felhasználó módosíthat egy tanúsítványt, ami rossz nyilvános kulcs használatához vezet. A veszélyből származtatott biztonsági cél:

- **O.Verified_Certificate:** a TSF-nek csak ellenőrizhető aláírással bíró tanúsítványokat szabad elfogadnia.

T.Expired_Certificate: a rendszer lejárt (és vélhetően visszavont) tanúsítványt használ aláírás ellenőrzésre. A veszélyből származtatott biztonsági cél:

- **O.Correct_Time:** a TSF-nek gondoskodnia kell érvényes pontos időről.
- **O.Current_Certificate:** a TSf-nek csak nem lejárt tanúsítványokat szabad elfogadnia.

T.Masquarade: egy nem megbízható egyed (CA) hamis azonosságú egyedeknek bocsát ki tanúsítványokat, akik ezáltal más legitim felhasználók nevében léphetnek fel. A veszélyből származtatott biztonsági cél:

- **O.Trusted_Keys:** a TSF-nek megbízható nyilvános kulcsokat kell használnia a tanúsítási útvonal érvényességének ellenőrzése során.

T.No_Crypto: a felhasználó nyilvános kulcsa és a kapcsolódó információk nem állnak rendelkezésre a kriptográfiai funkció elvégzéséhez. A veszélyből származtatott biztonsági cél:

- **O.Get_KeyInfo:** a TSF-nek gondoskodnia kell a felhasználó nyilvános kulcsáról és az ahhoz kapcsolódó információkról a kriptográfiai műveletek elvégzése céljából.

T.Path_Not_Found: egy érvényes tanúsítási útvonal rendszerfunkció hiánya miatt nem található. A veszélyből származtatott biztonsági cél:

- **O.Path_Find**: a TSF-nek képesnek kell lennie a tanúsítási útvonal felépítésére a végtanúsítványtól egy megbízható pontig.

T.Revoked_Certificate: egy visszavont tanúsítványt a rendszer érvényesként fogad el, ami a biztonság sérülésével jár. A veszélyből származtatott biztonsági cél:

- **O.Valid_Certificate:** a TSF-nek érvényes, azaz nem visszavont tanúsítványokat kell használnia.

T.User_CA: egy felhasználó CA-ként léphet fel, úgy, hogy nem engedélyezett tanúsítványokat bocsát ki. A veszélyből származtatott biztonsági cél:

- **O.User**: a TSF-nek csak CA által kibocsátott tanúsítványokat szabad elfogadnia.

A 8.4 táblázat a **Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése** csomag céljait vezeti vissza a veszélyekre, megmutatva, hogy minden célhoz tartozik veszély.

8.4 táblázat – A célok visszavezetése veszélyekre a CPV – Alap csomag esetén

Sorszám	Cél	Veszély
1	O.Correct_Time	T.Expired_Certificate
2	O.Current_Certificate	T.Expired_Certificate
3	O.Get_KeyInfo	T.No_Crypto
4	O.Path_Find	T.Path_Not_Found
5	O.Trusted_Keys	T.Masquarade
6	O.User	T.User_CA
7	O.Verfied_Certificate	T.Certificate_Modi
8	O.Valid_Certificate	T.Revoked_Certificate

8.1.2.2 PKI aláírás létrehozás csomag biztonsági céljainak indoklása

Először a veszélyek leképezését tekintjük át a 8.5 táblázat és az alatta olvasható magyarázó szöveg segítségével, majd a 8.6 táblázat a célokat vezeti vissza a veszélyekre.

8.5 táblázat A veszélyek leképezése célokra a PKI aláírás létrehozás csomag esetén

Sorszám	Veszély	Célok
1	T.Clueless_PKI_Sig	O.Give_Sig_Hints
2	T.Key_Leakage_Sig	O.Delete_Key_Sig

T.Clueless_PKI_Sig: a felhasználó jelzés hiányában csak rossz tanúsítványokkal próbálkozik a PKI aláírás létrehozásakor. A veszélyből származtatott biztonsági cél:

- **O.Give_Sig_Hints**: a TSF-nek utalni kell arra, hogy melyik tanúsítványt vagy kulcsot kell kiválasztani a PKI aláíráshoz.

T.Key_Leakage_Sig: az aláírás létrehozása után magán vagy titkos kulcsok válnak más folyamatok számára hozzáférhetővé. A veszélyből származtatott biztonsági cél:

- **O.Delete_Key_Sig:** A TSF-nek törölnie kell a felhasználó által megadott titkos kulcsot vagy az aláíráshoz használt magánkulcsot a memóriából azok felhasználása után.

8.6 táblázat – A célok visszavezetése veszélyekre a PKI aláírás létrehozási csomag esetén

Sorszám	Célok	Veszély
1	O.Give_Sig_Hints	T.Clueless_PKI_Sig
2	T.Key_Leakage_Sig	O.Delete_Key_Sig

8.1.2.3 PKI aláírás ellenőrzési csomag biztonsági céljainak indoklása

Először a veszélyek leképezését tekintjük át a 8.7 táblázat és az alatta olvasható magyarázó szöveg segítségével, majd a 8.8 táblázat a célokat vezeti vissza a veszélyekre.

