eSign Toolkit
minősített elektronikus aláíráshoz
v2.2.2

BIZTONSÁGI ELŐIRÁNYZAT

Verzió:	v1.1
Dátum:	2011.11.24.
Megrendelő:	NOREG Kft.
Fájl:	eSignTK_ST_v11.doc
Minősítés:	Nyilvános
Oldalak:	76

Tartalomjegyzék

Változás kezelés **4**

1. Bevezetés **5**

1.1 Azonosítás *5*

1.2 Áttekintés *6*

1.3 Kapcsolódó dokumentumok *7*

1.4 A biztonsági előirányzat szerkezete *8*

1.5 Common Criteria (Közös szempontok) megfelelőség *8*

2 Az értékelés tárgyának (eSign Toolkit v2.2.2) leírása **9**

2.1 Áttekintés *9*

2.2 Alkalmazott megközelítési mód *9*
2.2.1 CC 2. rész és kiterjesztett 2. rész funkcionális biztonsági követelmények 9

2.3 A TOE meghatározása *9*
2.3.1 A TOE típusa 9
2.3.2 A TOE felépítése 10

2.4 A TOE alkotóelemei *11*
2.4.1 Tanúsítási útvonal érvényességének ellenőrzése - Alapcsomag 12
2.4.2 PKI aláírás létrehozás csomag 13
2.4.3 PKI aláírás ellenőrzés csomag 13
2.4.4 Tanúsítvány visszavonási lista (CRL) érvényesség ellenőrzése csomag 13
2.4.5 Valós idejű tanúsítvány állapot protokoll (OCSP) kliens csomag 13
2.4.6 Időbélyeg kérése és ellenőrzése csomag 13

2.5 Garanciális követelmények *13*

3 Az eSign Toolkit v2.2.2 biztonsági környezete **14**

3.1 A biztonságos használattal kapcsolatos feltételezések *14*

3.2 Általános biztonsági fenyegetések *15*

3.3 Csomagokhoz kapcsolódó biztonsági fenyegetések *16*
3.3.1 Tanúsítási útvonal érvényesség ellenőrzése – Alap csomag 16
3.3.2 PKI aláírás létrehozás csomag 16
3.3.3 PKI aláírás ellenőrzés csomag 16
3.3.4 CRL érvényesség ellenőrzése csomag 17
3.3.5 OCSP kliens csomag 17
3.3.6 Időbélyeg kérése és ellenőrzése csomag 17

3.4 Szervezeti biztonsági szabályok *17*

4. Biztonsági célok **18**

4.1 A TOE-re vonatkozó általános biztonsági célok *18*

4.2 A csomagokra vonatkozó biztonsági célok *20*
4.2.1 Tanúsítási útvonal érvényességének ellenőrzése – Alap csomag 20
4.2.2 PKI aláírás létrehozási csomag 20
4.2.3 PKI aláírás ellenőrzési csomag 20
4.2.4 CRL érvényesség ellenőrzése csomag 21
4.2.5 OCSP kliens csomag csomag 21
4.2.6 Időbélyeg kérése és ellenőrzése csomag 21

5. IT biztonsági követelmények **22**

5.1 A TOE környezet által teljesítendő általános funkcionális biztonsági követelmények *23*
5.1.1 FDP osztály – Felhasználói adatok védelme 24
5.1.2 FIA osztály – Azonosítás és hitelesítés 26
5.1.3 FMT osztály – Biztonsági menedzsment 28
5.1.4 FCS osztály – Kriptográfiai támogatás 30
5.1.6 FPT osztály – A TOE biztonsági funkciók védelme 30
5.1.7 Funkcióerősségre vonatkozó követelmény 30
5.2. A TOE által teljesítendő, az egyes csomagokra vonatkozó funkcionális biztonsági követelmények *31*
5.2.1 „Tanúsítási útvonal érvényesség ellenőrzése – Alap" csomag 31
5.2.2 PKI aláírás létrehozás csomag 34
5.2.3 PKI aláírás ellenőrzési csomag 34
5.2.4 CRL érvényesség ellenőrzés csomag 36
5.2.5 OCSP kliens csomag 37
5.2.6 Időbélyeg kérése és ellenőrzése csomag 38
5.3 MIBÉTS fokozott garanciaszint *39*
5.3.1 Konfiguráció menedzselés (ACM, Assurance: Configuration Management) 40
5.3.2 Kiszállítás és működtetés (ADO, Assurance: Delivery and Operation) 41
5.3.3 Fejlesztés (ADV, Assurance: Development) 41
5.3.4 Útmutató dokumentumok (AGD, Assurance: Guidance Documents) 42
5.3.5 Életciklus támogatás (ALC, Assurance: Life Cycle Support) 44
5.3.6 Tesztek (ATE, Assurance: Tests) 44
5.3.7 A sebezhetőség felmérése (AVA, Assurance: Vulnerability Assessment) 45

6 TOE összefoglaló előírás 47
6.1 Az eSign Toolkit v2.2.2 biztonsági funkciói *47*
6.2 A TOE garanciális intézkedései *51*
6.2.1 Konfiguráció menedzselés 51
6.2.2 Kiszállítás és működtetés 51
6.2.3 Fejlesztés 51
6.2.4 Útmutató dokumentumok 52
6.2.5 Az életciklus támogatása 52
6.2.6 Tesztelés 52
6.2.7 Sebezhetőségek felmérése 52

7 PP megfelelőség 52

8 Indoklások 53
8.1 A biztonsági célok indoklása *53*
8.1.1 Az általános és a környezeti biztonsági célok indoklása 53
8.1.2 A biztonsági célok indoklása a csomagokra 57
8.2 A biztonsági követelmények indoklása *62*
8.2.1 A funkcionális biztonsági követelmények indoklása 62
8.2.2 A garanciális követelmények indoklása 71
8.3 A függőségek teljesítésének indoklása *71*
8.4 A TOE összefoglaló előírás indoklása *72*
8.4.1 A TOE funkcionális biztonsági követelményeinek leképezése a biztonsági funkciókra 72

9. Fogalmak, rövidítések 74
9.1 Fogalmak *74*
9.2 Rövidítések *77*

Változás kezelés

Verzió	Dátum	Leírás	Készítette
0.1	2008.05.04.	A szerkezet felállítása	Balázs István
0.8	2008.06.12.	Első teljes változat, néhány biztonsági funkció részlet még kiegészítésre szorul	Balázs István, Csaba László
0.9	2008.07.31.	Értékelésre átadott verzió	Csaba László
0.95	2008.09.28.	Az értékelés során pontosított változat	Csaba László
1.0	2008.11.02.	Az értékeléshez elfogadott végleges változat	Csaba László
1.1	2011.11.24.	Tanúsítvány karbantartáshoz a v2.2.2 verziónak megfelelő, kiegészített és pontosított változat (új támogatott hash függvények, új támogatott aláírás formátumok, minősített aláírás létrehozása esetén SHA-1 hash algoritmus tiltása)	Csaba László

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:	eSign Toolkit minősített elektronikus aláíráshoz v2.2.2 - Biztonsági előirányzat
Az értékelés tárgya:	eSign Toolkit fejlesztőkészlet v2.2.2
Az értékelés tárgya rövid neve:	eSign Toolkit, eSignTK, NoregPKI2.dll
Értékelési garancia szint:	MIBÉTS fokozott (EAL3)
Verzió szám:	1.1
Dátum:	2011. november 24.
Szerző:	Csaba László
Szponzor szervezet:	NOREG 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 <3> with augmentation
Kiegészítés:	Ebben a biztonsági előirányzatban az eredeti PKE PP család választott csomagjain túl kiegészült egy „Időbélyeg kérése és ellenőrzése”, csomaggal, amelyen nem képezték részét az eredeti PKE PP családnak.

1.2 Áttekintés

Az értékelés tárgya (eSign Toolkit v2.2.2) egy olyan C nyelven írt függvénygyűjtemény (fejlesztői programkönyvtár), melynek segítségével szabványos (X.509 szabványon alapuló) nyilvános kulcsú szolgáltatásokat biztosító alkalmazások fejleszthetők.

A függvénygyűjtemény az alábbi (fő funkciókat) biztosítja, illetve támogatja:

- TEXT/XML formátumú dokumentumokra szabványos formátumú (XAdES v1.2.2 és MELASZ-ready v2.0 szerinti XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL és XAdES-A, valamint RFC 3852 szerinti CMS) elektronikus aláírás létrehozása,
- TEXT/XML formátumú dokumentumokra létrehozott, szabványos formátumú (XAdES v1.2.2 és MELASZ-ready v2.0 szerinti XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL és XAdES-A, valamint RFC 3852 szerinti CMS) elektronikus aláírás ellenőrzése,
- X.509 v3 tanúsítványok és tanúsítványláncok kezelése (az RFC 5280 alapján),
- időbélyegzés kérés készítése és az időbélyeg válasz ellenőrzése (az RFC 3161 szabványt követő időbélyegző-szolgáltatókkal együttműködve),
- visszavonási információk (CRL és OCSP) kezelése (az RFC 5280 és RFC 2560 alapján),
- különböző aláírás-létrehozó eszközökkel (ALE) és PKCS#11-es felületen keresztül elérhető biztonságos aláírás-létrehozó eszközökkel (BALE) való együttműködési képesség.

A fenti fő funkciók alapján az eSign Toolkit v2.2.2 fejlesztői programkönyvtár segítségével alkalmazások széles köre fejleszthető, melyek a nyilvános kulcsú technológia alapján bizalmasságot, sértetlenséget, hitelesítést és letagadhatatlanságot biztosító szolgáltatások biztosítására használhatók.

