InfoSigno for Developer
minősített elektronikus aláíráshoz
v1.0.0

Biztonsági előirányzat

Verzió:	V1.0
Dátum:	2006.04.30.
Megrendelő:	Argeon Üzleti Szolgáltató Kft.
Fájl:	InfoSigno_ST_v10.pdf
Minősítés:	Nyilvános
Oldalak:	93

Tartalomjegyzék

Változás kezelés

Verzió	Dátum	Leírás	Készítette
0.4	2005.12.31.	A 2., 3., 4. és 6. fejezetek tervezetének elkészítése	Juhász Judit
0.7	2006.02.11.	Az ST további részeinek elkészítése	Juhász Judit
0.9	2006.04.20.	Az ST pontosítása a fejlesztői bizonyítékok alapján	Juhász Judit
0.98	2006.04.25	Az ST pontosítása és kiegészítése az értékelés megállapításai és kérdései alapján	Juhász Judit
1.0	2006.04.30.	Az ST véglegesítése a fejlesztők észrevételei alapján	Juhász Judit

1. Bevezetés

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

1.1 Azonosítás

Cím:	InfoSigno for Developer minősített elektronikus aláíráshoz v1.0.0 - Biztonsági előirányzat
Az értékelés tárgya:	InfoSigno for Developer fejlesztőkészlet (SDK) v1.0.0 r119
Az értékelés tárgya rövid neve:	InfoSigno v1.0.0
Értékelési garancia szint:	MIBÉTS kiemelt (EAL4)
Biztonsági funkcióerősség:	SOF-alap
Verzió szám:	1.0.0
Dátum:	2006. április 30.
Szerző:	Juhász Judit
Szponzor szervezet:	Argeon Üzleti és Szolgáltató Kft.
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 előirányzatban az eredeti PKE PP család választott csomagjain túl kiegészült egy „Időbélyeg kérése és ellenőrzése” 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;
- aszimmetrikus (kulcsátvitelhez) és szimmetrikus kulcsú (adatátvitelhez) titkosítás és dekódolás;
- időbélyegzés (kérése és ellenőrzése).

Ennek alapján az InfoSigno v1.0.0 fejlesztői készlet segítségével alkalmazások széles köre fejleszthető, 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 az InfoSigno v1.0.0 igényeinek.
Az alábbi táblázat az InfoSigno v1.0.0 legfontosabb funkcióit, a PKE PP védelmi profil családból kiválasztott csomagokat és az időbélyeg kliens csomagot tekinti át.

Csomag neve	**Funkcionalitás**	**Függések**
Tanúsítási útvonal érvényesség ellenőrzése (CPV) – Alap	X.509 érvényesség ellenőrzést hajt végre, kivéve a szabályzat és név megszorítás feldolgozását	Nincs
PKI aláírás létrehozás	Magánkulcs használata aláírás létrehozására Aláírási információk generálása	Nincs
PKI aláírás ellenőrzés	Feldolgozza az aláírási információkat Nyilvános kulcsot használ az aláírás ellenőrzésére	CPV – Alap
PKI titkosítás kulcs átviteli algoritmusok használatával	Rejtjelezési boríték információkat generálja Nyilvános kulcsot használ a rejtjelezéshez	CPV – Alap
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 (CPV) - Alap

1.1 táblázat: Felhasznált csomagok

1.3 Kapcsolódó dokumentumok

- Department of Defense (DoD) Class 3 Public Key Infrastructure (PKI) Public Key-Enabled Application Requirements," Version 1.0, 13 July 2000 PKE-PP
- 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)
- ETSI TS 101 862 v1.3.3 (2006-01) Qualified Certificate profile
- 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
- RFC 3275

1.4 A biztonsági előirányzat szerkezete

A 2., 3., és 4. fejezetek az InfoSigno leírását, a biztonsági környezetet (feltételezéseket, fenyegetéseket és szervezeti biztonsági szabályzatokat), illetve a biztonsági célokat adják meg. Ezek az egyes csomagok szerint külön kerültek leírásra.
Az 5.1-5.2 alfejezetek az általános, illetve az egyes csomagokra vonatkozó funkcionális biztonsági követelményeket írják le. Az 5.3 alfejezet a MIBÉTS kiemelt garaciaszint követelményeit írja le.
A 6. fejezet az InfoSigno által megvalósított biztonsági funkciókat és garanciális intézkedéseket határozza meg.
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).
Az InfoSigno v1.0.0 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 InfoSigno v1.0.0 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 tárgyának (TOE, InfoSigno) leírása

2.1 Áttekintés

A jelen biztonsági előirányzat követelményeinek megfelelő alkalmazás (InfoSigno v1.0.0 fejlesztői függvénykönyvtár) nyilvános kulcs szolgáltatásokat biztosít az alábbi funkciói alapján:

- Biztonságosan kezel kulcsokat, megbízható pontokat és tanúsítványokat.
- Elfogad és feldolgoz X509 v3 nyilvános kulcs tanúsítványokat.
- Képes a szükséges tanúsítványok és visszavonási adatok megszerzésére.
- Ellenőrzi minden tanúsítvány érvényességét, az X.509 szabványban [ISO 9594-8] leírt eljárások felhasználásával, beleértve a visszavonás ellenőrzését 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 (dekódolást) végez.

2.2 Megközelítés

Jelen biztonsági előirányzat a PKE védelmi profil családon alapul, bár PP-megfelelőségi nyilatkozatot nem tesz. A PKE PP-ben szereplő csomagok módosított, kiegészített követelményei adják az InfoSigno v1.0.0 funkcionalitását.

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

A CC 2. részét felhasználva a biztonsági szempontból fontos követelmények kialakításához jelen biztonsági előirányzat csak a PKI szolgáltatás biztonsági szempontjaival foglalkozik. A PP (s így jelen ST sem) 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 összetevői 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 (InfoSigno v1.0.0) meghatározása

Ebben a szakaszban az InfoSigno v1.0.0 típusát és struktúráját ismertetjük, bemutatjuk kapcsolatait és határait más összetevők felé.

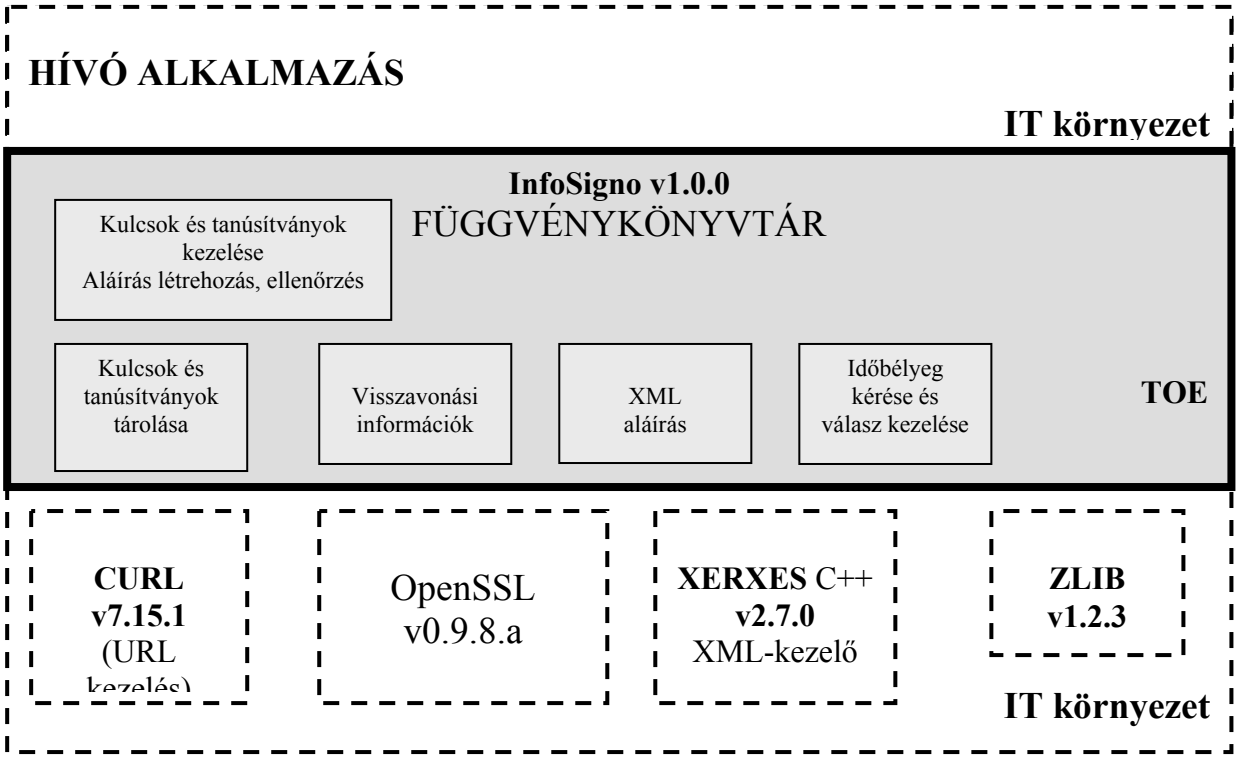
2.3.1 A TOE típusa

Az InfoSigno v1.0.0 szoftverfejlesztők számára készült, zárt rendszerben felhasználásra kerülő, nyilvános kulcs szolgáltatásokat biztosító C++ függvénykönyvtár, olyan funkcionalitással, mellyel elektronikus aláírások létrehozása, ellenőrzése, az ellenőrzéshez érvényesítő információk feldolgozása, tanúsítási útvonal felépítése, tanúsítványok érvényességének ellenőrzése, visszavonási információk érvényesség ellenőrzése, időbélyeg kérése és ellenőrzése, adatok titkosítása és megoldása valósítható meg.

Az InfoSigno v1.0.0 az OpenSSL funkcióira épít, azokat felhasználja működése során, ezen keresztül valósítja meg a kriptográfiai funkcionalitást. Ezen kívül a Windows tanúsítványtár kezelését a Windows Crypto API felhasználásával valósítja meg. A kriptográfiai token eszközök kezelése PKCS#11 felületen keresztül történik.

2.3.2 A TOE felépítése

Az 1. ábra az InfoSigno v1.0.0 struktúráját és az IT környezetbe való beágyazódását –a TOE határaival - mutatja be.



1. ábra Az InfoSigno v1.0.0 és környezete

Az InfoSigno v1.0.0 közvetlen interfészeit azok az OpenSSL és egyéb alapul szolgáló hívások képezik, amelyek a magasabb szintű alkalmazások, függvénykönyvtárak fejlesztői számára biztosítanak publikus függvényeket.
A TOE közvetlenül nem kezdeményez hálózati kapcsolatot és fájlhozzáférést. A fájlokat OpenSSL-en és XERXES-en keresztül, a hálózati kapcsolatokat pedig a CURL csomagon keresztül éri el.

Az InfoSigno v1.0.0 az IT környezet 1. ábrán látható elemeit az alábbi feladatok elvégzéséhez használja:

- CURL v7.15.1: URL-alapú adathozzáféréseket kiszolgáló modul.
- OpenSSL v 0.9.8.a: nyílt forrású eszközkészlet általános kriptográfiai szolgáltatások megvalósítására.
- XERXES C++ v2.7.0: XML feldolgozó modul.
- ZLIB v1.2.3: gzip formátum-kompatibilis tömörítési eljárásokat tartalmazó könyvtár.

Az InfoSigno v1.0.0 biztonsági funkciói szempontjából az OpenSSL és a CURL csomagok biztosítanak közvetve TOE biztonsági funkciót támogató funkciót.

Az InfoSigno v1.0.0 két használati esetet különböztet meg:

- Fokozott biztonságú aláírás létrehozás használati esete
    - Az InfoSigno v1.0.0-t biztonságos aláírás létrehozó eszköz nélkül használják elektronikus aláírások generálására és ellenőrzésére. Ezen belüli esetek:
        - KHE (kriptográfiai hardver eszköz) használata;
        - PKCS#12 szoftveres kulcstároló állomány használata
        - Windows tanúsítványtár.
- Minősített elektronikus aláírás létrehozás használati esete
    - Minősített aláírás létrehozása esetén kötelező a BALE használata, illetve nem megbízható környezetben a BALE és az aláírás létrehozó alkalmazás (TOE) között megbízható útvonal kiépítésére van szükség. Az aláírás létrehozásához használt tanúsítványnak minősítettnek kell lennie. Az InfoSigno v1.0.0 BALE-hez való hozzáférést PKCS#11 interfészen keresztül valósítja meg.

2.4 A TOE alkotóelemei

A 2.1 táblázat az alapul szolgáló PKE PP család által megvalósított csomag-elv alapján az InfoSigno v1.0.0-hoz kiválasztott funkciók összegzését adja, a táblázat után pedig a csomagok funkcionalitását találhatjuk.
Vannak olyan csomagok, melyek más csomagoktól függnek, azaz amikor egy függő csomagot szerepeltetünk biztonsági előirányzatban, akkor azt a csomagot is be kell venni teljes egészében, amelytől függ. A táblázat tartalmazza a csomagok közötti függéseket is.

2.1 táblázat – A csomagok áttekintése
Az InfoSigno v1.0.0 a PKE PP család alábbi csomagjainak biztonsági követelményeit veszi alapul.

Csomag neve	**Funkcionalitás**	**Függések**
Tanúsítási útvonal érvényesség ellenőrzése (CPV) – Alap	X.509 érvényesség ellenőrzést hajt végre, kivéve a szabályzat és név megszorítás feldolgozását	Nincs
PKI aláírás létrehozás	Magánkulcs használata aláírás létrehozására Aláírási információk generálása	Nincs
PKI aláírás ellenőrzés	Feldolgozza az aláírási információkat Nyilvános kulcsot használ az aláírás ellenőrzésére	CPV – Alap
PKI titkosítás kulcs átviteli algoritmusok használatával	Rejtjelezési boríték információkat generálja Nyilvános kulcsot használ a rejtjelezéshez	CPV – Alap
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 (CPV) - Alap

2.4.1 Tanúsítási útvonal érvényességének ellenőrzése - Alapcsomag

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. A megbízható pontok hozzáadását, törlését, menedzselését TOE hatáskörön kívül kell kezelni az erre szolgáló konfigurációs fájl segítségével.
- **Közbenső tanúsítványok**: Ezek a hitelesítés-szolgáltatók (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.

Jelen csomag a **keyUsage** biztonsággal kapcsolatos tanúsítvány kiterjesztési ellenőrzéseket veszi számításba. Minősített elektronikus aláírás létrehozása és ellenőrzése esetén pedig ellenőrzi a **qCStatement** kiterjesztést.
Az útvonal érvényesség ellenőrzése az elektronikus aláírásra kért időbélyeg (ha van), egyébként aláírás önbevallott ideje (SigningTime) szerint történik.