8.7 táblázat A veszélyek leképezése célokra a PKI aláírás ellenőrzés csomag esetén

Sorszám	Veszély	Célok
1	T.Assumed_identity_PKI_Ver	O.Linkage_Sig_Ver
2	T.Clueless_PKI_Ver	O.Use_Sig_Hints

T.Assumed_Identity_PKI_Ver: egy felhasználó felveheti egy másik felhasználó azonosságát a PKI aláírás ellenőrzéshez. A veszélyből származtatott biztonsági cél:

- **O.Linkage_Sig_Ver**: a TSF-nek a megfelelő felhasználói nyilvános kulcsot kell használnia az aláírás ellenőrzéséhez.

T.Clueless_PKI_Ver: a felhasználó jelzés hiányában csak rossz tanúsítványokkal próbálkozik az aláírás ellenőrzésekor. A veszélyből származtatott biztonsági cél:

- **O.Use_Sig_Hints**: a TSF-nek utalni kell arra, hogy melyik tanúsítványt vagy kulcsot kell kiválasztani az aláírás ellenőrzéshez.

8.8 táblázat – A célok visszavezetése veszélyekre a PKI aláírás ellenőrzési csomag esetén

Sorszám	Célok	Veszély
1	O.Use_Sig_Hints	T.Clueless_PKI_Ver
2	O.Linkage_Sig_Ver	T.Assumed_Identity_PKI_Ver

8.1.2.4 A PKI titkosítás kulcs átviteli algoritmusok használatával csomag biztonsági céljainak indoklása

8.9 táblázat A veszélyek leképezése célokra a PKI titkosítás kulcs átviteli algoritmusok használatával csomag esetén

Sorszám	Veszély	Célok
1	T.Assumed_Identity_WO_En	O.Linkage_Enc_WO
2	T.Clueless_WO_En	O.Hints_Enc_WO

T.Assumed_Identity_WO_En: Egy felhasználó egy másik felhasználónak adhatja ki magát, hogy végrehajthasson egy titkosítást kulcs átviteli algoritmussal. A veszélyből származtatott biztonsági cél:

- **O.Linkage_Enc_WO:** A TSF-nek a megfelelő felhasználói nyilvános kulcsot kell használnia a kulcs átvitelhez.

T.Clueless_WO_En: A felhasználó jelzés hiányában csak helytelen tanúsítványokkal próbál titkosítani, kulcs átviteli algoritmust használva. A veszélyből származtatott biztonsági cél:

- **O.Hints_Enc_WO**: A TSF-nek utalni kell arra, hogy mely tanúsítványokat vagy kulcsokat kell kiválasztani a kulcs átviteli algoritmusok használatával történő PKI titkosításhoz.

8.10 táblázat A célok leképezése veszélyekre a PKI titkosítás kulcs átviteli algoritmusok használatával csomag esetén

Sorszám	Célok	Veszélyek
1	O.Hints_Enc_WO	T.Clueless_WO_En
2	O.Linkage_Enc_WO	T.Assumed_Identity_WO_En

8.1.2.5 A PKI megoldás kulcs átviteli algoritmusok használatával csomag biztonsági céljainak indoklása

8.11 táblázat A veszélyek leképezése célokra a PKI dekódolás kulcs átviteli algoritmusok használatával csomag esetén

Sorszám	Veszély	Célok
1	T.Garble_WO_De	O.Correct_KT
2	T.Key_Leakage_De	O.Delete_Key_De

T.Garble_WO_De: A felhasználó nem a megfelelő kulcs átviteli algoritmust vagy nem a megfelelő magánkulcsot alkalmazza, ami az adatok összezagyválásához vezet. A veszélyből származtatott biztonsági cél:

- **O.Correct_KT:** A TSF-nek a megfelelő magánkulcsot és kulcs átviteli algoritmust kell használnia.

T.Key_Leakage_De: a megoldás után magán vagy titkos kulcsok válnak más folyamatok számára hozzáférhetővé. A veszélyből származtatott biztonsági cél:

- **O.Delete_Key_De:** A TSF-nek törölnie kell a felhasználó által megadott titkos kulcsot vagy a megoldáshoz használt magánkulcsot a memóriából azok felhasználása után.

8.12 táblázat A célok leképezése veszélyekre a PKI dekódolás kulcs átviteli algoritmusok használatával csomag esetén

Sorszám	Célok	Veszélyek
1	O.Correct_KT	T.Garble_WO_De
2	O.Delete_Key_De	T.Key_Leakage_De

8.1.2.6 A CRL ellenőrzés csomag biztonsági céljainak indoklása

Először a veszélyek leképezését tekintjük át a 8.13 táblázat és az alatta olvasható magyarázó szöveg segítségével, majd a 8.14 táblázat a célokat vezeti vissza a veszélyekre.