A jelen biztonsági előirányzat egy csomag koncepcióra (különböző csomagokból történő moduláris szerkeszthetőségre) épülő, Common Criteria szerint tanúsított védelmi profil családon (PKE PP) alapul. A biztonsági előirányzat kiegészült az időbélyegzés kezelését megvalósító csomaggal (az eredeti védelmi profil csomagjai között hiányoztak ezek a lehetőségek).
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 és kiegészítésre, mely megfelel a jelen értékelés tárgya, az eSign Toolkit v2.2.2 igényeinek.

Az alábbi táblázat az eSign Toolkit v2.2.2 legfontosabb funkcióit, a PKE PP védelmi profil családból kiválasztott csomagokat és az időbélyeg kliens csomagot tekinti át.

Csomag neve	Funkcionalitás	Függések
PKE PP csomagok		
Tanúsítási útvonal érvényesség ellenőrzése (CPV) – Alap	X.509 érvényesség ellenőrzés végrehajtása (kivéve a szabályzat és név megszorítás feldolgozását)	Nincs
PKI aláírás létrehozás	Aláírás létrehozására magánkulcs használatával Aláírási információk generálása	Nincs
PKI aláírás ellenőrzés	Az aláírási információk feldolgozása Az aláírás ellenőrzésére nyilvános kulcs használatával	CPV – Alap
CRL érvényesség ellenőrzés	CRL lekérése CRL ellenőrzése és feldolgozása	Nincs
OCSP protokoll kliens	OCSP kérés előállítása és az OCSP válasz ellenőrzése az RFC 2560-nak megfelelően	CPV – Alap
ST csomag		
Időbélyeg kérése és ellenőrzése	Időbélyeg kérése és ellenőrzése az RFC 3161-nek megfelelően	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 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 1999
- RFC 3161 X.509 Internet Public Key Infrastructure - Time-Stamp Protocol (TSP), August 2001
- RFC 3852 Cryptographic Message Syntax, July 2004
- RFC 5280: X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile, May 2008
- 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
- ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES), v1.2.2, 2004-04
- ISO/IEC 15408:2005 Information technology — Security techniques — Evaluation criteria for IT security (Part 1,2,3)
- ISO/IEC 18045:2005 Information technology — Security techniques — Methodology for IT security evaluation
- A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (v1.0, 2008 június)
- MELASZ-ready v2.0: Egységes MELASZ formátum elektronikus aláírásokra v2.0
- PKCS #11 v2.11: Cryptographic Token Interface Standard

1.4 A biztonsági előirányzat szerkezete

A 2., 3., és 4. fejezetek az eSign Toolkit v2.2.2 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 fokozott garanciaszint követelményeit írja le.
A 6. fejezet az eSign Toolkit v2.2.2 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 verzióján alapul (ISO/IEC 15408 IT biztonság értékelési követelményei, 1. rész: Bevezetés és általános modell, 2. rész: Funkcionális biztonsági követelmények, 3. rész: Garanciális biztonsági követelmények), kiterjeszti a 2. részt, valamint megfelel a 3. résznek, EAL3-as értékelési garanciaszinten.

/A „kiterjeszti a 2. részt” meghatározása a CC 3.rész 5.4 pontja szerint: „Egy PP vagy TOE kiterjesztett, ha a funkcionális követelmények a 2. részben nem szereplő funkcionális összetevőket is tartalmaznak.”/

Az eSign Toolkit v2.2.2 biztonságára vonatkozó értékelés az [MSZ ISO/IEC 15408, **CC**] szabványban meghatározott modell (az informatikai biztonságértékelés szempontjai), valamint az ennek megfelelő értékelési módszertan [ISO/IEC 18045, **CEM**] honosított változatát tartalmazó **MIBÉTS** (Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma) módszertant követi.

Az értékelés garanciaszintje: **fokozott garanciaszint** (mely a CC/CEM EAL3 értékelési garanciaszintjének felel meg).

2 Az értékelés tárgyának (eSign Toolkit v2.2.2) leírása

2.1 Áttekintés

Az értékelés tárgya (az eSign Toolkit v2.2.2 függvénygyűjtemény) az alábbi tulajdonságokkal rendelkezik:

- képes szabványos formátumú (XAdES v1.2.2 és MELASZ-ready v2.0 szerinti XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL és XAdES-A, valamint RFC 3852 szerinti CMS) elektronikus aláírás létrehozására,
- képes szabványos formátumú (XAdES v1.2.2 és MELASZ-ready v2.0 szerinti XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL és XAdES-A, valamint RFC 3852 szerinti CMS) elektronikus aláírás ellenőrzésére,
- képes X.509 v3 tanúsítványok és tanúsítványláncok kezelése (az RFC 5280 alapján),
- alkalmas időbélyegzés kérés készítésére és az időbélyeg válasz ellenőrzésére (az RFC 3161 szabványt követő időbélyegző-szolgáltatókkal együttműködve),
- képes visszavonási információk (CRL és OCSP) lekérdezésére a hitelesítés-szolgáltatóktól (a tanúsítványból kiolvasott elérési helyről),
- képes együttműködni különböző aláírás-létrehozó eszközökkel (ALE) és biztonságos aláírás-létrehozó eszközökkel (BALE).

2.2 Alkalmazott megközelítési mód

Jelen biztonsági előirányzat a PKE védelmi profil családon alapul, azokban szereplő csomagok közül választotta ki a funkcionalitás alapján a megfelelőket. Ezen kívül létrehozott egy (az említett családban nem szereplő) időbélyegzés funkcionalitással rendelkező csomagot, a TOE biztonsági funkcióira vonatkozó követelmények leírására.

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

A CC 2. részét felhasználva a biztonsági szempontból fontos követelmények kialakításához a PP-család 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.
Ugyanakkor 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 meghatározása

Ez az alfejezet az eSign Toolkit v2.2.2 típusát és szerkezetét ismerteti, bemutatva kapcsolatait és határait más komponensek felé.

2.3.1 A TOE típusa

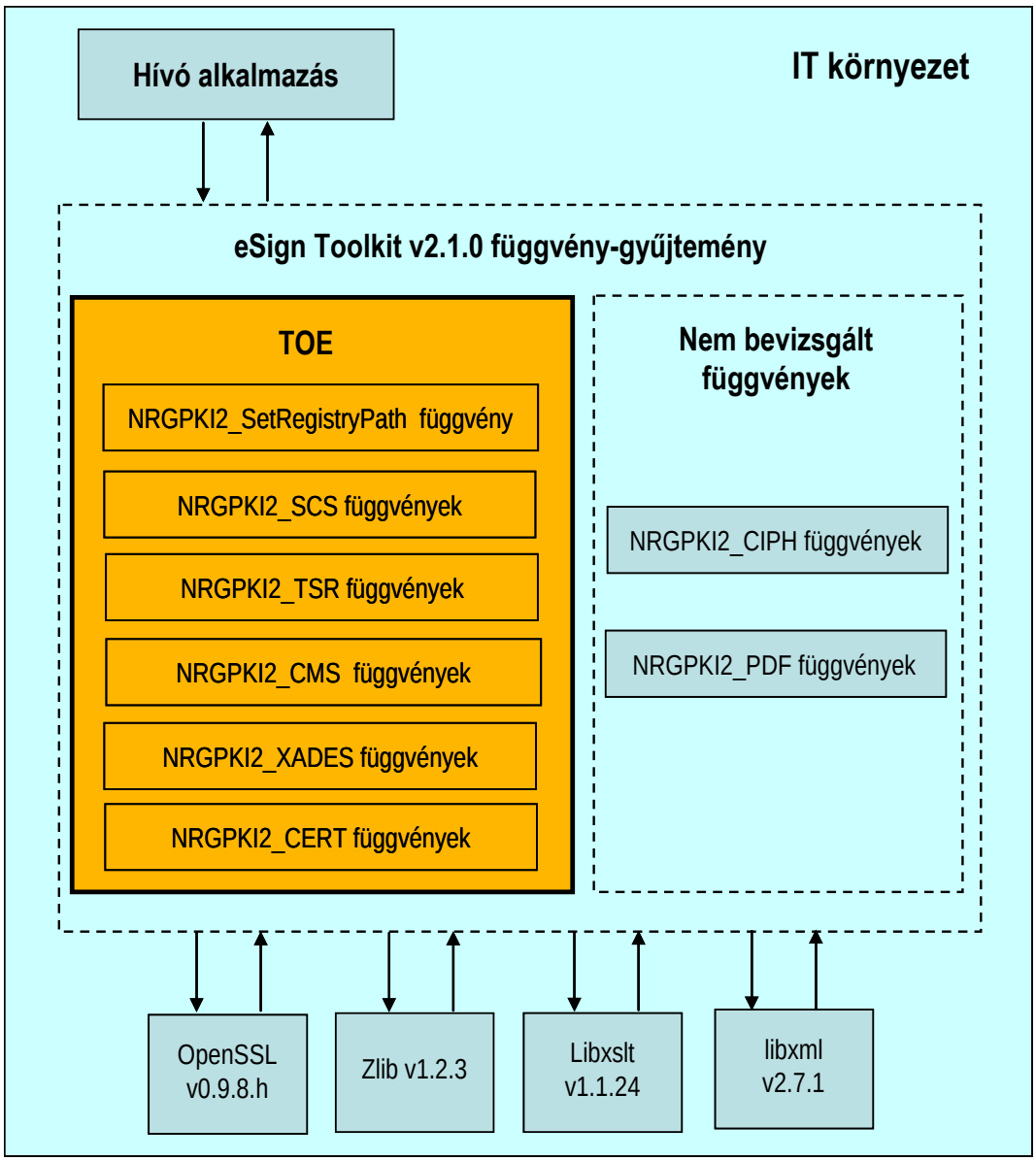
Az eSign Toolkit v2.2.2 szoftverfejlesztők számára készült, zárt rendszerben felhasználásra kerülő, nyilvános kulcs szolgáltatásokat biztosító C nyelven írt függvénygyűjtemény, olyan funkcionalitással, mellyel elektronikus aláírások létrehozása, ellenőrzése, az ellenőrzéshez érvényesítő információk feldolgozása, tanúsítási útvonal felépítése, tanúsítványok érvényességének ellenőrzése, visszavonási információk érvényesség ellenőrzése, időbélyeg kérése és ellenőrzése, OCSP kérése és ellenőrzése valósítható meg.