2.4.2 PKI aláírás létrehozás csomag

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

Az InfoSigno v1.0.0 az aláírás létrehozását és ellenőrzését az alábbi digitális aláírás sémák szerint valósítja meg:

- RSA algoritmus 1024 bit kulcshosszal, az SHA-1 lenyomatkészítő algoritmussal [PKCS#1.5-nek megfelelően].

A TOE-t úgy tervezték, hogy alkalmas legyen nemcsak fokozott biztonságú, hanem minősített elektronikus aláírások létrehozására és ellenőrzésére, a magyar jogszabályi előírásoknak megfelelően. Ez utóbbiak megkövetelik, hogy a magánkulcs műveletekhez szükség van egy külső biztonságos aláírás-létrehozó eszközre (tanúsított, NHH által nyilvántartásba vett BALE-re), amelyet a magánkulcs az életciklusa során nem hagy el, az aláírás létrehozása szigorúan az eszközön belül történik.

2.4.3 PKI aláírás ellenőrzés csomag

A PKI aláírás létrehozás csomag a **CPV – Alap** csomagtól függ. Aláírási információk, XML aláírás (XAdES-C formátum) feldolgozására és egy aláírás ellenőrzésekor a nyilvános kulcs használatára tartalmaz funkciókat.
További részletek: PKI aláírás létrehozás csomagnál.

2.4.4 PKI titkosítás kulcs átviteli algoritmusok használatával csomag

A „PKI titkosítás kulcs átviteli algoritmusok használatával” csomag a CPV – Alap csomagtól függ. Kulcs átviteli algoritmusokat alkalmazó (pl. RSA) nyilvános kulcsú titkosítás végrehajtására tartalmaz funkciókat.

Az InfoSigno v1.0.0 a titkosító-megoldó funkcionalitása részeként adatok rejtjelezésére és megoldására alkalmazható algoritmusokat valósít meg. A kulcsok kezelésének problémaköre kívül esik a TOE határain. A TOE funkciókat hívó alkalmazás gondoskodik a kulcsok TOE felé juttatásáról. A TOE nem módosítja az alkalmazástól kapott kulcsokat, és biztosítja, hogy a kulcsok védve legyenek más alkalmazások és egyedek elől.

A TOE az alábbi blokkos rejtjelezési algoritmusokat valósítja meg:

- AES 256 bit [FIPS PUB 197].

A blokkos rejtjelezéshez használt adatrejtjelezési session kulcs képzése a TOE határain kívül eső OpenSSL véletlenszám generátorával történik.

Az InfoSigno v1.0.0 a következő aszimmetrikus titkosító algoritmusokat valósítja meg:

- RSA algoritmus 1024 bit kulcshosszal, az SHA-1 lenyomatkészítő algoritmussal [PKCS#1.5-nek megfelelően]

2.4.5 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.
További részletek: a „PKI titkosítás kulcs átviteli algoritmusok használatával” csomagnál.

2.4.6 Tanúsítvány visszavonási lista (CRL) érvényesség ellenőrzése csomag

A „CRL érvényesség ellenőrzése” csomag lehetővé teszi, hogy a TOE 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.

2.4.7 Időbélyeg kérése és ellenőrzése csomag

Az „Időbélyeg kérése és ellenőrzése” csomag lehetővé teszi, hogy az InfoSigno v1.0.0 Időbélyeget kérjen egy időbélyegzés-szolgáltatótól, illetve ellenőrizze a kapott választ az RFC 3161-nek megfelelően.

2.5 Garanciális követelmények

A TOE értékelésre vonatkozó garanciakövetelménye: MIBÉTS kiemelt (CC 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**	Az infoSigno-t megfelelően telepítik és konfigurálják.
3	**AE.Crypto_Module**	Az InfoSigno által meghívott kriptográfiai funkciókról feltételezés, hogy hatáskörén kívüli modulok hajtják végre, melyek megbízhatónak tekinthetők az InfoSigno által hívott, kriptográfiai funkciók megvalósítása terén. Minősített elektronikus aláírás létrehozása esetén az InfoSigno 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.Physical_Protection**	A környezetről feltételezzük, hogy fizikailag véd. Az InfoSigno szoftverről feltételezzük, hogy védett a jogosulatlan fizikai hozzáféréssel szemben.
5	**AE.PKI_Info**	A tanúsítvány és tanúsítvány visszavonási információk a TOE rendelkezésére állnak.
6	**AE.Time**	A környezetről feltételezzük, hogy GMT formában és a megkívánt pontossággal gondoskodik a pontos rendszeridőről.
7	**AE.TimeStamp**	A környezetről feltételezzük, hogy biztosítja az időbélyegzés szolgáltatóhoz való hozzáférést.

3.2 Általános biztonsági fenyegetések

Ez az alfejezet az InfoSigno-t fenyegető általános (csomagoktól független) veszélyeket, a 3.3 alfejezet pedig a csomagokra vonatkozó biztonsági veszélyeket azonosítja. Minden vesély esetén igaz, hogy a támadott érték az értékelés tárgyán valamilyen formában áthaladó információ. Általánosságban a veszély forrásai az alábbiak lehetnek (de nem kizárólagosan):

1) az InfoSigno-hoz hozzáférő olyan egyének, akik „átlagos" szakértelemmel, kevés erőforrással bírnak és közepes motiváció jellemzi őket (alacsony támadási potenciálú támadók); vagy
2) az InfoSigno hibája.

3.2 táblázat – Álatános biztonsági fenyegetések

Sor-szám	Veszély megnevezése	Veszély leírása
1	**T.Attack**	Az InfoSigno 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 TOE-specifikus biztonsági fenyegetések

3.3.1 Tanúsítási útvonal érvényességének ellenőrzése – Alap csomag

Az alapveszélyeken kívül, az alábbi fenyegetések sorolhatók a "tanúsítási útvonal ellenőrzés - alap" csomagjába.

3.3 táblázat– A "tanúsítási útvonal érvényesség ellenőrzése – alap" 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 generálás" csomagot jellemzik.

3.4 táblázat – A PKI aláírás generálási 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.

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 feltételezhet 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 feltételezhet 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.

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_lnfo**	A felhasználó rossz időbélyeg válasz miatt elfogad egy visszavont tanúsítványt vagy visszautasít egy érvényeset.

3.4 Szervezeti biztonsági szabályok

Ezen biztonsági előirányzat alapját képező védelmi profil család nem tartalmaz szervezeti biztonsági szabályokat.
Jelen biztonsági előirányzat sem tartalmaz szervezeti biztonsági szabályokat.

4. Biztonsági célok

Ez a fejezet azonosítja az InfoSigno v1.0.0 (4.2 alfejezet), illetve annak informatikai környezete (4.1 alfejezet) által teljesítendő biztonsági célokat
„OE" előtag jelöli a környezet által, „O" előtag pedig az InfoSigno v1.0.0 által teljesítendő célokat.

4.1 Az InfoSigno informatikai környezetére vonatkozó általános biztonsági célok

4.1 táblázat – Az InfoSigno 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 TOE-t úgy kell telepíteni és konfigurálni, hogy a TOE biztonságos állapotban kezdjen el üzemelni.
16	OE.Crypto	A TOE által meghívott kriptográfiai funkciókat TOE hatáskörén kívüli modulok hajtják végre (például 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.
17	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 az áramingadozás elemzés és az időzítés elemzés különböző formái.
18	OE.PKI_Info	Az IT környezetnek biztosítania kell a TOE számára a tanúsítvány és tanúsítvány visszavonási információkat, valamint az időbélyegzés szolgáltatóhoz való hozzáférést.
19	OE.Time	A környezetnek hozzáférést kell biztosítania a pontos időhöz, megkívánt pontossággal, GMT formára alakítva.

4.2 Az InfoSigno v1.0.0 által teljesítendő biztonsági célok

4.2.1 Tanúsítási útvonal érvényességének ellenőrzése – Alap csomag

4.2 táblázat – Biztonsági célok a CPV – Alap 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.

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.

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 az InfoSigno v1.0.0 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.

Az alábbi táblázat összesíti jelen biztonsági előirányzat funkcionális követelményeit.

5.1 táblázat– Kiterjesztett 2. vagy 3. rész követelmények

Követelmény	**2. részből származó vagy kiterjesztett**
FDP_ACC.1	2. rész
FDP_ACF.1	2. rész
FDP_RIP.1	2. rész
FIA_AFL.1	2. rész
FIA_ATD.1	2. rész
FIA_UAU.1	2. rész
FIA_UAU.7	2. rész
FIA_UID.1	2. rész
FMT_MSA.1	2. rész
FMT_MSA.3	2. rész
FMT_MTD.1	2. rész
FMT_SMF.1	2. rész
FMT_SMR.2	2. rész
FPT_RVM.1	2. rész
FPT_SEP.1	2. rész
FPT_STM.1	2. rész
FCS_CRM_FPS.1	Kiterjesztett 2. rész
FDP_CPD.1	Kiterjesztett 2. rész
FDP_DAU_CPV_CER.1	Kiterjesztett 2. rész
FDP_DAU_CPV_CER.2	Kiterjesztett 2. rész
FDP_DAU_CPV_CER.3	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_PKI_INF.1/1 FDP_ITC_PKI_INF.1/2	Kiterjesztett 2. rész
FDP_ITC_SIG.1	Kiterjesztett 2. rész
FDP_DAU_TS.1	Kiterjesztett 2. rész

5.1 Az InfoSigno v1.0.0 környezete által teljesítendő általános funkcionális biztonsági követelmények

Az 5.2–es táblázat a PKE PP-ben szereplő általános funkcionális biztonsági követelményeket írja le, a táblázat után pedig a funkcionális követelmények kibontása következik. Jelen biztonsági előirányzatban az eredeti PKE PP általános biztonsági követelményeit kiegészítettük az eredeti védelmi profilban az IT környezetre vonatkozó követelményekkel.
Az általános biztonsági követelmények nagy részét az InfoSigno IT környezete biztosítja, de egyes funkciókat maga az InfoSigno is biztosít. Ilyen a hitelesítő adat cseréjét biztosító funkció.
Mivel jelen biztonsági előirányzat a PKE PP-t veszi alapul, ezért tartja magát a PP szemléletéhez. Az InfoSigno fejlesztői könyvtár jellege miatt azonban az általános követelmények némelyike TOE hatáskörbe esik, ezeket alkalmazási megjegyzésben jelezzük.

5.2 táblázat – Az InfoSigno IT környezetének általános funkcionális biztonsági követelményeinek készlete

Sorszám	Funkcionális követelmény	Cím
1	FDP_ACC.1	Részleges hozzáférés ellenőrzés - PKI engedélyek kezelése
2	FDP_ACF.1	Biztonsági tulajdonságokon alapuló hozzáférés ellenőrzés – PKI engedélyek kezelése
3	FIA_AFL.1	Sikertelen hitelesítés kezelése
4	FIA_ATD.1	Felhasználói tulajdonságok megadása
5	FIA_UAU.1	Hitelesítés időzítése
6	FIA_UAU.7	Védett hitelesítés visszacsatolás
7	FIA_UID.1	Azonosítás időzítése
8	FMT_MSA.1	Biztonsági tulajdonságok kezelése
9	FMT_MSA.3	Statikus tulajdonság inicializálás
10	FMT_MTD.1/1 FMT_MTD.1/2	TSF adatok kezelése
11	FMT_SMF.1/1 FMT_SMF.1/2	Menedzsment funkciók specifikációja
12	FMT_SMR.2	Megszorítások a biztonsági szerepkörökre
13	FPT_RVM.1	A TSP megkerülhetetlensége
14	FPT_SEP.1	TSF tartomány szétválasztás
15	FDP_ITC_PKI_INF.1/1 FDP_ITC_PKI_INF.1/2	PKI információk importálása a TSF-en kívülről
16	FDP_RIP.1	Részleges maradvány információ védelem
17	FCS_CRM_FPS.1	Kriptográfiai modulok
18	FPT_STM.1	Megbízható időbélyegek

5.1.1 FDP osztály – Felhasználói adatok védelme

FDP_ACC.1 Részleges hozzáférés ellenőrzés – PKI engedélyek kezelése
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FDP_ACC.1.1 Az **IT környezet TSF**-nek érvényt kell szereznie a **PKI engedélykezelési SFP**-nek az alábbi szubjektumok és objektumok között az alábbi műveletekre:
Szubjektumok:
- **Aláíró/ellenőrző fél által reprezentált folyamat**

Objektumok:
- **TOE folyamat által a hívó alkalmazástól kapott információ**

Műveletek:
- **TOE által szolgáltatott biztonsági funkció: aláírás létrehozás, aláírás ellenőrzés, időbélyeg kérés, időbélyeg válasz ellenőrzése, tanúsítvány útvonal felépítése, tanúsítvány útvonal érvényesítése, visszavonási információk lekérése.**

Függések: FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés

FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés – PKI engedélyek kezelése
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FDP_ACF.1.1 Az **IT környezet TSF-nek** érvényt kell szereznie **a PKI engedélykezelési SFP-nek** az objektumok vonatkozásában a szubjektum azonossága és a szubjektum által felvehető szerepkörök alapján.
FDP_ACF.1.2 Az **IT környezet TSF-nek** érvényre kell juttatnia az alábbi szabályokat annak meghatározása céljából, hogy megengedett-e egy művelet az ellenőrzött szubjektumok és ellenőrzött objektumok között
a) Magánkulcsok importálhatók, használhatók a TOE-t hívó alkalmazás által reprezentált folyamat által.
b) Nyilvános kulcs tanúsítványok importálhatók, exportálhatók, törölhetők, használhatók a TOE-t hívó alkalmazás által reprezentált folyamat által.
c) Nyilvános kulcs tanúsítványokat bárki felhasználhat.
d) Titkosításhoz használt session kulcs generálható a TOE-t hívó alkalmazás által reprezentált folyamat által.
e) Titkos kulcsot a TOE-t hívó alkalmazás csak RSA/1024 algoritmussal és kulcshosszal rejtjelezve továbbíthat és fogadhat.

FDP_ACF.1.3 Az **IT környezet TSF-nek** explicit módon kell megadnia a szubjektumok objektumokhoz való hozzáférési engedélyeit a következő szabályok alapján: **nincsenek további szabályok**.
FDP_ACF.1.4 Az **IT környezet TSF-nek** explicit módon le kell tiltania a szubjektumok objektumokhoz való hozzáféréseit**: nincsenek további szabályok**.
Függések: FDP_ACC.1 Részleges hozzáférés ellenőrzés
FMT_MSA.3 Statikus tulajdonságok inicializálása

FDP_ITC_PKI_INF.1/1 PKI információk importálása a TSF-en kívülről
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FDP_ITC_PKI_INF.1.1 Az **IT környezetnek** biztosítania kell a
- **magánkulcsok,**
- **tanúsítványok,**
- **kriptográfiai tokenekhez megfelelő PKCS#11 interfészek**

folyamatos helybeni rendelkezésre állását a következő feltételek figyelembe vétele alapján:
- **az IT környezet számára információ rendelkezésre állása.**

Függések: nincsenek.