8.13 táblázat – A veszélyek leképezése célokra a CRL ellenőrzés csomag esetén

Sorszám	Veszély	Célok
1	T.Replay_Revoc_Info_CRL	O.Fresh_Rev_Info
2	T.Wrong_Revoc_Info_CRL	O.Accurate_Rev_Info, O.Auth_Rev_Info

T.Replay_Revoc_Info_CRL: a felhasználó elfogadhat régi visszavonási információt, ami nem sokkal korábban visszavont tanúsítvány használatához vezethet. A veszélyből származtatott biztonsági cél:

- **O.Fresh_Rev_Info**: a TSF-nek valószerű aktuális (friss) CRL-t szabad csak elfogadnia.

T.Wrong_Revoc_Info_CRL: a felhasználó egy rossz CRL miatt elfogadhat lejárt tanúsítványt vagy visszautasíthat egy érvényes tanúsítványt. A veszélyből származtatott biztonsági cél:

- **O.Accurate_Rev_Info**: a TSF-nek csak pontos visszavonási információkat szabad elfogadnia.
- **O.Auth_Rev_Info**: a TSF-nek csak jogosult CRL forrásból szabad visszavonási információkat elfogadnia.

8.14 táblázat – A célok visszavezetése a veszélyekre a CRL ellenőrzés csomag esetén

Sorszám	Célok	Veszély
1	O.Accurate_Rev_Info	T.Wrong_Revoc_Info_CRL
2	O.Auth_Rev_Info	T.Wrong_Revoc_Info_CRL
3	O.Fresh_Rev_Info	T.Replay_Revoc_Info_CRL

8.1.2.7 Az időbélyeg kérése és ellenőrzése csomag biztonsági céljainak indoklása

Először a veszélyek leképezését tekintjük át a 8.15 táblázat és az alatta olvasható magyarázó szöveg segítségével, majd a 8.16 táblázat a célokat vezeti vissza a veszélyekre.

8.15 táblázat – A veszélyek leképezése célokra az Időbélyeg kérése és ellenőrzése csomag esetén

Sorszám	Veszély	Célok
1	T.Replay_TimeStamp	O.Fresh_TimeStamp_Info
2	T.Wrong_TimeStamp_lnfo	O.Accurate_TimeStamp_Info O.Auth_TimeStamp_Info

T.Replay_TimeStamp: A felhasználó elfogadhat egy régi időbélyeg választ, mely következtében a TOE visszavont tanúsítványt érvényesnek fogad el. A veszélyből származtatott biztonsági cél:

- **O.Fresh_TimeStamp_Info**: A TSF-nek csak friss időbélyeg válaszokkal szabad dolgoznia, azaz minden időbélyeg feldolgozásnál új kérést kell kiküldenie, és az arra adott választ kell feldolgoznia.

T.Wrong_TimeStamp_lnfo: A felhasználó rossz időbélyeg válasz miatt elfogadhat egy visszavont tanúsítványt vagy visszautasíthat egy érvényeset. A veszélyből származtatott biztonsági cél:

- **O.Accurate_TimeStamp_Info**: A TSF-nek csak pontos időbélyeg választ szabad elfogadnia.
- **O.Auth_TimeStamp_Info**: A TSF-nek csak jogosult időbélyeg szolgáltatótól (időbélyeg forrásból) szabad időbélyeg választ elfogadnia.

8.16 táblázat – A célok visszavezetése a veszélyekre az Időbélyeg kérése és ellenőrzése csomag esetén

Sorszám	Célok	Veszély
1	O.Accurate_TimeStamp_Info	**T.Wrong_TimeStamp_Info**
2	O.Auth_TimeStamp_Info	**T.Wrong_TimeStamp_Info**
3	O.Fresh_TimeStamp_Info	**T.Replay_TimeStamp**

8.2 A biztonsági követelmények indoklása

Ez a szakasz a célokat képezi le a funkcionális követelményekre és indoklást ad a választott EAL, annak összetevői és szigorításai ismeretében.

8.2.1 A funkcionális biztonsági követelmények indoklása

Az összes biztonsági cél funkcionális követelményekre vagy feltételezésekre való leképezését mutatja a 8.17 táblázat. Az explicit módon megfogalmazott követelmények jellegükben hasonlóak a CC 2. rész követelményeihez, így a CC 3. rész garanciális követelményei alkalmazhatók ezek tesztelésére is, a CC 3. részén kívüli garanciális követelményre nincs szükség.