Az eSign Toolkit v2.2.2 az OpenSSL funkcióira épít, azokat felhasználja működése során, ezen keresztül valósítja meg a legtöbb kriptográfiai funkcionalitást. A kriptográfiai token eszközök kezelése PKCS#11 felületen keresztül történik.

A DLL különféle nyelvi környezetből hívható felülettel rendelkezik, szoftver fejlesztői csomagban kerül forgalomba.

2.3.2 A TOE felépítése

A 2.1 ábra az eSign Toolkit v2.2.2 struktúráját és az IT környezetbe való beágyazódását –a TOE határaival - mutatja be.



2.1 ábra: Az eSign Toolkit v2.2.2 és környezete

Az eSign Toolkit v2.2.2 által elvárt operációs rendszer: Windows XP SP2

Az eSign Toolkit v2.2.2 függvény csoportokból áll:

- Az NRGPKI2_SetRegistryPath függvény beállítja a konfigurációs paramétereket.
- Az NRGPKI2_SCS_xxx függvények kezelik az intelligens kártyán (PKCS11-en keresztül) vagy PEM fájlban tárolt magánkulcsot.
- Az NRGPKI2_TSR_xxx függvények az időbélyegzéssel kapcsolatos feladatokat végzik el.
- Az NRGPKI2_CMS_xxx függvények kezelik a CMS formátumú elektronikus aláírásokat.
- Az NRGPKI2_XAdES_xxx függvények kezelik a XAdES formátumú elektronikus aláírásokat.
- Az NRGPKI2_PDF_xxx függvények kezelik a PDF formátumú elektronikus aláírásokat.
- Az NRGPKI2_CERT_xxx függvények tanúsítványra vonatkozó információkat adnak.
- Az NRGPKI2_CIPH_xxx függvények titkosítást és dekódolást végeznek.

Az NRGPKI2_CIPH_xxx és az NRGPKI2_PDF_xxx függvények nem képezték a vizsgálat tárgyát (tehát a TOE részét sem).

Az eSign Toolkit v2.2.2 az IT környezet elemeit (harmadik fél által fejlesztett, nyilvánosan elérhető és szabadon felhasználható függvények) az alábbi feladatok elvégzéséhez használja:

- OpenSSL: általános kriptográfiai műveletek végrehajtása,
- Libxml: XML kezelés,
- Libxslt: XML megjelenítés,
- ZLIB: tömörítés.

Az eSign Toolkit v2.2.2 biztonsági funkciói szempontjából az OpenSSL és a libxml csomagok biztosítanak közvetve TOE biztonsági funkciót támogató funkciót.

Az eSign Toolkit v2.2.2 két üzemmódot különböztet meg:

- Fokozott biztonságú aláírás létrehozás üzemmód
    - Az eSign Toolkit v2.2.2-t biztonságos aláírás létrehozó eszköz nélkül használják elektronikus aláírások generálására és ellenőrzésére.
- Minősített elektronikus aláírás létrehozás üzemmód
    - 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 eSign Toolkit v2.2.2 a 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 eSign Toolkit v2.2.2-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.
Az eSign Toolkit v2.2.2 a PKE PP család alábbi csomagjainak biztonsági követelményeit veszi alapul.

Csomag neve	Funkcionalitás	Függések
PKE PP csomagok		
Tanúsítási útvonal érvényesség ellenőrzése (CPV) – Alap	X.509 érvényesség ellenőrzés végrehajtása (kivéve a szabályzat és név megszorítás feldolgozását)	Nincs
PKI aláírás létrehozás	Aláírás létrehozására magánkulcs használatával Aláírási információk generálása	Nincs
PKI aláírás ellenőrzés	Az aláírási információk feldolgozása Az aláírás ellenőrzésére nyilvános kulcs használatával	CPV – Alap
CRL érvényesség ellenőrzés	CRL lekérése CRL ellenőrzése és feldolgozása	Nincs
OCSP kliens	OCSP kérés előállítása és az OCSP válasz ellenőrzése az RFC 2560-nak megfelelően	CPV – Alap
ST csomag		
Időbélyeg kérése és ellenőrzése	Időbélyeg kérése és ellenőrzése az RFC 3161-nek megfelelően	CPV – Alap

2.1 táblázat – A csomagok áttekintése

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 az aláírásban állított időpont (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 eSign Toolkit v2.2.2 az aláírás létrehozását és kezdeti ellenőrzését az alábbi digitális aláírás sémák szerint valósítja meg:
Minősített elektronikus aláírás esetén:

- RSA algoritmus legalább 1024 bit kulcshosszal, és az alábbi lenyomatoló algoritmusok egyikével [PKCS#1.5-nek megfelelően]: SHA-224, SHA-256, SHA-384, SHA-512.

Fokozott biztonságú elektronikus aláírás esetén:

- RSA algoritmus legalább 1024 bit kulcshosszal, és az alábbi lenyomatoló algoritmusok egyikével [PKCS#1.5-nek megfelelően]: MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512.

Az eSign Toolkit v2.2.2-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, NMHH 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

Ez a csomag a **CPV – Alap** csomagtól függ. Aláírási információk, XML aláírás feldolgozására és egy aláírás ellenőrzésekor a nyilvános kulcs használatára tartalmaz funkciókat.
További részletek: PKI aláírás létrehozás csomagnál.

2.4.4 Tanúsítvány visszavonási lista (CRL) érvényesség ellenőrzése csomag

Ez a csomag lehetővé teszi, hogy az eSign Toolkit v2.2.2- 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.

2.4.5 Valós idejű tanúsítvány állapot protokoll (OCSP) kliens csomag

Ez a csomag a **CPV – Alap** csomagtól függ. OCSP kérést állít elő és OCSP választ ellenőriz az RFC 2560-nak megfelelően.

2.4.6 Időbélyeg kérése és ellenőrzése csomag

Ez a csomag lehetővé teszi, hogy az eSign Toolkit v2.2.2 Időbélyeget kérjen egy időbélyegzés-szolgáltatótól, illetve ellenőrizze a kapott választ az RFC 3161-nek megfelelően.

2.5 Garanciális követelmények

Az eSign Toolkit v2.2.2 értékelésre vonatkozó garanciakövetelménye: MIBÉTS fokozott (megfelel a CC EAL3-nak).

3 Az eSign Toolkit v2.2.2 biztonsági környezete

3.1 A biztonságos használattal kapcsolatos feltételezések

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 eSign Toolkit v2.2.2-t megfelelően telepítik és konfigurálják.
3	**AE.Crypto_Module**	Az eSign Toolkit v2.2.2 által meghívott kriptográfiai funkciók (például OpenSSL) megbízhatóan valósítják meg az eSign Toolkit v2.2.2 által hívott, kriptográfiai funkciókat. Minősített elektronikus aláírás létrehozása esetén az eSign Toolkit v2.2.2 környezete tartalmaz egy (vagy több) NMHH által nyilvántartott, tanúsított BALE-t, mely tárolja és védi az aláíró magánkulcsát, illetve végrehajtja a digitális aláírást.
4	**AE.Physical_Protection**	A fejlesztői környezetben az eSign Toolkit v2.2.2 függvény-gyűjtemény védett a jogosulatlan fizikai hozzáféréssel szemben.
5	**AE.PKI_Info**	A tanúsítvány és tanúsítvány visszavonási információk az eSign Toolkit v2.2.2 rendelkezésére állnak.
6	**AE.Time**	A környezet GMT formában és a megkívánt pontossággal gondoskodik a pontos rendszeridőről.
7	**AE.TimeStamp**	A környezet biztosítja az időbélyegzés szolgáltatóhoz való hozzáférést

3.1 táblázat – Feltételezések az IT környezetre

3.2 Általános biztonsági fenyegetések

Ez az alfejezet az eSign Toolkit v2.2.2-t fenyegető általános veszélyeket azonosítja. A támadott érték a értékelés tárgyán valamilyen formában áthaladó információ. Általánosságban a veszély forrásai az alábbiak lehetnek (de nem kizárólagosan):

1) az eSign Toolkit v2.2.2-hoz hozzáférő olyan egyének, akik „átlagos" szakértelemmel, kevés erőforrással bírnak és közepes motiváció jellemzi őket; vagy
2) az eSign Toolkit v2.2.2 hibája.

Sor-szám	Veszély megnevezése	Veszély leírása
1	**T.Attack**	Az eSign Toolkit v2.2.2 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 az eSign Toolkit v2.2.2 biztonsági funkcióinak kikerülése és az eSign Toolkit v2.2.2 értékekhez való jogosulatlan hozzáférés megszerzése érdekében.
3	**T.Imperson**	Jogosulatlan egyed megszemélyesíthet egy jogosult eSign Toolkit v2.2.2 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 az eSign Toolkit v2.2.2-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.