FDP_ITC_PKI_INF.1/2 PKI információk importálása a TSF-en kívülről
Hierarchikus alárendeltség más komponensekhez képest: nincs.
FDP_ITC_PKI_INF.1.1 Az **IT környezetnek** biztosítania kell a
- **CRL-ek,**
- **időbélyeg szolgáltatás (kérések és válaszok)**

rendelkezésre állását a [***a TOE funkcióinak teljesítését biztosító időn belül***] mérték szerint a következő feltételek figyelembe vétele alapján:
- **hálózati kapcsolat rendelkezésre állása,**
- **információs szerver rendelkezésre állása,**
- **az alkalmazás protokollban információ rendelkezésre állása (időbélyeg kérés és válasz, CRL lekérdezés).**

Függések: nincsenek.

FDP_RIP.1 Részleges maradvány információ védelem
FDP_RIP.1.1 Az **IT környezet TSF-nek** biztosítania kell, hogy egy erőforrás korábbi információtartalma hozzáférhetetlenné válik az **erőforrás használat utáni közvetlen deallokációja** után az alábbi objektumokra: **magánkulcs, titkosító kulcs**.
Függések: nincsenek.
Alkalmazási megjegyzés:
Ezt a követelményt az InfoSigno v1.0.0 is támogatja, teljesíti.

5.1.2 FIA osztály – Azonosítás és hitelesítés

FIA_AFL.1 Sikertelen hitelesítés kezelése
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FIA_AFL.1.1 Az **IT környezet TSF-nek** észlelnie kell amikor **a magánkulcs tároló eszköz vagy TOE-t hívó alkalmazás által reprezentált folyamat által specifikált számú** sikertelen hitelesítési kísérlet történik a **magánkulcshoz való hozzáférés** eseményekkel kapcsolatban.
FIA_AFL.1.2 Amikor a definiált számú sikertelen hitelesítési kísérlet bekövetkezett, vagy a kísérletek száma meghaladta ezt az értéket, az **IT környezet TSF**-nek a következőket kell tennie: **a magánkulcs tároló eszköz által specifikált esemény (szoftveres magánkulcs tároló eszköz esetén fájl törlése, BALE vagy KHE esetén hitelesítő adat zárolása)**.
Függések: FIA_UAU.1 Hitelesítés időzítése

FIA_ATD.1 Felhasználói tulajdonságok megadása
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FIA_ATD.1.1 Az **IT környezet TSF-nek** kezelnie kell a következő, az egyedi felhasználókhoz tartozó biztonsági tulajdonság listát: *szerepkör*.
Függések: Nincsenek

FIA_UAU.1 Hitelesítés időzítése
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FIA_UAU.1.1 Az **IT környezet TSF-nek** lehetővé kell tennie a felhasználó nevében végrehajtandó **tevékenységeket: a TOE-t hívó alkalmazás által megadható paraméterek továbbítását (alkalmazható magánkulcs tároló eszköz paraméterei)**, valamint a felhasználó azonosítását, mielőtt a felhasználó hitelesítésre kerül.
FIA_UAU.1.2 Az **IT környezet TSF** megköveteli, hogy minden felhasználó sikeresen hitelesítve legyen, mielőtt bármilyen más, az **IT környezet TSF** által közvetített tevékenység történne a kérdéses felhasználó nevében.
Függések: FIA_UID.1 Azonosítás időzítése

FIA_UAU.7 Védett hitelesítés visszacsatolás
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FIA_UAU.7.1 Az **IT környezet TSF-nek** csak **fedőkaraktert (például * vagy ●)** szolgáltat a felhasználónak a hitelesítési folyamat végrehajtása közben.
Függések: FIA_UAU.1 Hitelesítés időzítése

FIA_UID.1 Azonosítás időzítése
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FIA_UID.1.1 Az **IT környezet TSF-nek** lehetővé kell tennie a felhasználó nevében végrehajtandó **tevékenységeket: a TOE-t hívó alkalmazás által megadható paraméterek továbbítását (alkalmazható magánkulcs tároló eszköz paraméterei)**, mielőtt a felhasználó azonosításra kerül.
FIA_UID.1.2 Az **IT környezet TSF-je** megköveteli, hogy minden felhasználó sikeresen azonosítva legyen, mielőtt bármilyen más TSF által közvetített tevékenység történne a kérdéses felhasználó nevében.
Függések: nincsenek.

5.1.3 FMT osztály – Biztonsági menedzsment

FMT_MSA.1 Biztonsági tulajdonságok menedzsmentje

Hierarchikus alárendeltség más komponensekhez képest: nincs.

FMT_MSA.1.1 Az **IT környezet TSF-nek** érvényt kell szereznie a **PKI engedélyezés kezelési SFP-nek azon** képesség ellenőrzése céljából, hogy **a TOE-t hívó alkalmazás által reprezentált folyamatra** korlátozza

- **a nyilvános kulcs tanúsítvány és a magánkulcs közötti kapcsolat,**
- **a TOE-t hívó alkalmazás által reprezentált folyamatot azonosító adatok,**
- **a TOE biztonsági funkciói működését befolyásoló paraméterek**

biztonsági tulajdonságok **lekérdezésének**, **módosításának**, **törlésének** képességét.
Függések: FMT_SMF.1 Menedzsment funkciók megadása
FMT_SMR.1 Biztonsági szerepkörök – FMT_SMR.2 Korlátozott biztonsági szerepkörök
FDP_ACC Részleges hozzáférés ellenőrzés

FMT_MSA.3 Statikus tulajdonságok kezdeti értékadása
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FMT_MSA.3.1 Az **IT környezet TSF-nek** érvényt kell szereznie **a PKI engedélykezelési SFP**-nek **specifikus** alapértékek biztosítása céljából, az SFP-t érvényre juttató biztonsági tulajdonságokra.
FMT_MSA.3.2 Az **IT környezet TSF-nek** lehetővé kell tennie a **TOE-t hívó alkalmazás által reprezentált folyamat** számára, hogy alternatív kezdeti értékeket adhasson meg az alapértelmezett értékek helyett egy objektum vagy információ létrehozásakor.

Függések: FMT_SMR.1 Biztonsági szerepkörök – FMT_SMR.2 Korlátozott biztonsági szerepkörök
FMT_MSA.1 Biztonsági tulajdonságok kezelése

FMT_MTD.1/1 TSF adatok kezelése
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FMT_MTD.1.1 Az **IT környezet TSF-nek** korlátoznia kell a
- **megbízható pontok,**
- **közbenső tanúsítványok,**
- **végtanúsítványok,**
- **CRL-ek,**
- **CRL használat konfigurációs paraméterei,**
- **időbélyeg használat paraméterei,**
- **megbízható időszerverek címei**

módosítását, törlését, tartalom törlését, hozzáadását a TOE-t hívó alkalmazás által reprezentált folyamatra és az alapul szolgáló operációs rendszerre.
Függések: FMT_SMF.1 Menedzsment funkciók megadása
FMT_SMR.1 Biztonsági szerepkörök - – FMT_SMR.2 Korlátozott biztonsági szerepkörök

FMT_SMF.1/1 Menedzsment funkciók megadása
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FMT_SMF.1.1/1 Az **IT környezet TSF-nek** képesnek kell lennie a következő biztonsági menedzsment funkciók végrehajtására:
- **megbízható pontok karbantartása;**
- **közbenső tanúsítványok karbantartása;**
- **végtanúsítványok karbantartása;**
- **a TOE-t hívó alkalmazás által beállítható paraméterek TOE felé való megbízható továbbítása; (CRL aktualitás elfogadását befolyásoló paraméterek állítása, időbélyeg kérés idejének konfigurálása, időbélyeg szolgáltató címe)**
- **a TOE kód sértetlenségét biztosító külső alkalmazás ellenőrző funkciójának aktivizálása.**

Függések: nincsenek.

FMT_SMR.2 Megszorítások a biztonsági szerepkörökre
Hierarchikus alárendeltség: FMT_SMR.1 komponensnek alárendelt.
FMT_SMR.2.1 Az **IT környezet TSF-nek** kezelnie kell **a TOE-t hívó alkalmazás által reprezentált folyamat** szerepkört.
FMT_SMR.2.2 Az **IT környezet TSF-nek** össze kell kapcsolnia a felhasználókat a szerepkörökkel.
FMT_SMR.2.3 Az **IT környezet TSF-nek** biztosítania kell, hogy a **TOE-t hívó alkalmazás által reprezentált folyamat jogosult TOE hozzáférése** biztosított legyen.
Függések: FIA_UID.1 Azonosítás időzítése

FMT_SMF.1/2– Menedzsment funkciók meghatározása
Hierarchikus alárendeltség más komponensekhez képest: nincs.
FMT_SMF.1.1 A **TOE TSF-nek** vagy az **IT környezet TSF-nek** képesnek kell lennie az alábbi biztonsági menedzsment funkciók végrehajtására:

- **az aláíró hitelesítő adat cseréje PKCS#12 kulcstároló fájl esetén.**

FMT_MTD.1/2 A TSF adatok kezelése
Hierarchikus alárendeltség más komponensekhez képest: nincs.
FMT_MTD.1.1 A **TOE TSF-nek** vagy az **IT környezet TSF-nek** az **aláíróra** kell korlátoznia a **PKCS#12-es kulcstároló eszközben tárolt magánkulcshoz való hozzáférést biztosító aláírói hitelesítő adat (PIN kód) módosításának** képességét.

Alkalmazási megjegyzés:
Az FMT_SMF.1/2 és FMT_MTD.1/2 követelményeket az általános biztonsági követelményeket tartalmazó csomag egyéb követelményeinek többségétől eltérően az InfoSigno teljesíti.

5.1.4 FCS osztály – Kriptográfiai támogatás

FCS_CRM_FPS.1 Kriptográfiai modulok
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FCS_CRM_FPS.1.1 Az **IT környezetnek** biztosítania kell minden, a TSF működéséhez szükséges kriptográfiai modult.
FCS_CRM_FPS.1.2 **Minősített elektronikus aláírás létrehozása esetén** a kriptográfiai modulnak **NHH által nyilvántartásba vett, tanúsított biztonságos aláírás létrehozó eszköznek (BALE)** kell lennie.

Függések: nincsenek.

5.1.6 FPT osztály – A TOE biztonsági funkciók védelme

FPT_STM.1 Megbízható időbélyegek
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FPT_STM.1.1 Az **IT környezet TSF-nek** a TSF használathoz megbízható időbélyeget kell biztosítania.
Függések: nincsenek.

FPT_RVM.1 A TSP megkerülhetetlensége
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FPT_RVM.1.1 Az **IT környezet TSF-nek** biztosítania kell, hogy a TSP-t érvényre juttató funkciók valóban meghívódnak, és befejeződnek, mielőtt a TSF hatáskörén belülre eső egyes funkciók futása lehetővé válik.
Függések: nincsenek.

FPT_SEP.1 TSF tartomány szétválasztás
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FPT_SEP.1.1 Az **IT környezet TSF-nek** biztonsági tartományt kell kezelnie a saját futásához, ami megvédi a nem megbízható egyedek általi beavatkozástól és hamisítástól.
FPT_SEP.1.2 A TSF-nek érvényre kell juttatnia a szétválasztást a szubjektumok biztonsági tartománya között a TSC-ben.
Függések: nincsenek.

5.1.7 Funkcióerősségre vonatkozó követelmény

A funkcionális biztonsági követelményekre vonatkozó minimális funkcióerősségi szint: SOF-alap, de az InfoSigno v1.0.0 hatáskörén belül nincsenek valószínűségi vagy permutációs mechanizmusok.

5.2. Az InfoSigno v1.0.0 által teljesítendő, az egyes csomagokra vonatkozó funkcionális biztonsági követelmények

Az alábbi alfejezetek a TOE által teljesítendő, az egyes csomagokra vonatkozó funkcionális követelményeket írják le.

5.3 táblázat – A csomagokban szereplő funkcionális biztonsági követelmények összegzése

Csomag neve	**Funkcionális követelmény**	**Függések**
Tanúsítási útvonal érvényesség ellenőrzése – Alap	FDP_CPD.1	Nincs
	FDP_DAU_CPV_CER.1	
	FDP_DAU_CPV_CER.2	
	FDP_DAU_CPV_CER.3	
	FDP_DAU_CPV_OUT.1	
PKI aláírás létrehozás	FDP_ETC_SIG.1	Nincs
PKI aláírás ellenőrzés	FDP_ITC_SIG.1	Tanúsítási útvonal érvényesség ellenőrzése – Alap
	FDP_DAU_SIG.1	
PKI titkosítás kulcs átviteli algoritmusokkal	FDP_ETC_ENC.1	Tanúsítási útvonal érvényesség ellenőrzése – Alap
	FDP_DAU_ENC.1	
PKI megoldás kulcs átviteli algoritmusokkal	FDP_ITC_ENC.1	Nincs
Tanúsítvány visszavonási lista érvényesség ellenőrzése	FDP_DAU_CRL.1	Nincs
Kiegészítő csomag		
Időbélyeg kérése és ellenőrzése	FDP_DAU_TS.1	Tanúsítási útvonal érvényesség ellenőrzése (CPV) – Alap

5.2.1 „Tanúsítási útvonal érvényesség ellenőrzése – Alap" csomag

5.2.1.1 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 ***az ellenőrző félt reprezentáló folyamat*** által biztosított megbízható pontig, a következő tanúsítvány mezők vagy kiterjesztésekre vonatkozó illesztési szabályok felhasználásával:

a) a tanúsítvány kibocsátó (issuer mezője) megegyezik a tanúsítvány aláírásához használt (szülő) tanúsítvány alanya 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-ban specifikált szabályok;

b) a tanúsítványláncban önkibocsátott tanúsítvány nem fordul elő.

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

a) A kibocsátó-tulajdonos névegyezőség bináris ellenőrzésének végrehajtása;

b) a pathLenConstraint megszorítás valóban teljesül.

FDP_CPD.1.4 A TSF-nek a tanúsítási útvonal felépítéséhez a következő megbízható forrásból: **IT környezetből** kell megszereznie az „***aktuális időt***".

Függések: nincsenek.

FDP_DAU_CPV_CER.1 Tanúsítvány feldolgozás -- végtanúsítványok

Hierarchia szerint alárendelt-e más komponensnek: nem.