8.17 táblázat – A biztonsági célok leképezése funkcionális követelményekre

Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése csomag céljainak leképezése		
1	O.Correct_Time	IT környezet
2	O.Current_Certificate	IT környezet, Certificate Management Library
3	O.Get_KeyInfo	FDP_DAU_CPV_OUT.1
4	O.Path_Find	FDP_CPD.1
5	O.Trusted_Keys	IT környezet, Certificate Management Library, FMT_SMF.1
6	O.User	IT környezet, Certificate Management Library
7	O.Verified_Certificate	IT környezet, Certificate Management Library
8	O.Valid_Certificate	IT környezet, Certificate Management Library
A PKI aláírás létrehozás csomag céljainak leképezése		
1	O.Give_Sig_Hints	FDP_ETC_SIG.1
2	O.Delete_Key_Sig	FDP_RIP.1
A PKI aláírás ellenőrzés csomag céljainak leképezése		
1	O.Use_Sig_Hints	FDP_ITC_SIG.1,
2	O.Linkage_Sig_Ver	FDP_DAU_SIG.1
A PKI titkosítás kulcs átviteli algoritmusokkal csomag céljainak leképezése		
1	O.Hints_Enc_WO	FDP_ETC_ENC.1
2	O.Linkage_Enc_WO	FDP_ETC_ENC.1, FDP_DAU_ENC.1
A PKI megoldás kulcs átviteli algoritmusokkal csomag céljainak leképezése		
1	O.Correct_KT	FDP_ITC_ENC.1
2	O.Delete_Key_De	FDP_RIP.1
A CRL ellenőrzés csomag céljainak leképezése		
1	O.Accurate_Rev_Info	FDP_DAU_CRL.1
2	O.Auth_Rev_Info	FDP_DAU_CRL.1
3	O.Fresh_Rev_Info	FDP_DAU_CRL.1
Az időbélyeg kérése és ellenőrzése csomag céljainak leképezése		
1	O.Fresh_TimeStamp_Info	FDP_DAU_TS.1
2	O.Accurate_TimeStamp_Info	FDP_DAU_TS.1
3	O.Auth_TimeStamp_Info	FDP_DAU_TS.1

8.2.1.1 A környezet biztonsági céljainak indoklása

A környezetre vonatkozó biztonsági célokat feltételezések adott készlete, valamint kapcsolódó célok és követelmények elégítik ki. Jelen biztonsági előirányzat a környezet által teljesítendő biztonsági megfontolásokat a biztonsági célok szintjéig vezeti le, ezért a célok követelményekre lebontása az indoklások szakaszban sem szerepel. Szerepelnek azonban a CML IT környezeti összetevő által megvalósított célok, mivel a vonatkozó csomag céljait a MultiSigno v3.0.1 és a CML együttesen teljesíti.

8.2.1.2 Biztonsági célok a „Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése" csomagra - indoklás

O.Correct_Time: a TSF-nek gondoskodnia kell érvényes pontos időről. A biztonsági célt az alábbi IT környezeti követelmény(ek) teljesíti(k):

- Az **OE.Time:** környezeti követelmény kimondja, hogy a környezetnek hozzáférést kell biztosítania a pontos időhöz, megkívánt pontossággal, GMT formára alakítva.

O.Current_Certificate: a TSF-nek csak nem lejárt tanúsítványokat szabad elfogadnia. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- IT környezet CML összetevője végzi a tényleges érvényesség ellenőrzést.

O.Get_KeyInfo: a TSF-nek gondoskodnia kell a felhasználó nyilvános kulcsáról és az ahhoz kapcsolódó információkról a kriptográfiai műveletek elvégzése céljából.

- FMT_SMF.1 biztosítja a a tanúsítványok és íga a felhasználó nyilvános kulcsának tárolását, hozzáférését, és az FDP_DAU_CPV_OUT.1, Tanúsítási útvonal kimenet – alapkövetelmény: a TSF az alany nyilvános kulcsát kiveszi a tanúsítási útvonalból.

O.Path_Find: a TSF-nek képesnek kell lennie a tanúsítási útvonal felépítésére a végtanúsítványtól a megbízható pontig. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FDP_CPD.1, Tanúsítási útvonal felépítése: megköveteli, hogy a TSF (itt a CML IT környezeti összetevő) a végtanúsítványtól a megbízható pontig felépítse a tanúsítási útvonalat.

O.Trusted_Keys: a TSF-nek megbízható nyilvános kulcsokat kell használnia a tanúsítási útvonal érvényességének ellenőrzése során. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- IT környezet CML összetevője végzi a tényleges érvényesség ellenőrzést.

O.User: a TSF-nek csak CA által kibocsátott tanúsítványokat szabad elfogadnia. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- IT környezet CML összetevője végzi a tényleges érvényesség ellenőrzést.

O.Verified_Certificate: a TSF-nek csak ellenőrizhető aláírással bíró tanúsítványokat szabad elfogadnia. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- IT környezet CML összetevője végzi a tényleges érvényesség ellenőrzést.

O.Valid_Certificate: a TSF-nek érvényes, azaz nem visszavont tanúsítványokat kell használnia. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- IT környezet CML összetevője végzi a tényleges érvényesség ellenőrzést.

8.2.1.3 Biztonsági célok a PKI aláírás létrehozás csomagra - indoklás

O.Give_Sig_Hints: a TSF-nek utalnia kell arra, hogy melyik tanúsítványt vagy kulcsot kell kiválasztani a PKI aláíráshoz. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FDP_ETC_SIG.1 PKI aláírás exportálása: megköveteli, hogy a TSF a magánkulcsot használja a digitális aláíráshoz és a TSF emelje be a követelményekben meghatározott egyéb információkat a digitális aláírásba.

O.Delete_Key_Sig: A TSF-nek törölnie kell a felhasználó által megadott titkos kulcsot vagy az aláíráshoz használt magánkulcsot a memóriából azok felhasználása után. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FDP_RIP.1 Részleges maradványinformáció védelem: megköveteli, hogy magán és titkos kulcsok ne maradjanak ideiglenes tárolóterületen azok felhasználása után.