3.2 táblázat – Alapvető biztonsági fenyegetések

3.3 Csomagokhoz kapcsolódó biztonsági fenyegetések

3.3.1 Tanúsítási útvonal érvényesség ellenőrzése – Alap csomag

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

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 táblázat– A "tanúsítási útvonal érvényesség ellenőrzése – alap" csomagot érintő veszélyek

3.3.2 PKI aláírás létrehozás csomag

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

Sorszám	Veszély megnevezése	Veszély leírása
1	**T.Clueless_PKI_Sig**	A felhasználó jelzés hiányában csak helytelen tanúsítványokat próbál ki az aláírás során.

3.4 táblázat – A PKI aláírás generálási csomaggal kapcsolatos veszélyek

3.3.3 PKI aláírás ellenőrzés csomag

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

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.

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

3.3.4 CRL érvényesség ellenőrzése csomag

Az alábbi veszélyek a "CRL érvényesség ellenőrzése" csomagra vonatkoznak.

Sorszám	Veszély megnevezése	Veszély leírása
1	**T.Replay_Revoc_Info_CRL**	A felhasználó elfogadhat 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 elfogadhat egy visszavont tanúsítványt, vagy elutasíthat egy érvényeset.

3.6 táblázat – A CRL érvényességi csomaggal kapcsolatos veszélyek

3.3.5 OCSP kliens csomag

Az alábbi veszélyek az "OCSP kliens" csomagra vonatkoznak.

Sorszám	Veszély megnevezése	Veszély leírása
1	**T.DOS_OCSP**	Az OCSP válasz vagy az OCSP szolgáltatáshoz való hozzáférés elérhetetlenné válik és emiatt a rendszer elveszíti a rendelkezésre állását.
2	**T.Replay_OCSP_Info**	A felhasználó elfogadhat egy régi OCSP választ, ami egy már visszavont tanúsítvány elfogadását eredményezheti.
3	**T.Wrong_OCSP_Info**	A felhasználó elfogadhat egy visszavont tanúsítványt vagy visszautasíthat egy érvényes tanúsítványt, egy rossz OCSP válasz miatt.

3.7 táblázat – Az OCSP kliens csomaggal kapcsolatos veszélyek

3.3.6 Időbélyeg kérése és ellenőrzése csomag

Az alábbi veszélyek az "Időbélyeg kérése és ellenőrzése" csomagra vonatkoznak.

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

3.8 táblázat – Az időbélyeg kéréssel és ellenőrzéssel kapcsolatos veszélyek

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

4.1 A TOE-re vonatkozó általános biztonsági célok

Az alábbiakban felsorolt biztonsági célok a jelen biztonsági előirányzat alapját képező PKE PP-ből származnak, és minden, a PP-n családon alapuló ST-ben szerepeltetni kell ezeket. Azonban az alapul szolgáló védelmi profil család megengedi ezen biztonsági célok IT környezet általi kielégítését is, ezért ezeket „OE." előtaggal jelöljük.
Ezen biztonsági célok IT környezeti célként való felvételét indokolja az eSign Toolkit v2.2.2 termék típusa, a fejlesztői könyvtár jelleg. Az eSign Toolkit v2.2.2 az alá, illetve a fölé épülő IT környezetre alapoz az alábbi általános biztonsági célok teljesítése érdekében.

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 NMHH 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.
19	OE.Time	A környezetnek hozzáférést kell biztosítania a pontos időhöz, megkívánt pontossággal, GMT formára alakítva.
20	OE.TimeStamp	A környezetnek biztosítania kell az időbélyegzés szolgáltatóhoz való hozzáférést.

4.1 táblázat – Az eSign Toolkit v2.2.2 informatikai környezete által teljesítendő biztonsági célok

4.2 A csomagokra vonatkozó biztonsági célok

4.2.1 Tanúsítási útvonal érvényességének ellenőrzése – Alap csomag

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 táblázat – Biztonsági célok a CPV – Alap csomag esetén

4.2.2 PKI aláírás létrehozási csomag

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.

4.3 táblázat – Biztonsági célok PKI aláírás létrehozási csomag esetén

4.2.3 PKI aláírás ellenőrzési csomag

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.

4.4 táblázat– Biztonsági célok a PKI aláírás ellenőrzési csomag esetén

4.2.4 CRL érvényesség ellenőrzése csomag

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.

4.5 táblázat – Biztonsági célok a CRL érvényesség ellenőrzése csomag esetén

4.2.5 OCSP kliens csomag csomag

Sorszám	Cél megnevezése	Cél leírása
1	O.Accurate_OCSP_lnfo	A TSF csak pontos OCSP választ fogad el.
2	O.Auth_OCSP_Info	A TSF a visszavonási információkat csak jogosult OCSP forrásból fogadja el.
3	O.Fresh_OCSP_lnfo	A TSF csak megfelelően aktuális visszavonási információkat fogad el az OCSP tranzakciók esetén.

4.6 táblázat – Biztonsági célok az OCSP kliens csomag esetén

4.2.6 Időbélyeg kérése és ellenőrzése csomag

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.

4.7 táblázat – Biztonsági célok az időbélyeg kérése és ellenőrzése csomag esetén

5. IT biztonsági követelmények

Ez a fejezet az eSign Toolkit v2.2.2 funkcionális és garanciális biztonsági követelményeit írja le. A követelmények a CC 2. és 3. részéből származnak, illetve a 2. rész kiterjesztései. A jelölések a CC-nek megfelelnek.

Az 5.1 táblázat összesíti a biztonsági előirányzat összes funkcionális követelményét.

Követelmény	**2. részből származó vagy kiterjesztett**
FDP_ACC.1	2. rész
FDP_ACF.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_SIG.1	Kiterjesztett 2. rész
FDP_ETC_SIG.1	Kiterjesztett 2. rész
FDP_ITC_PKI_INF.1	Kiterjesztett 2. rész
FDP_ITC_SIG.1	Kiterjesztett 2. rész
FDP_DAU_TSP.1	Kiterjesztett 2. rész
FDP_DAU_OCS.1	Kiterjesztett 2. rész

5.1 táblázat– Kiterjesztett 2. vagy 3. rész követelmények

Az 5.2 táblázat csomagonkénti bontásban adja meg a funkcionális követelményeket.

Alap/csomag	**#**	**Követelmények**	**2.kötet vagy kiterjesztése**
Alap	1	FDP_ACC.1	2. kötet
	2	FDP_ACF.1	2. kötet
	3	FIA_AFL.1	2. kötet
	4	FIA_ATD.1	2. kötet
	5	FIA_UAU.1	2. kötet
	6	FIA_UAU.7	2. kötet
	7	FIA_UID.1	2. kötet
	8	FMT_MSA.1	2. kötet
	9	FMT_MSA.3	2. kötet
	10	FMT_MTD.1	2. kötet
	11	FMT_SMF.1	2. kötet
	12	FMT_SMR.2	2. kötet
	13	FPT_RVM.1	2. kötet
	14	FPT_SEP.1	2. kötet
Tanúsítási útvonal érvényesítése (CPV) - Alap	1	FDP_CPD.1	2. kötet kiterjesztése
	2	FDP_DAU_CPV_INI.1	2. kötet kiterjesztése
	3	FDP_DAU_CPV_CER.1	2. kötet kiterjesztése
	4	FDP_DAU_CPV_CER.2	2. kötet kiterjesztése
	5	FDP_DAU_CPV_OUT.1	2. kötet kiterjesztése
PKI aláírás készítés	1	FDP_ETC_SIG.1	2. kötet kiterjesztése
PKI aláírás ellenőrzés	1	FDP_ITC_SIG.1	2. kötet kiterjesztése
	2	FDP_DAU_SIG.1	2. kötet kiterjesztése
Tanúsítvány visszavonási lista érvényesítés	1	FDP_DAU_CRL.1	2. kötet kiterjesztése
Időbélyeg kliens	1	FDP_DAU_TSP.1	2. kötet kiterjesztése
OCSP kliens	1	FDP_DAU_OCS.1	2. kötet kiterjesztése

5.2 táblázat– Az egyes csomagokhoz tartozó követelmények

5.1 A TOE környezet által teljesítendő általános funkcionális biztonsági követelmények

Az 5.3–as 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 eSign Toolkit v2.2.2 IT környezete biztosítja, de egyes funkciókat maga az eSign Toolkit v2.2.2 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 eSign Toolkit v2.2.2 fejlesztői könyvtár jellege miatt azonban az általános követelmények némelyike TOE hatáskörbe esik, ezeket alkalmazási megjegyzésben jelezzük.

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	TSF adatok kezelése
11	FMT_SMF.1	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	PKI információk importálása a TSF-en kívülről
16	FCS_CRM_FPS.1	Kriptográfiai modulok
17	FPT_STM.1	Megbízható időbélyegek

5.3 táblázat – Az eSign Toolkit v2.2.2 IT környezetének általános funkcionális biztonsági követelményeinek készlete

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 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.

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

FDP_ACF.1.4 A 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 válasz**

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 és OCSP lekérdezés).**

Függések: nincsenek.

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, a TSF-nek a következőket kell tennie: **a magánkulcs tároló eszköz által specifikált esemény (szoftveres magánkulcs tároló eszköz esetén fájl törlése, BALE 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** 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 A TSF-nek lehetővé kell tennie a felhasználó nevében végrehajtandó alábbi tevékenységeket: **a TOE-t hívó alkalmazás által megadható paraméterek továbbítását (alkalmazható magánkulcs tároló eszköz paraméterei)**, mielőtt a felhasználó azonosításra kerül.