FDP_DAU_CPV_CER.1.1 A TSF-nek csak akkor szabad elfogadnia egy tanúsítványt, ha sikeresen teljesülnek az alábbi ellenőrzések:

a) a notBefore mező a tanúsítványon <= aktuális idő;

b) a notAfter mező a tanúsítványon >= aktuális idő;

c) a TSF képes minden kritikusnak jelölt kiterjesztést feldolgozni;

d) a tanúsítvány kibocsátó mezője = szülő DN-je (megkülönböztető neve);

e) szülő nyilvános kulcs tanúsítvány felhasználásával ellenőrzi a tanúsítványon lévő aláírást;

f) keyUsage kiterjesztésben a nonRepudiation bit be van kapcsolva (aláírás ellenőrzése esetén);

g) keyUsage kiterjesztésben a keyEncipherment bit be van kapcsolva (kulcs átviteli algoritmust használó titkosításhoz szükséges tanúsítvány érvényesítése esetén);

FDP_DAU_CPV_CER.1.2 A TSF-nek csak akkor szabad elfogadnia egy tanúsítványt, ha a használt ***CRL (visszavonási lista információi)*** alapján megállapítja, hogy a tanúsítvány nem visszavont.

FDP_DAU_CPV_CER.1.3 A TSF a nyilvános kulcs paramétereket az alábbi szabályok alapján kezeli:

a) A nyilvános kulcs paramétereket a tanúsítvány subjectPublickeyInfo mezőjéből nyeri ki;

b) algoritmus paraméterként az RSA–SHA1-et használja.

Függések:
FCS_COP.1 Kriptográfiai műveletek
FPT_STM.1 Megbízható időbélyegek

FDP_DAU_CPV_CER.2 Tanúsítvány feldolgozás – Közbenső tanúsítványok
Hierarchia szerint alárendelt-e más komponensnek: nem.

FDP_DAU_CPV_CER.2.1 A TSF-nek csak akkor szabad egy közbenső tanúsítványt elfogadnia, ha az alábbi további ellenőrzések is sikeresek:

a) a notBefore mező a tanúsítványon <= aktuális idő;
b) a notAfter mező a tanúsítványon >= aktuális idő;
c) a TSF képes minden kritikusnak jelölt kiterjesztést feldolgozni;
d) a tanúsítvány kibocsátó mezője = szülő DN-je (megkülönböztető neve);
e) szülő nyilvános kulcs tanúsítvány felhasználásával ellenőrzi a tanúsítványon lévő aláírást;
f) a `basicConstraints` *mező jelen van a CA=TRUE értékkel;*
g) a `keyUsage` *kiterjesztésben a* `keyCertSign` *bit be van kapcsolva.*

FDP_DAU_CPV_CER.2.2 A TSF a nyilvános kulcs paramétereket az alábbi szabályok alapján kezeli:
a) A nyilvános kulcs paramétereket a tanúsítvány subjectPublickeyInfo mezőjéből nyeri ki;
b) algoritmus paraméterként az RSA–SHA1-et használja.
Függések:
FCS_COP.1 Kriptográfiai műveletek
FPT_STM.1 Megbízható időbélyegek

FDP_DAU_CPV_CER.3 Tanúsítvány feldolgozás – Megbízható pontok
Hierarchia szerint alárendelt-e más komponensnek: nem.

FDP_DAU_CPV_CER.3.1 A TSF-nek csak akkor szabad egy közbenső tanúsítványt elfogadnia, ha az alábbi további ellenőrzések is sikeresek:
a) a notBefore mező a tanúsítványon <= aktuális idő;
b) a notAfter mező a tanúsítványon >= aktuális idő;
c) a TSF képes minden kritikusnak jelölt kiterjesztést feldolgozni;
d) a tanúsítvány kibocsátó mezője = a tanúsítvány DN-je (megkülönböztető neve);
e) a tanúsítványban lévő nyilvános kulcs felhasználásával ellenőrzi a tanúsítványon lévő önaláírást;
f) a `basicConstraints` *mező jelen van a CA=TRUE értékkel.*

FDP_DAU_CPV_CER.3.2 A TSF a nyilvános kulcs paramétereket az alábbi szabályok alapján kezeli:
a) A nyilvános kulcs paramétereket a tanúsítvány subjectPublickeyInfo mezőjéből nyeri ki;
b) algoritmus paraméterként az RSA–SHA1-et használja.

Függések:

FCS_COP.1 Kriptográfiai műveletek
FPT_STM.1 Megbízható időbélyegek

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) kritikus `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.

5.2.2 PKI aláírás létrehozás csomag

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

5.2.2.1 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,***
- ***aláírási szabályzat azonosító.***

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.**

Alkalmazási megjegyzések:

1. Az InfoSigno v1.0.0 által előállított aláírás formátum XAdES-C.

2. Az aláírói hitelesítő adat felhasználó általi megadását a TOE fölé épülő IT környezethez tartozó alkalmazás vezérli, a TOE paraméterként kapja azt, vagy képes egy bekérő függvény meghívására.

Függések:

FCS_COP.1 Kriptográfiai műveletek

5.2.3 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 érvényességének ellenőrzés – alap” csomagtól függ. Az aláírás ellenőrzési csomag a „Tanúsítási útvonal érvényességének ellenőrzés” csomagot használja fel bemenetként.

5.2.3.1 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,***
- ***aláírási szabályzat azonosító.***

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 érvényességének ellenőrzése** 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 ellenőriznie kell, hogy a **Tanúsítási útvonal érvényességének ellenőrzése** csomagból kapott **`keyUsage`** kiterjesztés kimenetben a **`nonRepudiation`** bit be van-e kapcsolva.

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

a) ***minősített elektronikus aláírás esetén a `keyUsage` kiterjesztésben csak a `nonRepudiation` bit van beállítva;***
b) ***minősített elektronikus aláírás esetén az aláíró tanúsítványában a kötelező qcStatements kiterjesztés meglétének ellenőrzése szükséges;***
c) ***fokozott biztonsági aláírás esetén a `keyUsage` kiterjesztésben a `nonRepudiation` bit mellett csak a digSig bit lehet opcionálisan beállítva;***
d) ***az alany DN-je a tanúsítási útvonal ellenőrzéséből megegyezik-e az aláírt adatban lévővel.***

Függések:
FCS_COP.1 Kriptográfiai műveletek
FDP_DAU_CPV_OUT.1 Tanúsítási útvonal kimenet – alapelemek

5.2.4 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 – Alap** csomagtól függ.

5.2.4.1 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 ellenőrzésé**”-ből a rejtjeles adatok létrehozásához:

- ***alany nyilvános kulcs algoritmusa,***
- ***alany nyilvános kulcsa,***
- ***alany nyilvános kulcs paraméterek.***

Függések:
FCS_COP.1 Kriptográfiai műveletek
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 ellenőriznie kell, hogy a „**Tanúsítási útvonal érvényesség ellenőrzés**” **`keyUsage`** kimenetében a **`keyEncipherment`** bit be van-e állítva.

FDP_DAU_ENC.1.2 A TSF-nek a következő egyéb ellenőrzéseket kell végrehajtania:
a) Össze kell hasonlítania a „Tanúsítási útvonal érvényesség ellenőrzés” 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.

5.2.5 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.

5.2.5.1 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

5.2.6 Tanúsítvány visszavonási lista (CRL) érvényesség ellenőrzés csomag

Ez a csomag a CRL érvényességének ellenőrzésére használt követelményeket fogalmazza meg. A TOE-vel szemben nem követelmény a CRL kibocsátó szétosztó pont (IDP) vagy különbség (delta) CRL feldolgozása. A csomag olyan CRL feldolgozására használható, amelyre egy CRL szétosztó pont (CRLDP) kiterjesztés mutat a tanúsítványban, és a CRL teljes (melyet az IDP és deltaCRLIndicator kiterjesztések hiánya jelez).

Ez a csomag megengedi ugyanazon nyilvános kulcs használatát a CRL aláírás ellenőrzésre és a tanúsítványon lévő aláírás ellenőrzésére, de nem teszi ezt kötelezővé. Más szóval, egy, a csomag követelményeinek megfelelő alkalmazás választhatja ezt a nyilvános kulcsot, de fel is építheti a tanúsítási útvonalat.

5.2.6.1 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 pont nyilvános kulcsát, algoritmusát és nyilvános kulcs paramétereit***.
FDP_DAU_CRL.1.3 A TSF-nek ellenőriznie kell a CRL-en az aláírást a CRL kibocsátója ***megbízható pontjában található nyilvános kulcs, algoritmus és a nyilvános kulcs paraméterek*** ismeretében.
FDP_DAU_CRL.1.4 A TSF-nek ellenőriznie kell a **`keyUsage`** kiterjesztés meglétét a CRL kibocsátó tanúsítványban, illetve, hogy a kiterjesztés **`cRLSign`** bitje be van-e állítva.
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 nem szabad elfogadnia a CRL-t, ha a CRL olyan „kritikus” kiterjesztéseket tartalmaz, melyeket a TSF nem tud feldolgozni.
FDP_DAU_TS.1.7 A TSF-nek ellenőriznie kell, hogy a CRL megfelel-e az alábbi mértékadó útmutatóban definiált szabályoknak:
- ***RFC 3280.***

FDP_DAU_CRL.1.8 A TSF-nek a következő további ellenőrzéseket kell elvégeznie:
- ***CRL formátuma X.509 v2.***

Függések: FCS_COP.1 Kriptográfiai műveletek
FPT_STM.1 Megbízható időbélyegek

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

5.2.7 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 függ a „Tanúsítási útvonal érvényességének ellenőrzés – alap” csomagtól.

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.***

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 érvényesítése (CPV) - Alap** csomag felhasználásával.

FDP_DAU_TS.1.8 A TSF-nek a **Tanúsítási útvonal érvényességének ellenőrzése** csomagból az alábbi információkat kell használnia az időbélyeg válasz aláírásának ellenőrzéséhez: ***aláíró nyilvános kulcsa.***

FDP_DAU_TS.1.9 A TSF-nek ellenőriznie kell, hogy az időbélyeg válasz aláírásához használt tanúsítvány tartalmaz-e kritikus **`extendedKeyUsage`** kiterjesztést, és annak értéke **`id-kp-timeStamping-e`.**

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,*

b) ha a kérés tartalmazott TSAPolicyId-t, akkor az azonos-e a válaszban kapott TSAPolicyId 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

5.3 MIBÉTS kiemelt garanciaszint

Jelen biztonsági előirányzat (összhangban a minősített aláírásokra vonatkozó igen szigorú elvárásokkal) a MIBÉTS kiemelt garanciaszintet követeli meg. Valamennyi garanciaösszetevő a CC 3. részéből származik, s az 5.4 táblázat sorolja fel ezeket.

5.4 táblázat - A MIBÉTS kiemelt garanciaszint követelményei

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(ezés) 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

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

5.3.1 Konfiguráció menedzselés (ACM, Assurance: Configuration Management)

ACM_AUT.1: Részleges konfiguráció menedzselés automatizálás

Fejlesztői feladatok:

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

A bizonyíték elemek tartalma és bemutatása:

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

Értékelői feladatelemek:

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

ACM_CAP.4: A generálás támogatása és elfogadási eljárások

Fejlesztői feladatok:

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

A bizonyíték elemek tartalma és bemutatása:

- ACM_CAP.4.1C Az értékelés tárgya hivatkozásnak egyedi módon kell azonosítania az értékelés tárgya verzióit.
- ACM_CAP.4.2C Az értékelés tárgyát meg kell jelölni ezzel a hivatkozással.
- ACM_CAP.4.3C A konfiguráció menedzselés dokumentációnak tartalmaznia kell egy konfiguráció listát, egy konfiguráció menedzselés tervet és egy elfogadási tervet.
- ACM_CAP.4.4C A konfiguráció listának le kell írnia az értékelés tárgyát alkotó konfiguráció elemeket.
- ACM_CAP.4.5C A konfiguráció menedzselés dokumentációnak le kell írnia a konfiguráció elemek egyedi azonosításához használt módszert.
- ACM_CAP.4.6C A konfiguráció menedzselés rendszernek egyedi módon kell azonosítania minden konfiguráció elemet.
- ACM_CAP.4.7C A konfiguráció menedzselés tervnek le kell írnia a konfiguráció menedzselés rendszer használatát.
- ACM_CAP.4.8C A bizonyítékoknak meg kell mutatniuk, hogy a konfiguráció menedzselés rendszer a konfiguráció menedzselés tervnek megfelelően működik.
- ACM_CAP.4.9C A konfiguráció menedzselés dokumentációnak bizonyítékot kell adnia arra, hogy minden konfiguráció elemet megfelelően kezeltek és kezelnek a konfiguráció menedzselés rendszer alapján.
- ACM_CAP.4.10C A konfiguráció menedzselés rendszernek gondoskodnia kell arról, hogy csak jogosult változtatások történhessenek a konfiguráció elemekben.

- ACM_CAP.4.11C A konfiguráció menedzselés rendszernek támogatnia kell az értékelés tárgya generálását.
- ACM_CAP.4.12C Az elfogadási tervnek le kell írni az értékelés tárgya részét képező konfiguráció elemek módosítására vagy újra létrehozására vonatkozó elfogadási eljárásokat.

Értékelői feladatelemek:

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

ACM_SCP.2: A biztonsági hibákat követő konfiguráció menedzselés

Fejlesztői feladatok:

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

A bizonyíték elemek tartalma és bemutatása:

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

Értékelői feladatelemek:

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

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

ADO_DEL.2: A módosítás kimutatása

Fejlesztői feladatok:

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

A bizonyítékelemek tartalma és megjelenésmódja:

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

Értékelői tevékenységelemek:

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

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

Fejlesztői feladatok:

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

A bizonyítékelemek tartalma és megjelenésmódja:

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

Értékelői tevékenységelemek:

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

ADO_IGS.1.2E Az értékelőnek meg kell állapítania a hardver és szoftver telepítés, valamint az indítás eljárásairól, hogy azok biztonságos konfigurációt eredményeznek-e.

5.3.3 Fejlesztés (ADV, Assurance: Development)

ADV_FSP.2: Teljesen meghatározott külső interfészek

Fejlesztői feladatok:

ADV_FSP.2.1D A fejlesztőnek funkcionális specifikációt kell átadnia.

A bizonyíték elemek tartalma és bemutatása:

ADV_FSP.2.1C A funkcionális specifikációnak informális stílusban le kell írnia a TSF-t (az értékelés tárgya biztonsági funkcióit) és annak külső interfészeit.

ADV_FSP.2.2C A funkcionális specifikációnak belsőleg konzisztensnek (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-t.