8.2.1.4 Biztonsági célok a PKI aláírás ellenőrzés csomagra - indoklás

O.Use_Sig_Hints: a TSF-nek használnia kell azt az információt, mely arra utal, hogy melyik tanúsítványt vagy kulcsot kell kiválasztani az aláírás ellenőrzéshez. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FDP_ITC_SIG.1, PKI aláírás importálása: megköveteli, hogy a TSF a következő adatokat használja az aláírt adatból: hash algoritmus, aláírási algoritmus, aláíró nyilvános kulcs tanúsítványa, aláíró DN-je (megkülönböztető neve), aláíró alany másodlagos neve, aláíró alany kulcsazonosítója, illetve az aláírás ellenőrzés során felmerülő egyéb adatok.

O.Linkage_Sig_Ver: a TSF-nek a megfelelő felhasználói nyilvános kulcsot kell használnia az aláírás ellenőrzéséhez. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FDP_DAU_SIG.1, Digitális aláírás érték ellenőrzés: megköveteli, hogy a TSF a következő információkat használja a tanúsítási útvonal érvényességének ellenőrzéséből az aláírt adatokon lévő digitális aláírás ellenőrzéséhez: alany nyilvános kulcs algoritmus, alany nyilvános kulcsa, alany nyilvános kulcs paraméterek, továbbá
  - minősített elektronikus aláírás esetén az aláíró tanúsítványában a kötelező qcStatements kiterjesztés meglétének ellenőrzése szükséges;
  - az alany DN-je a tanúsítási útvonal ellenőrzéséből megegyezik-e az aláírt adatban lévővel.

8.2.1.5 Biztonsági célok a PKI titkosítás kulcs átviteli algoritmusok használatával csomagra - indoklás

O.Hints_Enc_WO A TSF-nek utalni kell arra, hogy mely tanúsítványokat vagy kulcsokat kell kiválasztani a kulcs átviteli algoritmusok használatával történő PKI titkosításhoz. A célt teljesíti:

- FDP_ETC_ENC.1, PKI titkosítás exportálása – Kulcs átviteli algoritmusok: a TSF-nek a rejtjeles adatokkal együtt bizonyos információkat mellékelnie kell, és a TSF-nek használnia kell az alábbi információkat „Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése”-ből a rejtjeles adatok létrehozásához: alany nyilvános kulcs algoritmusa, alany nyilvános kulcsa, alany nyilvános kulcs paraméterek.

O.Linkage_Enc_WO A TSF-nek a megfelelő felhasználói nyilvános kulcsot kell használnia a kulcs átvitelhez. A célt teljesíti:

- FDP_ETC_ENC.1, PKI titkosítás exportálása – Kulcs átviteli algoritmusok: a TSF-nek használnia kell az alábbi információkat „Tanúsítási útvonal érvényesség ellenőrzésé és tanúsítványok kezelése”-ből a rejtjeles adatok létrehozásához: alany nyilvános kulcs algoritmusa, alany nyilvános kulcsa, alany nyilvános kulcs paraméterek.
- FDP_DAU_ENC.1, PKI titkosítás ellenőrzése – kulcs átvitel: a TSF az ST szerzője által megadott módon a kulcsátvitelre ellenőrzéseket kell végrehajtania.

8.2.1.6 Biztonsági célok a PKI megoldás kulcs átviteli algoritmusok használatával csomagra - indoklás

O.Correct_KT A TSF-nek a megfelelő magánkulcsot és kulcs átviteli algoritmust kell használnia:

- FDP_ITC_ENC.1, PKI titkosítás importálása – Kulcs átviteli algoritmusok, amely megköveteli, hogy a TSF a követelményekben meghatározott információkat felhasználja a rejtjeles adatokból, hogy azonosítani lehessen a megfelelő magánkulcsot és kulcs átviteli algoritmust, és a TSF végre tudja hajtani a megoldást (dekódolást).

O.Delete_Key_De: A TSF-nek törölnie kell a felhasználó által megadott titkos kulcsot vagy a megoldáshoz használt magánkulcsot a memóriából azok felhasználása után. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FDP_RIP.1 Részleges maradványinformáció védelem: megköveteli, hogy magán és titkos kulcsok ne maradjanak ideiglenes tárolóterületen azok felhasználása után.

8.2.1.7 A CRL érvényesség ellenőrzés csomag indoklás

O.Accurate_Rev_Info: a TSF-nek csak pontos visszavonási információkat szabad elfogadnia. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FDP_DAU_CRL.1 Alap CRL ellenőrzés: megköveteli, hogy a TSF pontos visszavonási információkat fogadjon el. A pontosságot ellenőrzések sorozata és szabályok sora határozza meg ezen a 2. rész kiterjesztési követelményen belül.

O.Auth_Rev_Info: a TSF-nek csak jogosult CRL forrásból szabad visszavonási információkat elfogadnia. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FDP_DAU_CRL.1, Alap CRL ellenőrzés: megköveteli, hogy a TSF az ST szerzője által megjelölt vagy kiválasztott jogos forrástól fogadjon el visszavonási információkat.