FIA_UID.1.2 A TSF 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
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_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_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 Az **IT környezet TSF-nek** képesnek kell lennie az alábbi biztonsági menedzsment funkciók végrehajtására:

- **az aláíró hitelesítő adat cseréje PEM kulcstároló fájl esetén.**

FMT_MTD.1/2 A TSF adatok kezelése
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FMT_MTD.1.1 Az **IT környezet TSF-nek** az **aláíróra** kell korlátoznia a **PEM-es kulcstároló eszközben tárolt magánkulcshoz való hozzáférést biztosító aláírói hitelesítő adat (PIN kód) módosításának** képességét.

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 **NMHH 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 Az **IT környezet TSF-nek** érvényre kell juttatnia a szétválasztást a szubjektumok biztonsági tartománya között a TSC-ben.

Függések: nincsenek.

5.1.7 Funkcióerősségre vonatkozó követelmény

Az eSign Toolkit v2.2.2 nem tartalmaz funkcióerősségre vonatkozó követelményt, mert a hatáskörén belül nincsenek valószínűségi vagy permutációs mechanizmusok.

5.2. A TOE által teljesítendő, az egyes csomagokra vonatkozó funkcionális biztonsági követelmények

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

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	
OCSP kliens	FDP_DAU_OCS.1	Tanúsítási útvonal érvényesség ellenőrzése – Alap
Tanúsítvány visszavonási lista érvényesség ellenőrzése	FDP_DAU_CRL.1	Nincs
Kiegészítő csomag		
Időbélyeg kérése és ellenőrzése	FDP_DAU_TSP.1	Tanúsítási útvonal érvényesség ellenőrzése (CPV) – Alap

5.4 táblázat – A csomagokban szereplő funkcionális biztonsági követelmények összegzése

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 5280-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);**

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.**

FDP_ETC_SIG.1.3 A TSF-nek explicit módon le kell tiltania az aláírás létrehozását az alábbi feltételek esetén:
- **aláírói hitelesítő adat sikertelen megadása;**
- **nulla hosszúságú dokumentum megadása aláírásra.**

Függések: FCS_COP.1 Kriptográfiai műveletek

Alkalmazási megjegyzések:
1. Az eSign Toolkit v2.2.2 által előállított aláírás formátumok az alábbiak: XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL, XAdES-A, CMS.
2. Az aláírói hitelesítő adat felhasználó általi megadását a TOE fölé épülő IT környezethez tartozó alkalmazás vezérli, a TOE paraméterként kapja azt.

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.**

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:

a) **alany nyilvános kulcs algoritmusa,**
b) **alany nyilvános kulcsa,**
c) **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:

d) **minősített elektronikus aláírás esetén a `keyUsage` kiterjesztésben csak a `nonRepudiation` bit van beállítva;**
e) **minősített elektronikus aláírás esetén az aláíró tanúsítványában a kötelező qcStatements kiterjesztés meglétének ellenőrzése szükséges;**
f) **fokozott biztonsági aláírás esetén a `keyUsage` kiterjesztésben a `nonRepudiation` bit mellett csak a digSig bit lehet opcionálisan beállítva;**
g) **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 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.

5.2.4.1 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 (megadott könyvtár),**
- **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_CRL.1.7 A TSF-nek ellenőriznie kell, hogy a CRL megfelel-e az alábbi mértékadó útmutatóban definiált szabályoknak:
- **RFC 5280.**

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

5.2.5 OCSP kliens csomag

Ez a csomag a valós idejű tanúsítvány állapot protokoll (OCSP) kéréseket és az OCSP válaszok ellenőrzését teszi lehetővé. Az OCSP válaszadóra, egy megbízható legfelső szintű hitelesítés szolgáltató (CA) vagy egy OCSP válaszok aláírására jogosult végentitás használatát engedi meg. Az OCSP kliens csomag a tanúsítási útvonal érvényességének ellenőrzésével bírálja el az OCSP válasz aláírására szóló jogosultságot. Ez a csomag így függ a Tanúsítási útvonal érvényesítése (CPV) - Alap csomagtól.

5.2.5.1 Felhasználói adat védelem (FDP osztály)

FDP_DAU_OCS.1 Alap OCSP ellenőrzés

Hierarchikus kapcsolat: nincs más komponenshez.

FDP_DAU_OCS.1.1 A TSF-nek a PKIX RFC 2560-nek megfelelő formában kell összeállítania az OCSP kérést.

FDP_DAU_OCS.1.2 Az OCSP kérésnek tartalmaznia kell a következő kiterjesztéseket: n**once.**

FDP_DAU_OCS.1.3 A TSF-nek az OCSP választ aláíró tanúsítványt az OCSP válaszból kell megismernie.

FDP_DAU_OCS.1.4 A TSF-nek a következő további funkciókat kell végrehajtania: **az OCSP válaszadó megbízhatóságának megállapítása a Tanúsítási útvonal érvényesítése (CPV) - Alap csomag felhasználásával.**

FDP_DAU_OCS.1.5 A TSF-nek ellenőriznie kell az OCSP válaszon levő aláírást a Tanúsítási útvonal érvényesítése (CPV) – Alap csomag kimenetéből származó nyilvános kulccsal.

FDP_DAU_OCS.1.6 A TSF-nek ellenőriznie kell, hogy ha az OCSP válaszadó tanúsítványa tartalmazza az extendedKeyUsage kiterjesztést, akkor a kiterjesztés tartalmazza-e az id-kp-OCSPSigning OID-t vagy az anyExtendedKeyUsage OID-t.

FDP_DAU_OCS.1.7 A TSF-nek össze kell hasonlítania az OCSP válaszból a responderID-t az OCSP válaszadó tanúsítványában található megfelelő információval.

FDP_DAU_OCS.1.8 A TSF-nek az OCSP kérésben található certID-t össze kell hasonlítania az OCSP válasz singleResponse-ban található certID-vel.

FDP_DAU_OCS.1.9 A TSF-nek aktuálisnak kell elfogadnia az OCSP választ, amennyiben az OCSP válaszban lévő időpont későbbi, mint a kérésben szereplő időpont.

FDP_DAU_OCS.1.10 A TSF-nek vissza kell utasítania az OCSP választ, ha az olyan kritikus kiterjesztést tartalmaz, amelyet a TSF nem dolgoz fel.

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

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

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

PKIX RFC 3161

alábbi formátumnak megfelelően:

TimeStampReq

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

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

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

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

FDP_DAU_TSP.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_TSP.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_TSP.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_TSP.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_TSP.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 fokozott garanciaszint

Jelen biztonsági előirányzat a MIBÉTS fokozott garanciaszintet követeli meg. Valamennyi garanciaösszetevő a CC 3. részéből származik, s az 5.5 táblázat sorolja fel ezeket.

Garanciaösszetevő azonosító	Garanciaösszetevő megnevezés
ACM_SCP.1	TOE CM lefedettsége
ACM_CAP.3	Jogosultságok ellenőrzése
ADO_DEL.1	Szállítási eljárások
ADO_IGS.1	Telepítési, generálási, indítási eljárások
ADV_FSP.1	Informális funkcionális specifikáció
ADV_HLD.2	Biztonságot érvényre juttató magas szintű tervezés
ADV_RCR.1	Informális megfelelőség bemutatása
AGD_ADM.1	Adminisztrátori útmutató
AGD_USR.1	Felhasználói útmutató
ALC_DVS.1	A biztonsági intézkedések azonosítása
ATE_COV.2	A lefedettség elemzése
ATE_DPT.1	Tesztelés: magas szintű terv
ATE_FUN.1	Funkcionális tesztelés
ATE_IND.2	Független tesztelés – mintavétel
AVA_MSU.1	Az útmutatók vizsgálata
AVA_SOF.1	A TOE biztonsági funkciók erősségének értékelése
AVA_VLA.1	Fejlesztői sebezhetőségi elemzés

5.5 táblázat - A MIBÉTS fokozott garanciaszint követelményei

5.3.1 Konfiguráció menedzselés (ACM, Assurance: Configuration Management)

ACM_SCP.1 Az értékelés tárgya konfiguráció kezelés lefedettsége

Fejlesztői feladatok:

ACM_SCP.1.1D A fejlesztőnek konfiguráció kezelés dokumentációt kell készítenie.

A bizonyíték elemek tartalma és bemutatása:

ACM_SCP.1.1C A konfiguráció elemek listájának tartalmaznia kell a következőket: megvalósítási reprezentáció, valamint az ST garanciaösszetevői által megkövetelt értékelői bizonyítékok.

ACM_CAP.3 Jogosultságok ellenőrzése

Fejlesztői feladatok:

ACM_CAP.3.1D A fejlesztőnek meg kell adnia az értékelés tárgya hivatkozást.
ACM_CAP.3.2D A fejlesztőnek egy konfiguráció kezelés rendszert kell használnia.
ACM_CAP.3.3D A fejlesztőnek egy konfiguráció kezelés dokumentációt kell átadnia.

A bizonyíték elemek tartalma és bemutatása:

ACM_CAP.3.1C A TOE minden verziójára egyedi módon kell hivatkozni.
ACM_CAP.3.2C A TOE-t meg kell jelölni ezzel a hivatkozással.
ACM_CAP.3.3C A konfiguráció kezelés dokumentációnak tartalmaznia kell egy konfiguráció listát és egy konfiguráció kezelés tervet.
ACM_CAP.3.4C A konfiguráció listának egyértelműen azonosítania kell a TOE-t alkotó összes konfiguráció elemet.
ACM_CAP.3.5C A konfiguráció listának le kell írnia a TOE-t alkotó összes konfiguráció elemet.
ACM_CAP.3.6C A konfiguráció kezelés dokumentációnak le kell írnia a konfiguráció elemek egyedi azonosításához használt módszert.
ACM_CAP.3.7C A konfiguráció kezelés rendszernek egyedi módon kell azonosítania minden konfiguráció elemet.
ACM_CAP.3.8C A konfiguráció kezelés tervnek le kell írnia a konfiguráció kezelés rendszer használatát.
ACM_CAP.3.9C Bizonyítékoknak kell mutatniuk, hogy a konfiguráció kezelés rendszer a konfiguráció kezelés tervnek megfelelően működik.
ACM_CAP.3.10C A konfiguráció kezelés dokumentációnak bizonyítékot kell szolgáltatnia arra, hogy minden konfiguráció elemet megfelelően kezeltek és kezelnek a konfiguráció kezelés rendszer alapján.
ACM_CAP.3.11C A konfiguráció kezelés rendszernek gondoskodnia kell arról, hogy csak jogosult változtatások történhessenek a konfiguráció elemekben.