ADV_FSP.2.5C A funkcionális specifikációnak egy indoklást kell adnia arra, hogy teljes mértékben reprezentálja a TSF-et.

Értékelői feladatelemek:

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

ADV_FSP.1.2E Az értékelőnek meg kell állapítania, hogy a funkcionális specifikáció a TOE funkcionális biztonsági követelményeinek pontos és teljes megvalósulása-e.

ADV_HLD.2: Biztonságot érvényre juttató magas szintű tervezés

Fejlesztői feladatok:

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

A bizonyíték elemek tartalma és bemutatása:

ADV_HLD.2.1C A magas szintű terv bemutatásának informálisnak kell lennie.

ADV_HLD.2.2C A magas szintű tervnek belsőleg konzisztensnek kell lennie.

ADV_HLD.2.3C A magas szintű tervnek le kell írnia a TSF struktúráját alrendszerek szerint.

ADV_HLD.2.4C A magas szintű tervnek le kell írnia minden egyes TSF alrendszer által nyújtott biztonsági funkcionalitást.

ADV_HLD.2.5C A magas szintű tervnek azonosítania kell a TSF által megkövetelt minden alapul szolgáló hardvert, förmvert és/vagy szoftvert, az ezekkel megvalósított kiegészítő védelmi mechanizmus által biztosított funkciók bemutatásával.

ADV_HLD.2.6C A magas szintű tervnek azonosítania kell minden TSF alrendszer interfészt.

ADV_HLD.2.7C A magas szintű tervnek azonosítania kell, hogy a TSF alrendszerek interfészei közül melyek láthatók kívülről.

ADV_HLD.2.8C A magas szintű tervnek le kell írnia minden TSF alrendszer interfész használatának célját és módját, azok hatásával, kivételekkel és hibaüzenetekkel, amennyiben ez utóbbiak lényegesek.

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

Értékelői feladatelemek:

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

ADV_HLD.2.2E Az értékelőnek meg kell állapítania, hogy a magas szintű terv pontos és teljes megjelenítése a TOE funkcionális biztonsági követelményeinek.

ADV_IMP.1: A biztonsági funkciók részleges kivitelezési dokumentálása

Fejlesztői feladatok:

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

A bizonyíték elemek tartalma és bemutatása:

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

ADV_IMP.1.2C A megvalósítási reprezentációnak belsőleg konzisztensnek kell lennie.

Értékelői feladatelemek:

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

ADV_IMP.1.2E Az értékelőnek meg kell állapítania, hogy a rendelkezésére bocsátott legkevésbé absztrakt TSF reprezentáció pontos és teljes megjelenítése-e a TOE funkcionális biztonsági követelményeinek.

ADV_LLD.1: Leíró alacsony szintű terv

Fejlesztői feladatok:

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

A bizonyíték elemek tartalma és bemutatása:

ADV_LLD.1.1C Az alacsony szintű terv bemutatásának informálisnak kell lennie.

ADV_LLD.1.2C Az alacsony szintű tervnek belsőleg konzisztensnek kell lennie.

ADV_LLD.1.3C Az alacsony szintű tervnek le kell írnia a TSF struktúráját modulok szerint.

ADV_LLD.1.4C Az alacsony szintű tervnek le kell írnia minden modul célját.

ADV_LLD.1.5C Az alacsony szintű tervnek meg kell határoznia a modulok közötti belső kapcsolatokat a biztosított biztonsági funkcionalitás és a más moduloktól való függés szempontjából.

ADV_LLD.1.6C Az alacsony szintű tervnek le kell írnia, hogy a TSP-t érvényre juttató összes funkciót hogyan biztosítják.

ADV_LLD.1.7C Az alacsony szintű tervnek azonosítania kell a TSF moduljaihoz csatlakozó valamennyi interfészt.

ADV_LLD.1.8C Az alacsony szintű tervnek azonosítania kell, hogy a TSF moduljaihoz csatlakozó mely interfészek láthatók kívülről is.

ADV_LLD.1.9C Az alacsony szintű tervnek le kell írnia minden TSF modulhoz kapcsolódó interfész használatának célját és módját, azok hatásával, kivételekkel, illetve hibaüzenetekkel.

ADV_LLD.1.10C Az alacsony szintű tervnek le kell írnia a TOE felosztását TSP-t érvényre juttató és egyéb modulokra.

Értékelői feladatelemek:

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

ADV_LLD.1.2E Az értékelőnek meg kell állapítania, hogy az alacsony szintű terv pontos és teljes megjelenítése a TOE funkcionális biztonsági követelményeinek.

ADV_RCR.1: A kölcsönös megfelelés informális szemléltetése

Fejlesztői feladatok:

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

A bizonyíték elemek tartalma és bemutatása:

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

Értékelői feladatelemek:

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

5.3.4 Útmutató dokumentumok (AGD, Assurance: Guidance Documents)

AGD_ADM.1: Adminisztrátori útmutató

Fejlesztői feladatok:

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

A bizonyíték elemek tartalma és bemutatása:

AGD_ADM.1.1C Az adminisztrátori útmutatónak le kell írnia a TOE adminisztrátora rendelkezésére álló adminisztrátori funkciókat és interfészeket.

AGD_ADM.1.2C Az adminisztrátori útmutatónak le kell írnia, hogy hogyan kell a TOE-t biztonságos módon adminisztrálni.

AGD_ADM.1.3C Az adminisztrátori útmutatónak tartalmaznia kell azon funkciókkal és jogosultságokkal kapcsolatos figyelmeztetéseket, melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

AGD_ADM.1.4C Az adminisztrátori útmutatónak le kell írnia a felhasználói viselkedéssel kapcsolatos minden feltételezést, mely a TOE biztonságos üzemelése szempontjából lényeges.

AGD_ADM.1.5C Az adminisztrátori útmutatónak le kell írnia minden biztonsági szempontból fontos paramétert, mely az adminisztrátor ellenőrzése alá tartozik, jelezve (ahol ez lehetséges) a biztonságos értékeket.

AGD_ADM.1.6C Az adminisztrátori útmutatónak le kell írnia minden adminisztratív funkcióval kapcsolatban végrehajtandó, biztonsági szempontból fontos esemény típusát, ideértve a TSF ellenőrzése alá eső egyedek biztonsági tulajdonságait.

AGD_ADM.1.7C Az adminisztrátori útmutatónak konzisztensnek kell lennie minden más, értékeléshez beadott dokumentációval.

AGD_ADM.1.8C Az adminisztrátori útmutatónak le kell írnia minden olyan, az informatikai környezetre vonatkozó biztonsági követelményt, mely az adminisztrátor számára fontos.

Értékelői feladatelemek:

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

AGD_USR.1: Felhasználói útmutató

Fejlesztői feladatok:

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

A bizonyíték elemek tartalma és bemutatása:

AGD_USR.1.1C A felhasználói útmutatónak le kell írnia a TOE nem adminisztrátor felhasználói rendelkezésére álló funkciókat és interfészeket.

AGD_USR.1.2C A felhasználói útmutatónak le kell írnia, hogy a TOE által a felhasználók számára hozzáférhető biztonsági funkciókat hogyan kell biztonságosan használni.

AGD_USR.1.3C A felhasználói útmutatónak tartalmaznia kell azon felhasználók által hozzáférhető funkciókkal és jogosultságokkal kapcsolatos figyelmeztetéseket, melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

AGD_USR.1.4C A felhasználói útmutatónak egyértelműen be kell mutatnia minden felhasználói feladatot, mely a TOE biztonságos üzemeltetéséhez szükséges, ideértve azokat, melyek a TOE biztonsági környezetére vonatkozó leírásban található feltételezésekhez kapcsolódnak és a felhasználói viselkedést írják le.

AGD_USR.1.5C A felhasználói útmutatónak konzisztensnek kell lennie minden más, értékeléshez beadott dokumentációval.

AGD_USR.1.6C A felhasználói útmutatónak le kell írnia minden olyan, az informatikai környezetre vonatkozó biztonsági követelményt, mely a felhasználó számára fontos.

Értékelői feladatelemek:

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

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

ALC_DVS.1: A biztonsági intézkedések azonosítása

Fejlesztői feladatok:

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

A bizonyíték elemek tartalma és bemutatása:

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

ALC_DVS.1.2C A fejlesztési biztonságról szóló dokumentációnak bizonyítékot kell szolgáltatnia arról, hogy ezeket az intézkedéseket betartják a TOE fejlesztése és támogatása során.

Értékelői feladatelemek:

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

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

ALC_LCD.1: A fejlesztő által meghatározott életciklus modell

Fejlesztői feladatok:

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

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

A bizonyíték elemek tartalma és bemutatása:

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

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

Értékelői feladatelemek:

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

ALC_TAT.1:Jól meghatározott fejlesztő eszközök

Fejlesztői feladatok:

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

ALC_TAT.1.2D A fejlesztőnek dokumentálnia kell a fejlesztő eszközök kiválasztott megvalósítás-függő opcióit.

A bizonyíték elemek tartalma és bemutatása:

ALC_TAT.1.1C A megvalósításhoz használt fejlesztő eszközöknek jól meghatározottaknak kell lenniük.

ALC_TAT.1.2C A fejlesztő eszközök dokumentációjának egyértelműen meg kell határoznia az implementáció során használt valamennyi utasítás jelentését.

ALC_TAT.1.3C A fejlesztő eszközök dokumentációjának egyértelműen meg kell határoznia valamennyi megvalósítás-függő opció jelentését.

Értékelői feladatelemek:

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

5.3.6 Tesztek (ATE, Assurance: Tests)

ATE_COV.2: A teszt lefedettség elemzése

Fejlesztői feladatok:

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

A bizonyíték elemek tartalma és bemutatása:

ATE_COV.2.1C A teszt lefedettség elemzése mutassa be a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikációban leírt TOE biztonsági funkciók közötti megfeleltetést.

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

Értékelői feladatelemek:

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

ATE_DPT.1: A magas szintű terv tesztelése

Fejlesztői feladatok:

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

A bizonyítékok tartalma és bemutatása:

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

Értékelői feladatelemek:

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

ATE_FUN.1: Funkcionális tesztelés

Fejlesztői feladatok:

ATE_FUN.1.1D A fejlesztőnek le kell tesztelnie a TOE biztonsági funkcióit, és dokumentálnia kell az eredményeket.

ATE_FUN.1.2D A fejlesztőnek el kell készítenie, és át kell adnia a tesztelési dokumentációt.

A bizonyítékok tartalma és bemutatása:

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

ATE_FUN.1.2C A tesztelési terveknek azonosítaniuk kell a tesztelendő biztonsági funkciókat, és le kell írniuk a végrehajtandó tesztek célját.

ATE_FUN.1.3C A teszt eljárások leírásának azonosítania kell a végrehajtandó teszteket, és le kell írnia a tesztelési forgatókönyvet minden biztonsági funkcióra. A forgatókönyveknek tartalmazniuk kell minden, a tesztek sorrendiségére vonatkozó függőséget.

ATE_FUN.1.4C A várt teszteredményeknek meg kell mutatniuk a tesztek sikeres végrehajtásából keletkező várható kimenteket.

ATE_FUN.1.5C A fejlesztő által elvégzett tesztelés eredményeinek be kell mutatniuk, hogy minden tesztelt biztonsági funkció a specifikált módon működött.

Értékelői feladatelemek:

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

ATE_IND.2: Független tesztelés - mintavételezés

Fejlesztői feladatok:

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

A bizonyítékok tartalma és bemutatása:

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

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

Értékelői feladatelemek:

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

ATE_IND.2.2E Az értékelőnek tesztelnie kell a TSF megfelelő részeit annak megállapításához, hogy a TOE a specifikáltnak megfelelően működik-e.

ATE_IND.2.3E Az értékelőnek végre kell hajtania a tesztelési dokumentációban szereplő tesztek valamely részhalmazát (mintáját) a fejlesztői teszt eredmények ellenőrzése érdekében.

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

AVA_MSU.2: A vizsgálatok megerősítése

Fejlesztői feladatok:

AVA_MSU.2.1D A fejlesztőnek el kell készítenie az útmutató dokumentációkat.

AVA_MSU.2.2D A fejlesztőnek egy elemzést kell dokumentálnia az útmutató dokumentációkról.

A bizonyíték elemek tartalma és bemutatása:

AVA_MSU.2.1C Az útmutatónak azonosítani kell a TOE összes lehetséges üzemmódját (beleértve a meghibásodás vagy üzemhiba utáni műveleteket is), és azok biztonságos üzemeltetésre gyakorolt kihatásait és következményeit.

AVA_MSU.2.2C Az útmutatónak teljesnek, egyértelműnek, következetesnek és megalapozottnak kell lennie.

AVA_MSU.2.3C Az útmutatónak fel kell sorolnia minden feltételezést a leendő üzemi környezetről.

AVA_MSU.2.4C Az útmutatónak számba kell vennie a külső biztonsági intézkedésekkel kapcsolatos minden követelményt (beleértve a külső eljárásbeli, fizikai és személyi intézkedéseket is).

AVA_MSU.2.5C A fejlesztői elemzésnek ki kell mutatnia az útmutatók teljességét.

Értékelői feladatelemek:

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

AVA_MSU.2.2E Az értékelőnek meg kell ismételnie minden konfigurációs és telepítési eljárást, annak megállapítása érdekében, hogy a TOE kizárólag az átadott útmutató dokumentáció alapján biztonságosan konfigurálható és használható.

AVA_MSU.2.3E Az értékelőnek meg kell határoznia, hogy az útmutató dokumentáció használatával észrevehető-e minden nem biztonságos állapot.

AVA_MSU.2.4E Az értékelőnek meg kell erősítenie, hogy a fejlesztői elemzés kimutatja, hogy az útmutató a TOE valamennyi működési módjában útmutatást ad a biztonságos működtetésre.

AVA_SOF.1: Az értékelés tárgya biztonsági funkcióinak erősségértékelése

Fejlesztői feladatok:

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

A bizonyíték elemek tartalma és bemutatása:

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

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

Értékelői feladatelemek:

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

AVA_SOF.1.2E Az értékelőnek meg kell győződni arról, hogy az erősségi követelmények helyesek.

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 az InfoSigno v1.0.0 által teljesítendő biztonsági követelményeket teljesítő biztonsági funkciókat tartalmazza. Leírja az InfoSigno összes biztonsági funkcióját és garanciális intézkedését, amelyek az 5. fejezetben specifikált biztonsági követelményeknek a kielégítéséhez járulnak hozzá.