O.Fresh_Rev_Info: a TSF-nek csak aktuális (friss) CRL-t szabad elfogadnia. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FDP_DAU_CRL.1, Alap CRL ellenőrzés: megköveteli, hogy a TSF csak valószerű aktuális visszavonási információt fogadjon csak el, az FDP_DAU_CRL.1-ben definiált szabályok sorozata alapján.

8.2.1.8 Az Időbélyeg kérése és ellenőrzése csomag indoklása

O.Accurate_TimeStamp_Info: A TSF-nek csak pontos időbélyeg választ szabad elfogadnia. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FDP_DAU_TS.1 Időbélyeg kérés és ellenőrzés: megköveteli, hogy a TSF pontos időbélyeg választ fogadjon el. A pontosságot ellenőrzések sorozata és szabályok sora határozza meg ezen a 2. rész kiterjesztési követelményen belül.

O.Auth_TimeStamp_Info: A TSF-nek csak jogosult időbélyeg szolgáltatótól (időbélyeg forrásból) szabad időbélyeg választ elfogadnia. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FDP_DAU_TS.1, Időbélyeg kérés és ellenőrzés: megköveteli, hogy a TSF a TOE-t hívó alkalmazás által megjelölt vagy kiválasztott jogos forrástól fogadjon el visszavonási információkat.

O.Fresh_TimeStamp_Info: A TSF-nek csak friss időbélyeg válaszokkal szabad dolgoznia, azaz minden időbélyeg feldolgozásnál új kérést kell kiküldenie, és az arra adott választ kell feldolgoznia. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FDP_DAU_TS.1, Időbélyeg kérés és ellenőrzés: megköveteli, hogy a TSF csak valószerű aktuális időbélyeg választ fogadjon csak el, az FDP_DAU_TS.1-ben definiált szabályok sorozata alapján.

8.2.2 A garanciális követelmények indoklása

A MultiSigno v3.0.1 értékelési garanciaszintje: MIBÉTS kiemelt (EAL4). Ez olyan TOE-kre megfelelő választás, amelyek közepestől magas szintig terjedő függetlenül garantált biztonságot igényelnek a hagyományos piaci TOE-kre, és magasabb biztonsággal kapcsolatos megvalósítási költségeket is készek a gyártók áldozni a termékre. Az EAL4 a biztonsági funkciók elemzése által ad garanciát.

8.3 A függőségek teljesítésének indoklása

8.18 táblázat – Funkcionális követelmények közötti függések

Sorszám	**Követelmény**	**Függések**
Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése csomag		
1	FDP_CPD.1	Nincs
2	FDP_DAU_CPV_OUT.1	Nincs
3	FMT_SMF.1	Nincs
PKI aláírás létrehozás		
1	FDP_ETC_SIG.1	FCS_COP.1 (Lásd 2. megjegyzést)
2	FDP_RIP.1	Nincs
PKI aláírás ellenőrzés		
1	FDP_ITC_SIG.1	Nincs
2	FDP_DAU_SIG.1	FCS_COP.1 (Lásd 2. megjegyzést)
PKI titkosítás kulcs átviteli algoritmusokkal		
1	FDP_ETC_ENC.1 FCS_COP.1 (Lásd 2. megjegyzést)	FDP_DAU_CPV_OUT.1 (Lásd 3. megjegyzést)
2	FDP_DAU_ENC.1	FDP_DAU_CPV_OUT.1 (Lásd 3. megjegyzést)
PKI megoldás kulcs átviteli algoritmusokkal		
1	FDP_ITC_ENC.1	FCS_COP.1 (Lásd 2. megjegyzést)
2	FDP_RIP.1	Nincs
CRL ellenőrzés		
1	FDP_DAU_CRL.1	FCS_COP.1 (Lásd 2. megjegyzést) FPT_STM.1 (Lásd 1. megjegyzést)
Időbélyeg kérése és ellenőrzése		
1	FDP_DAU_TS.1	FCS_COP.1 (Lásd 2. megjegyzést) FPT_STM.1 (Lásd 1. megjegyzést)

1. megjegyzés: A megbízható időbélyegeket az informatikai környezet biztosítja, erre feltételezés szerepel az 3. fejezetben.
2. megjegyzés: The FCS_COP.1 függés nem szerepel a csomagban, mivel a kriptográfiai modul, amely része a környezetre vonatkozó feltételezéseknek, szolgáltatja a kriptográfiai műveleteket, beleértve a FCS_COP.1-et.

3. megjegyzés A függést teljesíti Tanúsítási útvonal érvényesség ellenőrzése és tanúsítványok kezelése csomag szerepeltetése.

8.4 A TOE összefoglaló előírás indoklása

Az alábbi táblázat felsorolja a MultiSigno v3.0.1 összes biztonsági követelményét, és megmutatja, hogy minden követelményt teljesíti egy vagy több biztonsági funkció, illetve egy biztonsági funkció visszavezethető egy vagy több biztonsági követelményre.