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

ADO_DEL.1 Szállítási eljárások

Fejlesztői feladatok:

ADO_DEL.1.1D A fejlesztőnek dokumentálnia kell az értékelés tárgya vagy annak részei felhasználóhoz való szállításának eljárásait.

ADO_DEL.1.2D A fejlesztőnek használnia kell a szállítási eljárásokat.

A bizonyíték elemek tartalma és bemutatása:

ADO_DEL.1.1C A szállítási dokumentációnak le kell írnia minden olyan eljárást, amely a TOE verzióinak felhasználókhoz történő szállítása során a biztonság fenntartásához szükséges.

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 bizonyíték elemek tartalma és bemutatása:

ADO_IGS.1.1C A telepítési, generálási és indítási dokumentációnak le kell írnia a TOE biztonságos telepítéséhez, generálásához és indításához szükséges valamennyi lépést.

5.3.3 Fejlesztés (ADV, Assurance: Development)

ADV_FSP.1 Informális funkcionális specifikáció

Fejlesztői feladatok:

ADV_FSP.1.1D A fejlesztőnek funkcionális specifikációt kell átadnia.

A bizonyíték elemek tartalma és bemutatása:

ADV_FSP.1.1C A funkcionális specifikációnak informális stílusban le kell írnia a TSF-et és annak külső interfészeit.

ADV_FSP.1.2C A funkcionális specifikációnak belső ellentmondásoktól mentesnek kell lennie.

ADV_FSP.1.3C A funkcionális specifikációnak le kell írnia minden külső TSF interfész használatának célját és módját, részletezve a hatásokat, kivételeket és hibaüzeneteket.

ADV_FSP.1.4C A funkcionális specifikációnak teljes mértékben be kell mutatnia a TSF-et.

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 belső ellentmondásoktól mentesnek kell lennie.

ADV_HLD.2.3C A magas szintű tervnek le kell írnia a TSF szerkezetét 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 összes interfészét.

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

ADV_HLD.2.8C A magas szintű tervnek le kell írnia minden TSF alrendszer interfész célját és használati módját, részletezve azok hatását, a kivételeket, illetve a hibaüzeneteket.

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

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 megfelelés elemzésnek be kell mutatnia, hogy az absztraktabb TSF reprezentáció minden lényeges biztonsági funkcionalitását helyesen és teljes mértékben finomítja tovább a kevésbé absztrakt TSF reprezentáció.

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 átadnia.

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 üzemeltetése szempontjából lényeges.

AGD_ADM.1.5C Az adminisztrátori útmutatónak le kell írnia az adminisztrátor ellenőrzése alá tartozó minden biztonsági szempontból fontos paramétert, 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, beleértve a TSF ellenőrzése alá eső egyedek biztonsági tulajdonságainak megváltoztatását is.

AGD_ADM.1.7C Az adminisztrátori útmutatónak ellentmondásoktól mentesnek 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 lényeges.

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 hogyan kell használni a TOE felhasználók számára elérhető biztonsági funkciókat.

AGD_USR.1.3C A felhasználói útmutatónak tartalmaznia kell a felhasználók által elérhető azon 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, beleértve a TOE biztonsági környezetének leírásában található, a felhasználói viselkedésre vonatkozó feltételezésekhez kapcsolódókat is.

AGD_USR.1.5C A felhasználói útmutatónak ellentmondásoktól mentesnek 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 lényeges.

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.

5.3.6 Tesztek (ATE, Assurance: Tests)

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 bizonyíték elemek 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 írniuk a tesztelési forgatókönyvet minden biztonsági funkcióra. A forgatókönyveknek tartalmazniuk kell a tesztek sorrendiségére vonatkozó minden függőséget.

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

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

ATE_COV.2 A teszt lefedettség elemzése

Fejlesztői feladatok:

ATE_COV.2.1D A fejlesztőnek elemzést kell biztosítania a teszt lefedettségről.

A bizonyíték elemek tartalma és bemutatása:

ATE_COV.2.1C A teszt lefedettség elemzésének szemléltetnie kell a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikációban leírt TSF közötti megfelelést.

ATE_COV.2.2C A teszt lefedettség elemzésének szemléltetnie kell, hogy a funkcionális specifikációban leírt TSF és a tesztelési dokumentációban azonosított tesztek közötti megfelelés teljes.

ATE_DPT.1 A magas szintű terv tesztelése

Fejlesztői feladatok:

ATE_DPT.1.1D A fejlesztőnek teszt mélység elemzést kell biztosítania.

A bizonyíték elemek tartalma és bemutatása:

ATE_DPT.1.1C A teszt mélység elemzésnek be kell mutatnia, hogy a tesztelési dokumentációban azonosított tesztek elegendőek a biztonsági funkciók magas szintű tervnek megfelelő működésének a bemutatásához.

ATE_IND.2 Független tesztelés - mintavételezés

Fejlesztői feladatok:

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

A bizonyíték elemek tartalma és bemutatása:

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

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

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

AVA_MSU.1 Az útmutatók vizsgálata

Fejlesztői feladatok:

AVA_MSU.1.1D A fejlesztőnek el kell készítenie az útmutató dokumentációkat.

A bizonyíték elemek tartalma és bemutatása:

AVA_MSU.1.1C 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.1.2C Az útmutatónak teljesnek, egyértelműnek, ellentmondás mentesnek és megalapozottnak kell lennie.

AVA_MSU.1.3C Az útmutatónak fel kell sorolnia minden feltételezést a tervezett környezetről.

AVA_MSU.1.4C Az útmutatónak számba kell vennie a külső biztonsági intézkedésekkel kapcsolatos minden követelményt (beleértve a külső eljárásbeli, fizikai és személyi intézkedéseket is).

AVA_SOF.1 Az értékelés tárgya biztonsági funkcióinak erősségértékelése

Fejlesztői feladatok:

AVA_SOF.1.1D A fejlesztőnek az ST-ben azonosított minden funkcióerősségi nyilatkozattal rendelkező mechanizmusra biztonsági funkcióerősség elemzést kell végeznie.

A bizonyíték elemek tartalma és bemutatása:

AVA_SOF.1.1C Minden TOE biztonsági funkcióerősségi nyilatkozattal rendelkező mechanizmus esetén az elemzésnek meg kell mutatnia, hogy a funkció erőssége azonos vagy magasabb szintű annál, mint amely a PP-ben / ST-ben minimális erősségi szintként szerepel.

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

AVA_VLA.1 Fejlesztői sebezhetőség vizsgálat

Fejlesztői feladatok:

AVA_VLA.1.1D 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.1.2D A fejlesztőnek dokumentálnia kell az azonosított sebezhetőségek kiküszöbölését (sebezhetőségi elemzés dokumentáció).

A bizonyíték elemek tartalma és bemutatása:

AVA_VLA.1.1C A sebezhetőségi elemzés dokumentációnak le kell írnia azt a fejlesztői bizonyítékokra végrehajtott elemzést, mely olyan nyilvánvaló módokat keres, amelyekkel egy felhasználó megsértheti a TOE biztonsági szabályzatát (TSP-t).

AVA_VLA.1.2C A sebezhetőségi elemzés dokumentációnak jellemeznie kell a nyilvánvaló sebezhetőségeket.

AVA_VLA.1.3C A sebezhetőségi elemzés dokumentációnak minden nyilvánvaló sebezhetőségre ki kell mutatnia, hogy az nem kihasználható a TOE tervezett környezetében.

6 TOE összefoglaló előírás

A TOE összefoglaló előírás az eSign Toolkit v2.2.2 által teljesítendő biztonsági követelményeket teljesítő biztonsági funkciókat tartalmazza. Leírja az eSign Toolkit v2.2.2 összes biztonsági funkcióját és garanciális intézkedését, amelyek az 5.2 alfejezetben specifikált biztonsági követelmények kielégítéséhez járulnak hozzá.

6.1 Az eSign Toolkit v2.2.2 biztonsági funkciói

Az eSign Toolkit v2.2.2-nek az alábbi biztonsági funkciói vannak:

- BF1 Aláírás létrehozása
- BF2 Aláírás ellenőrzése
- BF3 Időbélyeg kérés
- BF4 Időbélyeg ellenőrzés
- BF5 Tanúsítvány útvonal felépítése és érvényesség ellenőrzése
- BF6 Szabványos aláírás formátumú aláírás
- BF7 működési paraméterek beállítása

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 eSign Toolkit v2.2.2 lehetőséget biztosít fokozott biztonságú és minősített elektronikus aláírások létrehozására. A magánkulcsot tokenből (PKCS#11 felületen keresztül), fokozott biztonságú aláírások esetén fájlból is (PEM kulcsfájlból) képes kezelni.

A magánkulcs közvetlen aktivizálása előtt az eSign Toolkit v2.2.2 a paraméterként kapott aláíró hitelesítő adatot használja az aláíró hitelesítéséhez.