6.1 A TOE biztonsági funkciói

BF1 Aláírás létrehozása

BF2 Digitális aláírás ellenőrzés

BF3 Üzenet digitális aláírása

BF4 Elektronikus aláírás ellenőrzése

BF5 Időbélyeg kérés

BF6 Időbélyeg ellenőrzés

BF7 Tanúsítvány útvonal felépítése és érvényesség ellenőrzése

BF8 Titkosítás, megoldás

BF9 A TSF védelme és menedzsmentje

BF1 Aláírás létrehozása

A **BF1 Aláírás létrehozása** biztonsági funkció hozza létre az aláírói dokumentumra és az aláírási információkra az elektronikus aláírást az aláírói magánkulcs felhasználásával.

Az InfoSigno v1.0.0 lehetőséget biztosít fokozott biztonságú és minősített elektronikus aláírások létrehozására. Fokozott biztonságú aláírások esetén képes fájlban (PKCS#12-es formátumban), Microsoft tanúsítványtárban, vagy kriptográfiai hardver eszközben (KHE) tárolt magánkulcs használatára.
(Fájl formátumban nem csak PKCS#12-es privát kulcs fájlokat, hanem tanúsítványokat és CRL-eket is kezel a rendszer.)
A magánkulcs közvetlen aktivizálása előtt az InfoSigno a paraméterként kapott aláíró hitelesítő adatot (vagy a kapott függvénnyel bekért) hitelesítő adatot használja az aláíró hitelesítéséhez.

Minősített elektronikus aláírás létrehozása esetén az InfoSigno v1.0.0 kommunikációt kezdeményez az aláírás létrehozását ténylegesen végző BALE-vel. Az aláíró által kiválasztott tanúsítványhoz tartozó magánkulccsal és az ennek megfelelő algoritmussal (ami az InfoSigno esetén az RSA algoritmus 1024 bit kulcshosszal) létrehozza az aláírást. A BALE eszköz végzi a magánkulcs aktivizáláshoz szükséges aláíró hitelesítő adat bekérést. Ez esetben az aláírás létrehozásához használt tanúsítványnak minősített tanúsítványnak kell lennie (qCStatement

kiterjesztés használatával - ETSI TS 101 862 v1.3.3), és a keyUsage kiterjesztésben csak a nonRepudiation bit lehet beállítva.

Fokozott biztonságú aláírás létrehozása esetén

- Aktivizálja a PKCS#12-es fájlban tárolt magánkulcsot, és az RSA algoritmus és 1024 bit kulcshossz használatával létrehozza a lenyomatra az aláírást, amit beletesz az XML aláírásba.

Vagy

- Aktivizálja a Microsoft tanúsítványtárában tárolt magánkulcsot, és az RSA algoritmus és 1024 bit kulcshossz használatával létrehozza a lenyomatra az aláírást, amit beletesz az XML aláírásba.

Vagy

- Kezdeményezi a KHE (Kriptográfiai hardver eszköz) felé az aláírás létrehozását, majd a kapott aláírás érték felhasználásával összeállítja az XML aláírást.

Fokozott biztonságú aláírás létrehozása esetén a keyUsage kiterjesztésben a kötelezően beállított nonRepudiation bit mellett opcionálisan a digitalSignature bit lehet még beállítva.

A funkció által létrehozott elektronikus aláírás formátuma megfelel a következőknek: RFC3275, XAdES v1.2.2.

Lenyomat készítés

Az aláírás létrehozás biztonsági funkció ezen alfunkciója hozza létre a lenyomatot, amire az aláírás készül. Az aláírás létrehozása során az aláírandó adatokra alkalmazott lenyomatkészítő algoritmus: SHA-1 [FIPS 180-1].

Megengedett dokumentum formátumok:

Az InfoSigno v1.0.0 a következő dokumentum formátumok aláírását engedi meg: XML, JPEG, TXT, PNG.

Aláírás előtt megvizsgálja a kapott dokumentum kiterjesztését; ha nem a fentiek egyike, de WORD, NOTES vagy HTML formátum, akkor figyelmeztetést ad vissza a hívó félnek, egyébként nem engedi a dokumentum hozzáadását.

Az aláírást az InfoSigno v1.0.0 az alábbi szabályok alapján készíti el:

- Az elektronikus aláírásban csak az **aláíró tanúsítvány azonosítója** szükséges.
- A [`keyinfo`] elemben az **aláíró tanúsítvány**t kell megadni.
- A kötelező aláírási tulajdonságok:
- **Aláírás ideje**
- **Aláírási szabályzat azonosítója**
- **Aláírói tanúsítvány**

BF2 Digitális aláírás ellenőrzés

Az InfoSigno v1.0.0 ezen biztonsági funkciójának képessége biztosítja egy létrehozott digitális aláírás érték ellenőrzését. A funkció kiszámítja az aláírt adat lenyomatát, majd az aláírónak az aláírásba foglalt nyilvános kulcs tanúsítványában található nyilvános kulcs és az aláírási algoritmus felhasználásával ellenőrzi a digitális aláírást. Amennyiben a kiszámított lenyomat és a digitális aláírás ellenőrzése során kapott érték megegyezik, akkor a digitális aláírás érték helyes.

BF3 Üzenet digitális aláírása

Az InfoSigno v1.0.0 ezen biztonsági funkciója az adat sértetlenség követelmény biztosítása érdekében digitális aláírást képes létrehozni felhasználói adatokra. A funkció az SHA-1 algoritmust használja az adat lenyomat elkészítésére, és ezt kódolja az RSA/1024 bites aláíró algoritmussal.

BF4 Elektronikus aláírás ellenőrzése

Ez a biztonsági funkció valósítja meg – a **BF2 Digitális aláírás ellenőrzés** biztonsági funkciónak csak az aláírás érték kriptográfiai érvényesség ellenőrzésével szemben –, az elektronikus aláírás ellenőrzését az aláíró tanúsítványának felhasználásával.
A funkció paraméterezésétől függően kezdeti vagy utólagos ellenőrzést végez.

A kezdeti ellenőrzés folyamata három lépésből áll: első lépésben a funkció megnézi, hogy kapcsolódik-e időbélyeg az aláíráshoz. Amennyiben nem, akkor végrehajtja a **BF5 Időbélyeg kérés** és a **BF6 Időbélyeg ellenőrzés** biztonsági funkciókat. Az ellenőrzés második lépéseként az aláírás érvényességének megállapításához szükséges információk összegyűjtését végzi. Ezt a **BF7 Tanúsítványlánc felépítése és érvényesség ellenőrzése** biztonsági funkció végzi el. Végül a harmadik lépésben kerül sor az elektronikus aláírás ellenőrzésére.

A kezdeti ellenőrzésnek három lehetséges kimeneti állapota lehet:
- befejezetlen;
- sikeres;
- sikertelen.

Sikeres esetben befejeződött az összes érvényesítő adat összegyűjtése, és az aláírás ezek alapján érvényesnek tekinthető.
Sikertelen ellenőrzés olyan esetben történhet, ha például az aláírás formátuma nem megfelelő vagy a digitális aláírás értéke érvénytelen.
Befejezetlen esetben nincs elegendő információ az aláírás érvényességének pozitív megállapításhoz.

Az utólagos ellenőrzés folyamata a már korábban (a kezdeti ellenőrzés során) begyűjtött információk alapján közvetlenül (BF7 aktivizálása nélkül) végrehajtja az elektronikus aláírás ellenőrzését. Csak két lehetséges kimeneti állapota lehet:
- sikeres;
- sikertelen (ez utóbbi azt az esetet is lefedi, amikor nem áll rendelkezésre elegendő információ az aláírás ellenőrzéséhez).

A funkció által ellenőrizni képes elektronikus aláírás formátumok: XML digital signature szabvány, XAdES v1.2.2.

BF5 Időbélyeg kérés

Az InfoSigno v1.0.0 biztosítja az időbélyeg kérés képességét **az aláírás ellenőrzése során**. Az RFC 3161-ben specifikáltaknak megfelelően összeállítja az időbélyeg kérést a hash értékkel, és elküldi a külső időbélyeg szolgáltatóhoz.

BF6 Időbélyeg ellenőrzés

Az InfoSigno v1.0.0 a szolgáltatótól kapott időbélyeg választ importálja, és elvégzi a szükséges ellenőrzéseket: ellenőrzi a válasz státuszt, azt, hogy érvényes-e az időbélyegen lévő aláírás, ellenőrzi az időbélyeg aláírásához használt tanúsítvány érvényességét.

BF7 Tanúsítási útvonal felépítése és érvényesség ellenőrzése

Ez a biztonsági funkció végzi az aláíró tanúsítványból kiindulva a megbízható pontig (gyökértanúsítványig) tartó tanúsítvány lánc elemeinek összegyűjtését.
Az InfoSigno az IT környezet által sértetlenségében megvédett konfigurációs fájlból olvassa be a kulcsadat tárolók elérését, amiket a tanúsítási útvonal érvényesség ellenőrzése során felhasznál. Ezen fájl tartalmának módosítása kívül esik a TOE hatókörén.
A tanúsítási útvonal felépítéséhez az InfoSigno betöltésekor lefut egy ***inicializáló*** rutin, amely elvégzi a használt tanúsítványtárak inicializálást.
Ehhez az alábbi tanúsítványtár funkciókat biztosítja:

- megbízható pont (gyökér tanúsítvány) hozzáadása
- megbízható pontok (gyökér tanúsítványok) listázása
- közbenső tanúsítvány hozzáadása
- közbenső tanúsítványok listázása
- végfelhasználói tanúsítvány hozzáadása
- végfelhasználói tanúsítványok listázása
- PKCS#12 formátumú magánkulcsok hozzáadása
- CRL tárolása

Az InfoSigno az érvényesség ellenőrzés során a végtanúsítványra **visszavonási információkat (CRL) gyűjt** be. A paraméterezhető türelmi idő letelte után megismétli a visszavonási információk lekérését, hogy az aláírás érvényességének ellenőrzése a legfrissebb CRL-ek alapján történjen meg. Ellenőrzi a tanúsítványokon és a CRL-eken lévő aláírásokat.
A **tanúsítványlánc tanúsítványai**ra megnézi, hogy az érvényességi idejükbe beleesik-e az aláíráshoz csatolt időbélyegben szereplő időpont. Továbbá megvizsgálja, hogy szerepel-e a visszavonási listán a tanúsítvány, és amennyiben igen, akkor az időbélyeg által meghatározott időpontban visszavont állapotú volt-e.

BF8 Titkosítás, megoldás

Az InfoSigno v1.0.0 titkosítás és kapcsolódó megoldás biztonsági funkciója aszimmetrikus RSA/1024 algoritmust használ a szimmetrikus AES/256 rejtjelezés/megoldás által használt titkos kulcs továbbítására.
Támogatott kulcs átviteli algoritmusok:

- RSA algoritmus 1024 bit kulcshosszal.

Támogatott szimmetrikus titkosítási algoritmusok:

- • AES 256 bit [FIPS PUB 197].

A küldő fél a címzett nyilvános kulcsát tartalmazó tanúsítvány felhasználásával rejtjelezi az adatok titkosításához használt véletlen kulcsot.
A küldő fél a támogatott szimmetrikus algoritmus és a hozzá tartozó kulcshossz alapján rejtjelezi a továbbítandó adatokat.
A fogadó fél a saját magánkulcsának felhasználásával dekódolja az adatok titkosításához használt véletlen kulcsot.
A fogadó fél a támogatott szimmetrikus algoritmus és a hozzá tartozó kulcshossz alapján megoldja a kapott rejtjeles adatokat.

BF9 A TSF védelme és menedzsmentje

Ez a biztonsági funkció az alábbi feladatok végrehajtására képes:

- PIN kód közvetlen használat utáni törlése a memóriából;
- magánkulcs közvetlen használat utáni törlése a memóriából;
- PIN kód cseréje PKCS#12 formátumú kulcstároló fájl esetén.

6.2 A TOE garanciális intézkedései

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 meghatározása, ahol ez alkalmas, megadható a fontosabb tervdokumentációkra, életciklus tervekre vagy menedzseri tervekre való utalással.

6.2.1 Konfiguráció menedzselés

Az infoSigno v1.0.0 fejlesztése során keletkezett összes elemet figyelemmel kíséri a konfigurációmenedzsment rendszer, ezáltal biztosítja az egyes elemek rendelkezésre állását a termék teljes életciklusa alatt. A lefedettség az alábbi tételekre terjed ki:

- megvalósított termék;
- a termék forráskódja;
- tervezési dokumentáció;
- felhasználói és adminisztrátori útmutatók;
- konfiguráció menedzselés dokumentáció;
- teszt dokumentáció és teszt szoftver.

Az infoSigno v1.0.0 fejlesztése egy gépen történt, ennek védelme biztosítja, hogy csak engedélyezett módosítások történhessenek a fejlesztés alatt álló szoftveren. Az InfoSigno v1.0.0 termékhez verziószámot rendelnek, az értékelés során egyértelműen látható, hogy mely verzió értékelését végzik az értékelők.
A konfiguráció kezelési tervről készült leírás:
"InfoSigno v1.0.0 – A konfiguráció menedzselés dokumentációja"

6.2.2 Kiszállítás és működtetés

Az InfoSigno v1.0.0 szállításával és használatával kapcsolatos eljárások leírását az "InfoSigno v1.0.0 – Fejlesztői útmutató" /Reference Manual/ című dokumentum tartalmazza.

6.2.3 Fejlesztés

Az informális funkcionális specifikáció megfogalmazza az InfoSigno v1.0.0 fő biztonsági funkcióit, a külső interfészeket, ezek célját. Az informális specifikációt leíró dokumentum: „InfoSigno for Developers fejlesztő készlet minősített elektronikus aláíráshoz v1.0.0 Funkcionális specifikáció”.
A magas szintű terv informális eszközökkel leírja a fejlesztés alatt álló rendszer fő elemeit, a közöttük lévő kapcsolatokat. Az erről készült leírás:
„InfoSigno for Developers fejlesztő készlet minősített elektronikus aláíráshoz v1.0.0 - Magas szintű terv”.
Az alacsony szintű tervről készült dokumentáció: "InfoSigno - Alacsony szintű terv" /InfoSigno Dokumentáció - automatikus dokumentáció készítő eszközzel készült változat/

Az "InfoSigno v1.0.0 – Megfeleltetés elemzések" című dokumentum bemutatja, hogy a magasabb szintű informális leírásokban megadott biztonsági funkciókat hogyan valósítják meg az alacsonyabb szinteken, azaz hogyan felel meg egymásnak például a funkcionális specifikáció és a magas szintű terv.