	BF1 Aláírás létrehozása	**BF2 Elektronikus aláírás ellenőrzése**	**BF3 Időbélyeg kérések és válaszok kezelése**	**BF4 Tanúsítási útvonal felépítése és érvényesség ellenőrzése**	**BF5 Tanúsítványtár kezelés**	**BF6 Titkosítás és megoldás**
FDP_CPD.1			**X**	**X**		
FDP_DAU_CPV_OUT.1		**X**	**X**	**X**		**X**
FMT_SMF.1					**X**	
FDP_ETC_SIG.1	**X**					
FDP_ITC_SIG.1		**X**				
FDP_DAU_SIG.1		**X**				
FDP_ETC_ENC.1						**X**
FDP_DAU_ENC.1						**X**
FDP_ITC_ENC.1						**X**
FDP_DAU_CRL.1				**X**		
FDP_DAU_TS.1			**X**			
FDP_RIP.1	**X**					**X**

9. Fogalmak, rövidítések

9.1 Fogalmak

Aláírás dátuma
A digitális aláírás létrehozásának dátuma. A dátum tartalmazza a naptári dátumot és az időpontot. Az elfogadó félnek meg kell bíznia az aláírás dátumának pontosságában. A dátum lehet a tényleges dátum vagy egy feltételezett dátum. Az elfogadó fél feltételezheti, hogy az aláírás dátuma a dokumentum vételének a dátuma. Az elfogadó fél tudatában van, hogy az aláírásnak a vételt megelőzően kellett történnie.

Aláírás ellenőrzés
Az a folyamat, mely során egy aláírást ellenőriznek, és a következő lépésekből áll: 1. Tanúsítási útvonal érvényesség ellenőrzése az aláíró nyilvános kulcsa iránti bizalom megalapozásához; 2. Az ellenőrzendő üzenet hash értékének kiszámítása; és 3. Az első lépésben ellenőrzött aláíró nyilvános kulcsának, és a második lépésben számított hash értéknek, illetve az aláírásnak a segítségével megfelelő kriptográfiai algoritmus alkalmazása az aláírás érvényességének megállapítása céljából.

Aláíró
Az az egyed (például személy), aki egy tanúsítványban szereplő nyilvános kulcshoz tartozó magánkulcsot birtokol. A tanúsítvány alany mezője nevezi meg az aláírót.

Aszimmetrikus kulcsok
Olyan kulcspár, mely két tagját (az úgynevezett magánkulcsot és az ennek megfelelő nyilvános kulcsot) egyszerre generálják, különböző értéket vesznek fel, és az egyikkel titkosított információt a másikkal lehet dekódolni, vagy az egyikkel digitálisan aláírt információt a másikkal lehet ellenőrizni. A magánkulcsot nem lehet a nyilvános kulcsból származtatni, csak igen nagy —gyakorlati szempontból kivitelezhetetlen— számítási komplexitás révén.

Digitális boríték
Egy szimmetrikus session (munkaszakasz) kulccsal titkosított adatokból álló adathalmaz, ahol a session kulcsot az egyes fogadók számára a fogadó nyilvános kulcsával titkosították.

Digitálisan aláírt adatok
Adatok összessége (az aláírt adatok) és egy érték (a digitális aláírás), melyet az adatokból számítottak. Az aláírás az adatokon (vagy az adatokból származtatott közbenső értéken) elvégzett aszimmetrikus kriptográfiai algoritmus alkalmazásának eredménye. Az adathalmaz tartalmazhat olyan információkat, melyek segítik az adatot aláíró egyed hitelességének ellenőrzését.

Digitális aláírás (Aláírás)
Olyan érték, mely úgy képződik, hogy az aláírandó adatból először egy hash értéket számítanak, majd egy kriptográfiai funkciót (az aláírási algoritmust) alkalmaznak a hash értékre az aláíró magánkulcsa segítségével.

Elfogadó fél
Olyan egyed vagy szervezet, amely megbízik egy tanúsítványban (azaz felhasználja a tanúsítványban lévő nyilvános kulcsot digitális aláíráshoz és/vagy rejtjelezéshez), valamint megbízik a tanúsítványban szereplő aláíró azonosságának (alany neve) és nyilvános kulcsának összetartozásában.

Gyökér tanúsítvány
A hitelesítő szervezet hierarchiájának tetején szereplő tanúsítvány. Ez egy önaláírt tanúsítvány, ami azt jelenti, hogy a tanúsítvány kibocsátója és az alany ugyanaz az egyed, jelen esetben a gyökér CA. A tanúsítvány általában egy megbízható pont. Mivel az önaláírt tanúsítványokban nem bíznak meg, ezért a gyökér tanúsítványt vagy bármilyen más önaláírt tanúsítványt biztonságos módszerek segítségével kell szétosztani.

Hash algoritmus
Olyan algoritmus, amely változó hosszú bemenetet képez le rögzített hosszúságú eredményre, melyet "digest"-nek vagy "hash"-nek neveznek. Az algoritmus N:1 típusú függvény, elvileg több bemenet is ugyanazt az értéket produkálhatja, de egy kívánt vagy rendelkezésre álló eredményhez a bemeneti érték kiszámítása gyakorlatilag nem kivitelezhető.

Kulcspár
Két összetartozó kulcs, melyeket az aszimmetrikus kriptográfia használ. A kulcsokat egy kulcsgenerálási algoritmus hozza létre.