Minősített elektronikus aláírás létrehozása esetén az eSign Toolkit v2.2.2 kommunikációt kezdeményez az aláírás létrehozását ténylegesen végző BALE-vel. Az aláíró által kiválasztott tanúsítványhoz tartozó magánkulccsal és az ennek megfelelő algoritmussal (ami az eSign Toolkit v2.2.2 esetén az RSA algoritmus legalább 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 PEM kulcsfájlban tárolt magánkulcsot, és az RSA algoritmus és legalább 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: ETSI TS 101 733 v1.6.3 (CAdES), ETSI TS 101903 v1.2.2 (XAdES).

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 lenyomatoló algoritmus:

- fokozott biztonságú aláírások esetén: MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512,
- minősített aláírások esetén: SHA-224, SHA-256, SHA-384, SHA-512.

Megengedett dokumentum formátumok:

Az eSign Toolkit v2.2.2 a következő dokumentum formátumok aláírását engedi meg: TXT/XML.

Támogatott aláírás formátumok:

A funkció által támogatott elektronikus aláírás formátumok: XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL, XAdES-A, CMS.

BF2 Elektronikus aláírás ellenőrzése

Ez a biztonsági funkció valósítja meg az elektronikus aláírás ellenőrzését az aláíró tanúsítványának felhasználásával.

Az aláírás ellenőrzés folyamata három lépésből áll: első lépésben a funkció megnézi, hogy kapcsolódik-e időbélyeg az aláíráshoz. Amennyiben nem, akkor végrehajtja a **BF3 Időbélyeg kérés** és a **BF4 Időbélyeg ellenőrzés** biztonsági funkciókat. Az ellenőrzés második lépéseként az aláírás érvényességének megállapításához szükséges információk összegyűjtését végzi, amennyiben ez még nem áll rendelkezésre. Ezt a **BF5 Tanúsítványlánc felépítése és érvényesség ellenőrzése** biztonsági funkció végzi el. Végül a harmadik lépésben kerül sor az elektronikus aláírás ellenőrzésére.

Az aláírás ellenőrzés által visszaadott értékekből a meghívó alkalmazás dönthet az alábbi három lehetséges állapot közül:

- 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.

A funkció által ellenőrizni képes elektronikus aláírás formátumok: XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL, XAdES-A, CMS. Az alábbi szabványoknak megfelelőséget is képes ellenőrizni: XAdES v1.2.2, MELASZ-ready v2.0.

BF3 Időbélyeg kérés

Az eSign Toolkit v2.2.2 biztosítja az időbélyeg kérés képességét**.** Az RFC 3161-ben specifikáltaknak megfelelően összeállítja az időbélyeg kérést a hash értékkel, és elküldi a külső időbélyeg szolgáltatóhoz.

BF4 Időbélyeg ellenőrzés

Az eSign Toolkit v2.2.2 a szolgáltatótól kapott időbélyeg választ importálja, és elvégzi a szükséges ellenőrzéseket: ellenőrzi a válasz státuszt, azt, hogy érvényes-e az időbélyegen lévő aláírás, valamint ellenőrzi az időbélyeg aláírásához használt tanúsítvány érvényességét.

BF5 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 eSign Toolkit v2.2.2 az IT környezet által sértetlenségében megvédett konfigurációs fájlból vagy a registry-ből 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 eSign Toolkit v2.2.2 betöltésekor lefut egy inicializáló rutin, amely elvégzi az elérési helyek inicializálását.
A konfigurációs fájl vagy a registry, valamint a tanúsítványokat és CRL-eket tároló könyvtár feltöltése kívül esik a TOE hatókörén.
Az eSign Toolkit v2.2.2 az érvényesség ellenőrzés során a végtanúsítványra **visszavonási információkat (CRL) gyűjt** be, amennyiben a CRL-eket tároló könyvtár nem tartalmazza azt. A paraméterezhető türelmi idő letelte után a TOE-t meghívó alkalmazásnak kell megismételnie a visszavonási információk lekérését, hogy az aláírás érvényességének ellenőrzése a legfrissebb CRL-ek alapján történjen meg. A TOE 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. A tanúsítványlánc felépítésekor azt is megvizsgálja, hogy a kibocsátott tanúsítványok érvényességi ideje beleesik-e a kibocsátó tanúsítvány érvényességi idejébe (kagyló modell). Azt is megvizsgálja, hogy szerepel-e a visszavonási listán a tanúsítvány, és amennyiben igen, akkor az időbélyeg által meghatározott időpontban visszavont állapotú volt-e.

BF6 Szabványos aláírás formátumú aláírás

Ez a biztonsági funkció az alábbi szabványos aláírás formátumokat támogatja:

- aláírás létrehozásakor:
  - XAdES v1.2.2 szerinti XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL és XAdES-A,
  - MELASZ-ready v2.0 szerinti XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL és XAdES-A,
  - RFC 3852 szerinti CMS.

- aláírás ellenőrzésekor:
  - XAdES v1.2.2 szerinti XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL és XAdES-A,
  - MELASZ-ready v2.0 szerinti XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL és XAdES-A,
  - RFC 3852 szerinti CMS.

BF7 Működési paraméterek beállítása

Ez a biztonsági funkció meghatározza a konfigurációs paraméterek elérhetőségét a Windows Registry gyűjtő és elérési út értékeinek beállításával, vagy egy XML konfigurációs fájl kijelölésével.

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 eSign Toolkit v2.2.2 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;
- útmutató;
- konfiguráció menedzselés dokumentáció;
- teszt dokumentáció.

Az eSign Toolkit v2.2.2 fejlesztése egy gépen történt, ennek védelme biztosítja, hogy csak engedélyezett módosítások történhessenek a fejlesztés alatt álló szoftveren. Az eSign Toolkit v2.2.2 termékhez verziószámot rendelnek, az értékelés során egyértelműen látható, hogy mely verzió értékelését végzik az értékelők.
A konfiguráció kezelési tervről készült leírás:
"eSign Toolkit v2.2.2 – A konfiguráció kezelés dokumentációja"

6.2.2 Kiszállítás és működtetés

Az eSign Toolkit elsődleges felhasználója a termék gyártója, aki alkalmazásokat fejleszt a függvény-készletből. Külön szerződéses kapcsolat esetén a meghívó alkalmazásokat más cég is fejlesztheti, de ezekben az esetekben is az eSign Toolkit függvény-készlet szállítását és átadását a termék gyártója végzi.

6.2.3 Fejlesztés

A "NOREGPKI2.DLL – Fejlesztői útmutató" című dokumentum egyszerre képezi a TOE informális funkcionális specifikációját (mely megfogalmazza az eSign Toolkit v2.2.2 fő biztonsági funkcióit, a külső interfészeket, ezek célját), valamint a magas szintű tervet (mely informális eszközökkel leírja a fejlesztés alatt álló rendszer fő elemeit, a közöttük lévő kapcsolatokat).

6.2.4 Útmutató dokumentumok

A "NOREGPKI2.DLL – Fejlesztői útmutató" című dokumentum a TOE felhasználói (alkalmazás fejlesztők) számára készült. Minden olyan ismeretet tartalmaz, mely a függvénygyűjtemény biztonságos meghívásához szükséges.

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 "eSign Toolkit v2.2.2 – A fejlesztési biztonság dokumentációja" leírás tartalmazza a fejlesztők által az értékelés tárgya fejlesztése során alkalmazott szabályok leírását.

6.2.6 Tesztelés

Az eSign Toolkit v2.2.2 teszteléséhez az alábbi, teszteléssel kapcsolatos dokumentumok készültek:
"eSign Toolkit v2.2.2 – Tesztelési dokumentáció"

"eSign Toolkit v2.2.2 – Teszt lefedettség elemzés"

"eSign Toolkit v2.2.2 – Teszt mélység elemzés"

6.2.7 Sebezhetőségek felmérése

A fejlesztő sebezhetőségi elemzését az alábbi dokumentum tartalmazza:
"eSign Toolkit v2.2.2 - Sebezhetőség elemzés"

7 PP megfelelőség

Jelen Biztonsági előirányzat a PKE PP alapján készült, de az eSign Toolkit v2.2.2 specifikus biztonsági jellemzői miatt PP megfelelőségi nyilatkozatot nem tesz.

8 Indoklások

Ez a fejezet tartalmazza azon indoklásokat, melyek megmutatják, hogy az eSign Toolkit v2.2.2 valóban kivédi a számításba vett veszélyeket és teljesíti a biztonsági céljait. Mivel az eSign Toolkit v2.2.2 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 az ALE/BALE eszköz és annak biztonságos használatát biztosító programok.

8.1 A biztonsági célok indoklása

8.1.1 Az általános és a környezeti biztonsági célok indoklása

A 8.1 táblázat az általános feltételezéseket és veszélyeket képezi le a biztonsági célokra, 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 célhoz tartozik legalább egy veszély vagy feltételezés.

Feltételezés/veszély	**Célok**
AE.Authorized_Users	OE.Authorized_Users
AE.Configuration	OE.Configuration
AE.Crypto_Module	OE.Crypto
AE.Physical_Protection	OE.Physical_Security
AE.PKI_Info	OE.PKI_Info
AE.Time	OE.Time
AE.TimeStamp	OE.TimeStamp
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

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

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 (például OpenSSL), melyek megbízhatónak tekinthetők a TOE által hívott, kriptográfiai funkciók megvalósítása terén. Minősített elektronikus aláírás létrehozása esetén a TOE környezetéről feltételezés, hogy tartalmaz legalább egy NMHH 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 NMHH 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.

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.TimeStamp**: a környezetnek biztosítania kell 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 cél visszavezethető egy feltételezésre vagy veszélyre. Az indoklás az előző, itt már nem ismételjük meg.