6.2.4 Útmutató dokumentumok

A TOE felhasználói (alkalmazásfejlesztők) számára készült dokumentum: "InfoSigno v1.0.0 – Fejlesztői útmutató" /Reference Manual/

6.2.5 Az életciklus támogatása

A tervezés és fejlesztés során az értékelés tárgya bizalmasságának és sértetlenségének biztosításához a fejlesztői környezetre és a fejlesztők személyére vonatkozó szabályokat alkalmaztak. A fejlesztők a tervek és fejlesztés részleteit a termék teljes élete folyamán csak az arra feljogosított személyekkel beszélhetik meg, a fejlesztési telephelyen csak az arra jogosult személyek férhetnek hozzá a termékkel kapcsolatos programokhoz, dokumentációkhoz.
Az "InfoSigno v1.0.0 – A fejlesztési biztonság dokumentációja" leírás tartalmazza a fejlesztők által az értékelés tárgya fejlesztése során alkalmazott szabályok leírását.

Az InfoSigno fejlesztői környezetében a teljes fejlesztési és karbantartási folyamatot ellenőrzés alatt tartják. Az InfoSigno fejlesztéséhez és karbantartáshoz felállított és használt életciklus modellt az "InfoSigno v1.0.0 – Az életciklust meghatározó dokumentáció" című dokumentáció írja le.

6.2.6 Tesztelés

Az InfoSigno v1.0.0 teszteléséhez az alábbi, teszteléssel kapcsolatos dokumentumok készültek:
"InfoSigno v1.0.0 – Tesztelési dokumentáció"

"InfoSigno v1.0.0 – Teszt lefedettség elemzés"

"InfoSigno v1.0.0 – Teszt mélység elemzés"

6.2.7 Sebezhetőségek felmérése

Az útmutató dokumentumok ismeretében a tesztelési eljárással párhuzamosan sebezhetőségi elemzésre is sor került. Az azonosított sebezhetőségek esetén ki kell mutatni, hogy az adott sebezhetőség miért nem használható ki az értékelés tárgya működési környezetében.

A fejlesztői sebezhetőségi elemzést az alábbi dokumentum tartalmazza:
"InfoSigno v1.0.0 - Sebezhetőség elemzés"

7 PP megfelelőség

Jelen Biztonsági előirányzat a PKE PP alapján készült, de az InfoSigno specifikus biztonsági jellemzői miatt PP megfelelőségi nyilatkozatot nem tesz.

8 Indoklások

Ez a fejezet tartalmazza azon indoklásokat, melyek megmutatják, hogy az InfoSigno v1.0.0 valóban kivédi a számításba vett veszélyeket és teljesíti a biztonsági céljait. Mivel az InfoSigno 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 TOE IT környezetébe tartoznak a TOE által használt programcsomagok és az operációs rendszer, továbbá minősített elektronikus aláírás esetén a BALE eszköz és annak biztonságos használatát biztosító programok, vagy a KHE eszköz és annak meghajtó programjai.

8.1 A biztonsági célok indoklása

8.1.1 A környezeti biztonsági célok (általános 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.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, melyek megbízhatónak tekinthetők a TOE által hívott, kriptográfiai funkciók megvalósítása terén. Minősített elektronikus aláírás létrehozása esetén a TOE környezetéről feltételezés, hogy tartalmaz legalább egy NHH által nyilvántartott, tanúsított BALE-t, mely tárolja és védi az aláíró magánkulcsát, illetve végrehajtja a digitális aláírást. A feltételezésből származtatott biztonsági cél:

- **OE.Crypto**: A TOE által meghívott kriptográfiai funkciókat TOE hatáskörén kívüli modulok hajtják végre (például 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.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 azonosító és hitelesítő 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 biztonsági cél visszavezethető egy vagy több feltételezésre vagy veszélyre. Az indoklás az előző, itt már nem ismételjük meg.

8.2 táblázat – A környezeti biztonsági célok leképezése veszélyekre és feltételezésekre

Cél	**Feltételezés/veszély**
OE.Authorized_Users	AE.Authorized_Users
OE.Configuration	AE.Configuration
OE.Crypto	AE.Crypto_Module
OE.PKI_Info	AE.PKI_Info AE.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.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 Az InfoSigno v1.0.0 által teljesítendő biztonsági célok indoklása

Az itt szereplő biztonsági célok mind az InfoSigno v1.0.0 hatáskörén belül teljesítendőek.

8.1.2.1 CPV – Alap csomag biztonsági céljainak indoklása

A „CPV – Alap” 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 CPV – Alapcsomag 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 (vagyis egy megbízható pontig visszavezethető) 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 **CPV – Alap** 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

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.

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

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

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

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

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

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_lnfo**
2	O.Auth_TimeStamp_Info	**T.Wrong_TimeStamp_lnfo**
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 tekintetében.

8.2.1 A funkcionális biztonsági követelmények indoklása

Az összes biztonsági cél funkcionális követelményekre vagy feltételezésekre való leképezését mutatja a 8.17 táblázat. Az alap TOE funkcionális követelmények leképezéséhez és a csomagokhoz az indoklásokat külön alfejezetek tartalmazzák. 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

Sorszám	Biztonsági cél	Funkcionális komponens
A környezetre vonatkozó biztonsági célok leképezése a környezet által megvalósítandó funkcionális követelményekre		
1	OE.DAC	FDP_ACC.1, FDP_ACF.1
2	OE.I&A	FIA_ATD.1, FIA_UAU.1, FIA_UID.1
3	OE.Init_Secure_Attr	FMT_MSA.3
4	OE.Invoke	FPT_RVM.1
5	OE.Limit_Actions_Auth	FIA_UAU.1, FIA_UID.1
6	OE.Limit_Tries	FIA_AFL.1
7	OE.No_Echo	FIA_UAU.7
8	OE.Protect_I&A_Data	FMT_MTD.1, FMT_SMF.1
9	OE.Secure_Attributes	FMT_MSA.1, FMT_SMF.1
10	OE.Security_Roles	FMT_SMR.2
11	OE.Self_Protect	FPT_SEP.1
12	OE.Trust_Anchor	FMT_MTD.1, FMT_SMF.1
13	OE.TSF_Data	FMT_MTD.1, FMT_SMF.1
14	OE.Authorized_Users	(Nem a TOE-ra vonatkozó) adminisztrátori és felhasználói útmutatókban megadva (AGD_ADM.1 és AGD_USR.1)
15	OE.Configuration	(Nem a TOE-ra vonatkozó) indítási és telepítési útmutatókban megadva (ADO_IGS.1)
16	OE.Crypto	FCS_CRM_FPS.1
17	OE.Physical_Security	A fizikai biztonsági szabályok részeként definiálva a (nem a TOE-ra vonatkozó) AGD_ADM.1 és AGD_USR.1 összetevőkben.
18	OE.PKI_Info	FDP_ITC_PKI_INF.1/1 FDP_ITC_PKI_INF.1/2
19	OE.Time	FPT_STM.1

CPV – Alap csomag céljainak leképezése		
1	O.Correct_Time	FDP_CPD.1
2	O.Current_Certificate	FDP_DAU_CPV_CER.1 FDP_DAU_CPV_CER.2 FDP_DAU_CPV_CER.3
3	O.Get_KeyInfo	FDP_DAU_CPV_OUT.1
4	O.Path_Find	FDP_CPD.1
5	O.Trusted_Keys	FDP_DAU_CPV_CER.1 FDP_DAU_CPV_CER.2 FDP_DAU_CPV_CER.3
6	O.User	FDP_DAU_CPV_CER.2
7	O.Verified_Certificate	FDP_DAU_CPV_CER.1 FDP_DAU_CPV_CER.2 FDP_DAU_CPV_CER.3
8	O.Valid_Certificate	FDP_DAU_CPV_CER.1
A PKI aláírás létrehozás csomag céljainak leképezése		
1	O.Give_Sig_Hints	FDP_ETC_SIG.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
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 (lásd 3.1 szakasz), valamint kapcsolódó célok és követelmények elégítik ki. Minden esetben a feltételezések arra a funkcionalitásra vonatkoznak, melyet a környezet biztosít a környezeti célok teljesítése érdekében. Az alábbiakban az egyes környezeti célok indoklása következik.
Jelen TOE esetén IT környezeti célként kerültek a biztonsági előirányzatba az PKE PP családban általános biztonsági célként jelölt biztonsági célok. Így ezen alfejezet ezeknek az indoklását is tartalmazza.

OE.Authorized_Users: az engedéllyel rendelkező felhasználók megbízhatók a téren, hogy a számukra kijelölt feladatokat hajtják végre.
Ez a környezeti biztonsági cél az AE.Authorized_Users feltételezést fedi le, amely kimondja, hogy a jogosult felhasználók megbízhatók a tekintetben, hogy a nekik kijelölt feladatokat hajtják végre. A cél és feltételezés teljesítését teszik lehetővé a következők:

- Az adminisztrátori és felhasználói útmutatók, amint azt az AGD_ADM.1 és AGD_USR.1 garanciakövetelmények előírják.

OE.Configuration: a TOE-t úgy kell telepíteni és konfigurálni, hogy a TOE biztonságos állapotban kezdjen el üzemelni.
Ez az AE.Configuration-t fedi le, azaz a TOE-t megfelelően telepítik és konfigurálják. A cél és feltételezés teljesítését teszik lehetővé:

- Az indítási és telepítési útmutatók, ahogyan azt az ADO_IGS.1 garanciakövetelmény előírja: pontos telepítési és konfigurálási dokumentációt kell készíteni, amely biztosítja a TOE megfelelő (biztonságos állapotú) installálását és beállítását.

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. A TOE környezetnek minősített elektronikus aláírás létrehozása esetén tartalmaznia kell legalább egy NHH által nyilvántartásba vett, tanúsított BALE-t, mely tárolja és védi az aláíró magánkulcsát, illetve végrehajtja a digitális aláírást Ezt a célt az AE.Crypto_Module feltételezés elégíti ki, azaz egy feltételezés, amely kimondja, hogy a TOE által meghívott kriptográfiai funkciókat TOE hatáskörén kívüli modulok hajtják végre (OpenSSL), melyek megbízhatónak tekinthetők a TOE által hívott, kriptográfiai funkciók megvalósítása terén.
Továbbá, 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.

- FCS_CRM_FPS.1, az IT környezetben minősített elektronikus aláírás létrehozása esetén NHH által nyilvántartott, tanúsított biztonságos aláírás létrehozó eszköznek (BALE) kell lennie.

OE.Physical_Security: kimondja, hogy 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.
Az AE.Physical_Protection feltételezést fedi le, amely kimondja, hogy léteznie kell fizikai védelmi intézkedéseknek a TOE környezetben. A TOE szoftver feltételezés szerint védett a jogosulatlan fizikai hozzáféréstől. A cél teljesüléséhez hozzájárulnak még:

- Az adminisztrátori és felhasználói útmutatók, amint azt az AGD_ADM.1 és AGD_USR.1 garanciakövetelmények előírják. Az adminisztrátori és felhasználói útmutatók adják meg a TOE telepítési és üzemeltetési biztonsági szabályzatát.

OE.PKI_Info: az IT környezetnek biztosítania kell a TOE számára a tanúsítvány és tanúsítvány visszavonási információkat, valamint az időbélyegzés szolgáltatóhoz való hozzáférést. A cél megvalósítását biztosító követelmények:

- FDP_ITC_PKI_INF.1/1 és FDP_ITC_PKI_INF.1/2, PKI információk importálása a TSF-en kívülről, amely megköveteli, hogy az IT környezetnek lehetővé kell

tennie, hogy a tanúsítványok és CRL-ek, valamint az időbélyegzés szolgáltatás igény szerint a TOE rendelkezésére álljanak.

OE.Time: a környezetnek hozzáférést kell biztosítania a pontos időhöz, megkívánt pontossággal, GMT formára alakítva.
Az AE.Time-t fedi le, amely feltételezi, hogy a környezet a TOE számára biztosítja a pontos időt a megkívánt pontossággal, GMT formátumban. Teljesülését biztosító követelmény:

- FPT_STM.1 Megbízható időbélyegek, amely megköveteli, hogy az IT környezet képes legyen megbízható időbélyegeket biztosítani a TSF számára.

OE.DAC: Az IT környezet TSF-nek ellenőriznie és korlátoznia kell a felhasználók hozzáféréseit a TOE értékekhez, egy megadott hozzáférés ellenőrzési szabályzatnak megfelelően. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FDP_ACC.1, Részleges hozzáférés ellenőrzés – PKI engedélyek kezelése, ami megköveteli, hogy a TSF érvényre juttassa a PKI engedélykezelési SFP-t.
- FDP_ACF.1, Biztonsági tulajdonság alapú hozzáférés ellenőrzés – PKI engedélyek kezelése, amely megköveteli, hogy a TSF megvalósítsa a PKI engedélykezelési SFP hozzáférés ellenőrzési szabályzatát az objektumokra. Ez a követelmény az FDP_ACC.1-ben specifikált szabályzat meghatározását és kikényszerítését jelenti.
- Bár nem (csak) IT környezeti követelmény, de itt kell megemlíteni az FDP_RIP.1 Részleges maradvány információ védelem követelményt, ami megköveteli, hogy a TOE működése szempontjából érzékeny adatokat a TOE törölje azok közvetlen használata után.

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. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FIA_ATD.1, Felhasználói tulajdonság megadása, amely megköveteli, hogy a TSF karbantartsa az egyedi felhasználók számára a szerepköröket. Ez a követelmény azt biztosítja, hogy minden felhasználó beletartozik egy vagy több szerepkörbe, mely(ek) bizonyos engedélyeket és hozzáféréseket jelent(enek) számára.
- FIA_UID.1, Azonosítás időzítése, amely megköveteli, hogy a TSF tegyen lehetővé olyan tevékenységeket, melyeket a felhasználó nevében annak azonosítása előtt végre kell hajtani, majd a TSF követelje meg a felhasználó sikeres azonosítását minden más TSF által közvetített tevékenység előtt. Ez a követelmény azt biztosítja, hogy minden felhasználó azonosításra kerül.
- FIA_UAU.1, Hitelesítés időzítése, amely megköveteli, hogy a TSF tegyen lehetővé olyan tevékenységeket, melyeket a felhasználó nevében annak hitelesítése előtt végre kell hajtani, és a TSF követelje meg a felhasználó sikeres hitelesítését minden más TSF által közvetített tevékenység előtt. Ez a követelmény azt biztosítja, hogy minden felhasználó hitelesítésre kerül.

OE.Init_Secure_Attr: Az IT környezet TSF-nek érvényes és helyes alapértelmezett biztonsági tulajdonságokról kell gondoskodnia egy objektum inicializálásakor. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FMT_MSA.3, Statikus tulajdonság inicializálás, amely megköveteli, hogy a TSF érvényre juttassa a PKI engedélykezelés SFP-t az olyan biztonsági tulajdonságok specifikus kezdeti értékeinek biztosítása érdekében, amely tulajdonságokat az SFP teljesítésére használ a TOE. Ez a követelmény azt biztosítja, hogy egy objektum létrejöttekor érvényes alapértelmezett biztonsági tulajdonságok legyenek megadva.