Lejárt tanúsítvány
Olyan tanúsítvány, melyben az érvényességi mező **not after** eleme korábbi értéket tartalmaz, mint az aktuális dátum. A lejáratuk után az ilyen tanúsítványok vagy megjelennek a CRL-ekben vagy nem.

Letagadhatatlanság
Egy tevékenység végrehajtásának letagadását megakadályozó tulajdonság. A letagadhatatlanság egy üzenet aláírója azonosságának és az üzenet integritásának bizonyítéka, amely elegendő ahhoz, hogy meggátolja azt, hogy valamely fél letagadja egy üzenet eredetét, kibocsátását vagy továbbítását, valamint biztosítja az üzenettartalom sértetlenségét.

Magánkulcs
Kizárólag egy adott egyed számára ismert szám, mely egyedet a kulcs tulajdonosának nevezünk (a tulajdonos gondoskodik a titkosságról). A tulajdonosok a magánkulcsot az általuk elküldött adatok aláírásának számítására, illetve a nekik továbbított üzenetek dekódolására használják.

Megbízható harmadik fél
Olyan egyed, akit vagy amelyet más entitások megbízhatónak tartanak, hiteles és feddhetetlennek ítélt bizonyos szolgáltatás elvégzése tekintetében. A megbízható harmadik fél rendszerint nem részrehajló, és semleges a szolgáltatás elvégzése szempontjából.

Megbízható időpecsét
Digitálisan aláírt adathalmaz vagy más olyan eszköz, amely bizonyítékul szolgál arra, hogy egy dokumentum egy bizonyos időpont előtt már létezett. Az adathalmaz tartalmazza a dátumot és időpontot, valamint a dokumentumot vagy annak hash értékét. Gyakran egy megbízható harmadik fél biztosítja az időpecsét szolgáltatást.

Megbízható pont
Olyan tanúsítvány, melyben az ellenőrző fél közvetlenül megbízik. A tanúsítvány tartozhat CA-hoz vagy végentitáshoz. A tanúsítvány megbízható, mert az aláírás ellenőrző fél a PKI-n kívüli megbízható eszközökkel jutott a tanúsítvány birtokába, és elhiszi, hogy a tanúsítvány pontosan köti össze az előfizető egyed nevét annak nyilvános kulcsával. Amennyiben a megbízható pont egy CA tanúsítvány, akkor az ellenőrző félnek meg kell bíznia minden, a CA által kibocsátott tanúsítványban. Ez a bizalom tranzitív, az X.509 tanúsítvány kiterjesztés által megengedett mértékig; ha a CA egy másik CA-nak bocsát ki tanúsítványt, az ellenőrző fél ebben a másik CA-ban is megbízik, ha az X.509 útvonal érvényesség ellenőrzési logika teljesül.

Nyilvános kulcs
Olyan szám, mely egy adott egyedhez tartozik, és mindenki számára ismertté tehető. A nyilvános kulcs szolgál egy aláírás ellenőrzésére és/vagy olyan információk rejtjelezésére, melyeket csak ezen egyed tud dekódolni.

Nyilvános kulcs infrastruktúra
Azon erőforrások (emberek, rendszerek, folyamatok és eljárások), melyek új tanúsítványok tulajdonosait regisztrálják és azonosítják, visszakeresik a tanúsítványokat és meghatározzák azok érvényességét.

Nyilvános kulcsú szolgáltatásokat tartalmazó alkalmazás
Olyan szoftver alkalmazás, amely nyilvános kulcs technológiát használ a következőkhöz: felhasználók (emberek, rendszerek és eszközök) hitelesítése, információ módosítás megakadályozása átvitel vagy tárolás során, felhasználók felelősségre vonhatóságának és elszámoltathatóságának biztosítása (azaz felelősség letagadás kivédése), információ rejtjelezése, akik között az előzetes egyeztetés nem lehetséges vagy nem kivitelezhető. A nyilvános kulcs szolgáltatásokat tartalmazó alkalmazások a PKI-ra épülnek a tanúsítványok létrehozása (mely eredményeként korrekt módon összekapcsolják a magánkulcs tulajdonosának nevét és nyilvános kulcsát), tanúsítványok visszanyerése és a tanúsítványok érvényességének meghatározása (például CRL lehívása) céljából.

9.2 Rövidítések

CA	**Certification Authority**	**Hitelesítés-szolgáltató**
CC	**Common Criteria**	**Közös szempontok**
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./
PP	**Protection Profile**	**Védelmi profil** /Megvalósítástól független, olyan biztonsági követelményrendszer az értékelés tárgyainak (TOE-k) egy kategóriájára, amely adott fogyasztói igényeket elégít ki./
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 funkció (SF) által érvényre juttatott biztonsági szabályzat./
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./
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./
TSF	**TOE Security Functions**	**TOE biztonsági funkciói** **/**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./
TSP	**TOE Security Policy**	**TOE biztonsági szabályzata** **/**Szabályok olyan összessége, amely szabályozza a vagyontárgyak kezelését, védelmét, elosztását az értékelés tárgyán (TOE-n) belül./
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./