Cél	**Feltételezés/veszély**
OE.Authorized_Users	AE.Authorized_Users
OE.Configuration	AE.Configuration
OE.Crypto	AE.Crypto_Module
OE.PKI_Info	AE.PKI_Info
OE.Physical_Security	AE.Physical_Protection
OE.Time	AE.Time
OE.TimeStamp	AE.TimeStamp
OE.DAC	T.Attack, T.Modify, T.Private_key
OE.Invoke	T.Bypass
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

8.2 táblázat – Az alap TOE és környezeti célok leképezése veszélyekre és feltételezésekre

8.1.2 A biztonsági célok indoklása a csomagokra

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.

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

8.3 táblázat – A veszélyek leképezése célokra a CPV – Alapcsomag esetén

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.

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

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

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.

Sorszám	Veszély	Célok
1	T.Clueless_PKI_Sig	O.Give_Sig_Hints

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

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.

Sorszám	Célok	Veszély
1	O.Give_Sig_Hints	T.Clueless_PKI_Sig

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

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.

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

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

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.

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

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

8.1.2.4 A CRL ellenőrzés csomag biztonsági céljainak indoklása

Először a veszélyek leképezését tekintjük át a 8.9 táblázat és az alatta olvasható magyarázó szöveg segítségével, majd a 8.10 táblázat a célokat vezeti vissza a veszélyekre.

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

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

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.

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

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

8.1.2.5 Az OCSP kliens csomag biztonsági céljainak indoklása

Először a veszélyek leképezését tekintjük át a 8.11 táblázat és az alatta olvasható magyarázó szöveg segítségével, majd a 8.12 táblázat a célokat vezeti vissza a veszélyekre.

Sorszám	Veszély	Célok
1	T.DOS_OCSP	O.Fresh_OCSP_Info
2	T.Replay_OCSP_lnfo	O.Accurate_OCSP_Info O.Auth_OCSP_Info
3	T.Wrong_OCSP_lnfo	O.Accurate_OCSP_Info

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

T.DOS_OCSP: Az OCSP válasz vagy az OCSP szolgáltatáshoz való hozzáférés elérhetetlenné válik és emiatt a rendszer elveszíti a rendelkezésre állását. A veszélyből származtatott biztonsági cél:

- **O.Fresh_OCSP_Info**: A TSF csak megfelelően aktuális visszavonási információkat fogad el az OCSP tranzakciók esetén.

T.Replay_OCSP_lnfo: A felhasználó elfogadhat egy régi OCSP választ, ami egy már visszavont tanúsítvány elfogadását eredményezheti. A veszélyből származtatott biztonsági cél:

- **O.Accurate_OCSP_Info**: A TSF csak pontos OCSP választ fogad el
- **O.Auth_OCSP_Info**: A TSF a visszavonási információkat csak jogosult OCSP forrásból fogadja el.

T.Wrong_OCSP_lnfo: A felhasználó elfogadhat egy visszavont tanúsítványt vagy visszautasíthat egy érvényes tanúsítványt, egy rossz OCSP válasz miatt. A veszélyből származtatott biztonsági cél:

- **O.Accurate_OCSP_Info**: A TSF csak pontos OCSP választ fogad el.

Sorszám	Célok	Veszély
1	O.Accurate_OCSP_Info	T.Wrong_OCSP_lnfo T.Replay_OCSP_lnfo
2	O.Auth_OCSP_Info	T.Replay_OCSP_lnfo
3	O.Fresh_OCSP_Info	T.DOS_OCSP

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

8.1.2.6 Az időbélyeg kérése és ellenőrzése 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.

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

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

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.

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**

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

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 8.15 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.

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/A FDP_ITC_PKI_INF.1/B
19	OE.Time	FPT_STM.1
20	OE.TimeStamp	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 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 OCSP csomag céljainak leképezése		
1	O.Fresh_OCSP_Info	FDP_DAU_OCS.1
2	O.Accurate_OCSP_Info	FDP_DAU_OCS.1
3	O.Auth_OCSP_Info	FDP_DAU_OCS.1
Az időbélyeg kérése és ellenőrzése csomag céljainak leképezése		
1	O.Fresh_TimeStamp_Info	FDP_DAU_TSP.1
2	O.Accurate_TimeStamp_Info	FDP_DAU_TSP.1
3	O.Auth_TimeStamp_Info	FDP_DAU_TSP.1

8.15 táblázat – A biztonsági célok leképezése funkcionális követelményekre

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 NMHH 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 NMHH 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 NMHH 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. A cél megvalósítását biztosító követelmény:

- FDP_ITC_PKI_INF.1, PKI információk importálása a TSF-en kívülről, amely megköveteli, hogy az IT környezetnek lehetővé kell tennie, hogy a tanúsítványok és CRL-ek 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.TimeStamp: a környezetnek biztosítania kell az időbélyegzés szolgáltatóhoz való hozzáférést.
Az AE.TimeStamp-et fedi le, amely feltételezi, hogy a környezet biztosítjal az időbélyegzés szolgáltatóhoz való hozzáférést.

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.

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.

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 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.

8.2.1.6 Az Időbélyeg kérése és ellenőrzése csomag indoklása

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

- FDP_DAU_OCS.1 Alap OCSP ellenőrzés: megköveteli, hogy a TSF csak pontos OCSP választ fogadjon el. A pontosságot ellenőrzések sorozata és szabályok sora határozza meg ezen a 2. rész kiterjesztési követelményen belül.

O.Auth_OCSP_Info: A TSF-nek csak jogosult OCSP szolgáltatótól (OCSP forrásból) szabad OCSPválaszt elfogadnia. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FDP_DAU_OCS.1 Alap OCSP ellenőrzés: megköveteli, hogy a TSF a TOE-t hívó alkalmazás által megjelölt vagy kiválasztott jogos forrástól fogadjon el visszavonási információkat.

O.Fresh_OCSP_Info: A TSF-nek csak friss OCSP válaszokkal szabad dolgoznia. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FDP_DAU_OCS.1 Alap OCSP ellenőrzés: megköveteli, hogy a TSF csak valószerű aktuális OCSP választ fogadjon csak el, az FDP_DAU_OCS.1-ben definiált szabályok sorozata alapján.

8.2.1.7 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_TSP.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_TSP.1, Időbélyeg kérés és ellenőrzés: megköveteli, hogy a TSF a TOE-t hívó alkalmazás által megjelölt vagy kiválasztott jogos forrástól fogadjon el időbélyeg válaszokat.

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

8.2.2 A garanciális követelmények indoklása

Az eSign Toolkit v2.2.2 értékelési garanciaszintje: MIBÉTS fokozott (EAL3). Ez olyan TOE-kre megfelelő választás, amelyek közepes függetlenül garantált biztonságot igényelnek a hagyományos piaci TOE-kre. A MIBÉTS fokozott garanciaszint a biztonsági funkciók elemzése által ad garanciát.
A biztonsági funkciók működésének megértéséhez az alábbiak feldolgozására kerül sor: funkcionális interfész specifikáció, az útmutató leírások, valamint az eSign Toolkit v2.2.2 magas szintű terve.

8.3 A függőségek teljesítésének indoklása

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	Nincs
17	FPT_STM.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)
CRL ellenőrzés csomag		
1	FDP_DAU_CRL.1	FCS_COP.1 (Lásd 2. megjegyzést) FPT_STM.1 (Lásd 1. megjegyzést)
OCSP kliens csomag		
1	FDP_DAU_OCS.1	FCS_COP.1 (Lásd 2. megjegyzést) FPT_STM.1 (Lásd 1. megjegyzést)
Időbélyeg kérés és ellenőrzés csomag		
1	FDP_DAU_TSP.1	FCS_COP.1 (Lásd 2. megjegyzést)

8.16 táblázat – biztonsági követelményeinek leképezése a biztonsági funkciókra

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

A 8.17 táblázat felsorolja az eSign Toolkit v2.2.2 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 Aláírás ellenőrzése	BF3 Időbélyeg kérés	BF4 Időbélyeg ellenőrzés	BF5 Tanúsítási útvonal felépítése és ellenőrzése	BF6 Szabványos formátumú aláírás	BF7 Működési paraméterek beállítása
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**				**X**	
FDP_DAU_SIG.1 Függések: FCS_COP.1 FDP_DAU_CPV_OUT.1		**X**				**X**	
FDP_DAU_OCS.1 Függések: FCS_COP.1 FPT_STM.1			**X**	**X**			
FDP_DAU_CRL.1 Függések: FCS_COP.1 FPT_STM.1					**X**		
FDP_DAU_TSP.1 Függések: FCS_COP.1			**X**	**X**			
FMT_MSA.3 Függések: -							**X**

8.17 táblázat – Funkcionális követelmények közötti függések

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.

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**
CMS	**Cryptogtraphic Message Syntax**	**Kriptográfiai üzenet szintaxis**
EAL	**Evaluation Assurance Level**	**Értékelési garanciaszint** /A CC 3. rész olyan garanciális összetevőiből álló csomag, amely a CC előre meghatározott garanciális skáláján egy szintet képvisel./
PP	**Protection Profile**	**Védelmi profil** /Megvalósítástól független, olyan biztonsági követelményrendszer az értékelés tárgyainak (TOE) egy kategóriájára, amely adott fogyasztói igényeket elégít ki./
SF	**Security Function**	**Biztonsági funkció** /Az értékelés tárgyának 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, valamint a hozzákapcsolódó 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./
XAdES	**XML Advanced Electronic Signatures**	**XML fokozott biztonságú elektronikus aláírás**
XML	**Extensible Markup Language**	**Extensible Markup Language**