OE.Invoke: kimondja, hogy az IT környezet biztosítania kell, hogy a TSF minden tevékenység esetén érvényesüljön. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FPT_RVM.1, A TSP megkerülhetetlensége, amely megköveteli, hogy a TSF-nek biztosítania kell, hogy minden TSP-t kikényszerítő funkció meghívódik és sikeresen lefut, mielőtt bármilyen más, a TSF felügyelete alá tartozó más funkció végrehajtódhatna. Ez a követelmény a TSF meghívását biztosítja minden tevékenységre.

OE.Limit_Actions_Auth: Az IT környezet TSF-nek korlátoznia kell azon tevékenységeket, melyeket egy felhasználó végrehajthat, mielőtt a TSF ellenőrzi a felhasználó kilétét. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FIA_UID.1, Azonosítás időzítése, amely megköveteli, hogy a TSF tegye lehetővé azon tevékenységek megadását, amelyeket a felhasználó nevében annak azonosítása előtt végre kell hajtani, majd a TSF követelje meg a felhasználó sikeres azonosítását minden más TSF által közvetített tevékenység előtt. Ez a követelmény azt biztosítja, hogy minden felhasználó azonosításra kerül.
- FIA_UAU.1, Hitelesítés időzítése, amely megköveteli, hogy a TSF tegye lehetővé azon TSF által közvetített tevékenységek listájának megadását, melyeket a felhasználó nevében annak hitelesítése előtt végre kell hajtani, és a TSF követelje meg a felhasználó sikeres hitelesítését minden más TSF által közvetített tevékenység előtt. Ez a követelmény azt biztosítja, hogy minden felhasználó hitelesítésre kerül.

OE.Limit_Tries: Az IT környezet TSF-nek korlátoznia kell az egymás utáni sikertelen hitelesítések számát. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FIA_AFL.1, Hitelesítési hibák kezelése, amely megköveteli, hogy a TSF észlelje, amikor egy adott számú sikertelen hitelesítési kísérlet történik az IT környezet által végrehajtott hitelesítési folyamatban. Amikor a megadott darabszámot eléri vagy meghaladja a sikertelen kísérletek száma, a TSF az IT környezet TSF által előírt műveletet hajtja végre.

OE.No_Echo: Az IT környezet TSF-nek nem szabad kijeleznie a hitelesítési információkat. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FIA_UAU.7, Védett hitelesítési visszacsatolás, amely megköveteli, hogy a TSF csak a specifikált visszacsatolásokat biztosítsa a felhasználó felé a hitelesítési folyamat közben. Ez a követelmény arról gondoskodik, hogy a TSF ne jelezze ki a hitelesítési információkat.

OE.Protect_I&A_Data: a TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie az I&A adatok módosítását. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FMT_MTD.1, TSF adatok kezelése: A követelmény célja, hogy a jogosult felhasználók és műveleteik megadott TSF adatokra legyenek megadva.
- FMT_SMF.1, Menedzsment funkciók megadása, amely megköveteli, hogy a TSF képes legyen biztonsági menedzsment funkciók végrehajtására.

OE.Secure_Attributes: Az IT környezet TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie a biztonsági tulajdonságok módosítását. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FMT_MSA.1, Biztonsági tulajdonságok kezelése, amely megköveteli, hogy a TSF érvényre juttassa a PKI engedélyezés kezelés SFP-t. Ez a követelmény azt biztosítja, hogy csak jogosult felhasználók, azaz a megfelelő szerepkörbe tartozók számára megengedett a specifikált biztonsági tulajdonságok módosítása.
- FMT_SMF.1, Menedzsment funkciók megadása, amely megköveteli, hogy a TSF képes legyen biztonsági menedzsment funkciók végrehajtására.

OE.Security_Roles: Az IT környezet TSF-nek karban kell tartania a biztonsági szempontból lényeges szerepköröket és a felhasználók ezen szerepkörökhöz való rendelését. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FMT_SMR.2, Megszorítások a biztonsági szerepkörökre, amely megköveteli, hogy a szerepkörök azonosítottak legyenek és minden felhasználó tartozzon bele valamelyikbe.

OE.Self_Protect: kimondja, hogy az IT környezet TSF-nek a saját futásához egy tartományt kell kezelnie, melyet és melynek értékeit védi a külső beavatkozástól, hamisítástól vagy jogosulatlan felfedéstől. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FPT_SEP.1, TSF tartomány szétválasztás, amely megköveteli, hogy a TSF saját futásához egy biztonsági tartományt tart fenn, amely megvédi a nem megbízható egyedek által megkísérelt hamisítástól és beavatkozástól, és a TSF kikényszeríti a szétválasztást a TSC-ben lévő szubjektumok biztonsági tartományai között.

OE.Trust_Anchor, kimondja, hogy az IT környezet TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie a megbízható pontok karbantartását. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FMT_MTD.1, TSF adatok kezelése: a követelmény célja, hogy a jogosult felhasználók és műveleteik megadott TSF adatokra (beleértve a megbízható pontokat) legyenek megadva.
- FMT_SMF.1, Menedzsment funkciók megadása, amely megköveteli, hogy a TSF képes legyen biztonsági menedzsment funkciók végrehajtására.

OE.TSF_Data, kimondja, hogy a TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie a TSF adatok módosítását. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FMT_MTD.1, TSF adatok kezelése: a követelmény célja, hogy a jogosult felhasználók és műveleteik megadott TSF adatokra legyenek megadva.
- FMT_SMF.1, Menedzsment funkciók megadása, amely megköveteli, hogy a TSF képes legyen biztonsági menedzsment funkciók végrehajtására.
- FDP_RIP.1 Részleges maradvány információ védelem követelmény célja, hogy a TOE működése szempontjából érzékeny adatokat a TOE törölje azok közvetlen használata után.

8.2.1.2 Biztonsági célok a „Tanúsítási útvonal érvényesség ellenőrzése – Alap” csomagra - indoklás

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

- FDP_CPD.1: megköveteli, hogy a TSF egy megbízható forrásból kapja meg a pontos időt.

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

- FDP_DAU_CPV_CER.1, FDP_DAU_CPV_CER.2 és FDP_DAU_CPV_CER.3, melyek megkövetelik, hogy a TSF csak akkor fogadjon el egy tanúsítványt, ha a megadott ellenőrzések sikeresek voltak, beleértve a tanúsítvány érvényességi idejének ellenőrzését is.

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

- FDP_DAU_CPV_OUT.1, Tanúsítási útvonal kimenet – alapkövetelmény: a TSF az alany nyilvános kulcsát és más, az ST írója által megadott információt 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 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):

- FDP_DAU_CPV_CER.1, FDP_DAU_CPV_CER.2 és FDP_DAU_CPV_CER.3, melyek megkövetelik, hogy a TSF a tanúsítási útvonal érvényesség ellenőrzésekor megbízható nyilvános kulcsokat használjon.

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

- FDP_DAU_CPV_CER.2, Közbenső tanúsítvány feldolgozás- alapkövetelmény: megköveteli, hogy a TSF csak akkor fogadjon el közbenső tanúsítványt, ha azt egy CA bocsátotta ki.

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

- FDP_DAU_CPV_CER.1, FDP_DAU_CPV_CER.2 és FDP_DAU_CPV_CER.3, melyek megkövetelik, hogy a TSF a tanúsítási útvonal érvényesség ellenőrzésekor csak ellenőrizhető aláírással bíró tanúsítványokat fogadjon el.

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

- FDP_DAU_CPV_CER.1, Tanúsítvány feldolgozás – alapkövetelmény: megköveteli, hogy a TSF csak olyan tanúsítványokat használjon, amelyek érvényesek, azaz a visszavonási állapot információ jelzi, hogy a tanúsítvány nem visszavont.

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 az ST írója által meghatározott egyéb információkat a digitális aláírásba.

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 a `keyUsage` kiterjesztésben csak a `nonRepudiation` bit van beállítva
  - minősített elektronikus aláírás esetén az aláíró tanúsítványában a kötelező qCStatements kiterjesztés meglétének ellenőrzése szükséges;
  - fokozott biztonsági aláírás esetén a `keyUsage` kiterjesztésben a `nonRepudiation` bit mellett csak a digSig bit lehet opcionálisan beállítva;
  - 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, ahogyan azt az ST írója előírja, és a TSF-nek használnia kell az alábbi információkat „Tanúsítási útvonal érvényesség ellenőrzésé”-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”-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 az ST írója által kiválasztott információkat felhasználja a rejtjeles adatokból, hogy azonosítani lehessen a megfelelő magánkulcsot és kulcs átviteli algoritmust, és a TSF végre tudja hajtani a megoldást (dekódolást).

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

Az infoSigno v1.0.0 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. A MIBÉTS kiemelt garanciaszint a biztonsági funkciók elemzése által ad garanciát.
A biztonsági funkciók működésének megértéséhez az alábbiak feldolgozására kerül sor: funkcionális és a teljes interfész specifikáció, az útmutató leírások, az InfoSigno v1.0.0 magas és alacsony szintű terve, továbbá a megvalósítás egy részhalmaza. A MIBÉTS kiemelt garanciaszint olyan fejlett mechanizmusokat és/vagy eljárásokat követel meg, amelyek biztosítják, hogy a TOE-t nem hamisították meg a fejlesztés vagy szállítás során.

8.3 A függőségek teljesítésének indoklása

8.18 táblázat – Funkcionális követelmények közötti függések

Sorszám	Követelmény	Függések
IT környezet funkcionális követelményei		
1	FDP_ACC.1	FDP_ACF.1
2	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
3	FIA_AFL.1	FIA_UAU.1
4	FIA_ATD.1	Nincs
5	FIA_UAU.1	FIA_UID.1
6	FIA_UAU.7	FIA_UAU.1
7	FIA_UID.1	Nincs
8	FMT_MSA.1	FDP_ACC.1, FMT_SMF.1, FMT_SMR.1
9	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
10	FMT_MTD.1	FMT_SMF.1, FMT_SMR.1
11	FMT_SMF.1	Nincs
12	FMT_SMR.2	FIA_UID.1
13	FPT_RVM.1	Nincs
14	FPT_SEP.1	Nincs
15	FCS_CRM_FPS.1	Nincs
16	FDP_ITC_PKI_INF.1/1 FDP_ITC_PKI_INF.1/2	Nincs
17	FPT_STM.1	Nincs
18	FDP_RIP.1	Nincs
CPV – Alap csomag		
1	FDP_CPD.1	Nincs
2	FDP_DAU_CPV_CER.1	FCS_COP.1 (Lásd 2. megjegyzést) FPT_STM.1 (Lásd 1. megjegyzést)
3	FDP_DAU_CPV_CER.1	FCS_COP.1 (Lásd 2. megjegyzést) FPT_STM.1 (Lásd 1. megjegyzést)
4	FDP_DAU_CPV_CER.1	FCS_COP.1 (Lásd 2. megjegyzést) FPT_STM.1 (Lásd 1. megjegyzést)
5	FDP_DAU_CPV_OUT.1	Nincs
PKI aláírás létrehozás csomag		
1	FDP_ETC_SIG.1	FCS_COP.1 (Lásd 2. megjegyzést)
PKI aláírás ellenőrzés csomag		
1	FDP_ITC_SIG.1	Nincs
2	FDP_DAU_SIG.1	FCS_COP.1 (Lásd 2. megjegyzést) FDP_DAU_CPV_OUT.1 (Lásd 3. megjegyzést)

PKI titkosítás kulcs átviteli algoritmusokkal csomag		
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 csomag		
1	FDP_ITC_ENC.1	FCS_COP.1 (Lásd 2. megjegyzést)
CRL ellenőrzés csomag		
1	FDP_DAU_CRL.1	FCS_COP.1 (Lásd 2. megjegyzést) FPT_STM.1 (Lásd 1. megjegyzést)
Időbélyeg kérés és ellenőrzés csomag		
1	FDP_DAU_TS.1	FCS_COP.1 (Lásd 2. megjegyzést)

1. megjegyzés: Az FPT_STM.1 függést teljesíti az IT környezetre vonatkozó FPT_STM.1 követelmény.
2. megjegyzés: Az 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 CPV – Alap csomag szerepeltetése.

8.4 A TOE összefoglaló előírás indoklása

8.4.1 A TOE funkcionális biztonsági követelményeinek leképezése a biztonsági funkciókra

Az alábbi táblázat felsorolja az InfoSigno v1.0.0 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 Digitális aláírás ellenőrzés**	**BF3 Üzenet digitális aláírása**	**BF4 Elektronikus aláírás ellenőrzés**	**BF5 Időbélyeg kérés**	**BF6 Időbélyeg ellenőrzés**	**BF7 Tanúsítási útvonal felépítése és érvényesség ellenőrzése**	**BF8 Titkosítás, megoldás**	**BF9 A TSF védelme és menedzsmentje**
FDP_CPD.1 Függés: nincs							**X**		
FDP_DAU_CPV_CER.1 Függések: FCS_COP.1 FPT_STM.1							**X**		
FDP_DAU_CPV_CER.2 Függések: FCS_COP.1 FPT_STM.1							**X**		
FDP_DAU_CPV_CER.3 Függések: FCS_COP.1 FPT_STM.1							**X**		
FDP_DAU_CPV_OUT.1 Függések: nincsenek		**X**					**X**	**X**	
FDP_ETC_SIG.1 Függések: FCS_COP.1	**X**		**X**						
FDP_ITC_SIG.1 Függések: nincsenek				**X**					
FDP_DAU_SIG.1 Függések: FCS_COP.1 FDP_DAU_CPV_ OUT.1		**X**							
FDP_ETC_ENC.1 Függések: FCS_COP.1 FDP_DAU_CPV_ OUT.1								**X**	

FDP_DAU_ENC.1 Függések: FDP_DAU_CPV_OUT.1								**X**	
FDP_ITC_ENC.1 Függések:FCS_COP.1								**X**	
FDP_DAU_CRL.1 Függések: FCS_COP.1 FPT_STM.1							**X**		
FDP_DAU_TS.1 Függések: FCS_COP.1					**X**	**X**			
FDP_RIP.1									**X**
FMT_SMF.1/2									**X**
FMT_MTD.1/2									**X**

Megjegyzés: FCS_COP.1 és FPT_STM.1 IT környezeti követelmények.

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 időbélyeg
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 időbélyegzés 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 kulcsú 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

BALE		**Biztonságos aláírás-létrehozó eszköz**
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./
KHE		**Kriptográfiai hardver eszköz**
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./