XadesMagic
elektronikus aláírás alkalmazás fejlesztőkészlet fokozott biztonságú elektronikus aláíráshoz
v1.0

BIZTONSÁGI ELŐIRÁNYZAT

Verzió:	v1.0
Dátum:	2006. október 08.
Fájl:	XM_ST_v10.pdf
Minősítés:	Nyilvános
Oldalak:	100

Tartalomjegyzék

1. Bevezetés

Ez a rész 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 a 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 a CC jelen értékelésnél irányadó verzióját határozza meg.

1.1 Azonosítás

Cím:	XadesMagic elektronikus aláírás alkalmazás fejlesztőkészlet fokozott biztonságú elektronikus aláíráshoz v1.0 – Biztonsági előirányzat
Az értékelés tárgya:	XadesMagic elektronikus aláírás alkalmazás fejlesztőkészlet
Az értékelés tárgya rövid neve:	XadesMagic v1.0
Értékelési garancia szint:	EAL3
Biztonsági funkcióerősség:	SOF-alap
Verzió szám:	1.0
Dátum:	2006. október 8.
Szerzők:	Székely Márk
Szponzor szervezet:	SDA Stúdió Kft.
Alapot képező védelmi profil:	USMC PKE PP with < Certificate Path Validation (CPV) – Basic, PKI Signature Generation, PKI Signature Verification, PKI Based Entity Authentication, Online Certificate Status Protocol Client, Certificate Revocation List (CRL) Validation Audit Management, Continuous Authentication > at EAL <3> with augmentation
Kiegészítés:	A biztonsági előirányzat kiegészült az „Időbélyeg kérése és ellenőrzése” csomaggal is, amely nem képezi részét az eredeti PKE PP családnak.

1.2 Áttekintés

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

- elektronikus aláírás létrehozása;
- elektronikus aláírás ellenőrzése, a kapcsolódó tanúsítvány útvonal felépítési és érvényesítési szolgáltatásokkal;
- időbélyegzés (kérése és ellenőrzése);
- PKI-alapú felhasználói hitelesítés távoli szolgáltatás elérésénél.

A XadesMagic v1.0 fejlesztőkészlet segítségével alkalmazások széles köre fejleszthető, melyeknél az elektronikus aláírás létrehozása és ellenőrzése alapvető szükséglet.

A jelen biztonsági előirányzat készítésénél figyelembe vettek egy csomag koncepcióra (különböző csomagokból történő moduláris szerkeszthetőségre) épülő, Common Criteria szerint tanúsított védelmi profilt (PKE PP), de ennek való megfelelőségről nincs szó. A biztonsági előirányzat kiegészült egy olyan csomaggal is, amely az időbélyegzés ügyfél oldali kezelését valósítja meg (az eredeti védelmi profil csomagjai között hiányzott ez a lehetőség).

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, mely a leginkább megfelel a XadesMagic v1.0 igényeinek.

Az alábbi táblázat a XadesMagic v1.0 legfontosabb funkcióit, a PKE PP védelmi profil családból kiválasztott csomagokat és az időbélyeg ügyfél csomagot tekinti át.

1.1 táblázat – A felhasznált csomagok

Csomag neve	Funkcionalitás	Függések
PKE PP védelmi profilból átvett csomagok		
Tanúsítási útvonal érvényesség ellenőrzése (CPV) – Alap	Végrehajtja az összes X.509 érvényesség ellenőrzést, kivéve a szabályzat és név megszorítás feldolgozását	Nincs
PKI aláírás létrehozás	Magánkulcs használata aláírás létrehozására Aláírási információk generálása (pl. Nyilvános kulcsú kriptográfiai szabvány)	Nincs
PKI aláírás ellenőrzés	Feldolgozza az aláírási információkat Nyilvános kulcsot használ az aláírás ellenőrzésére	CPV – Alap
PKI alapú felhasználó hitelesítés	Végrehajtja a „kijelölt” hitelesítési protokoll(oka)t Nyilvános kulcsot használ hitelesítéshez	CPV – Alap
Online tanúsítvány állapot protokoll kliens	OCSP kérést generál az RFC 2560-nak megfelelően	Nincs
CRL érvényesség ellenőrzés	CRL lehívása CRL feldolgozása	Nincs
Naplózás	Naplóadatok generálása napló védelme Ember számára olvasható naplójelentések generálása	Nincs

Folyamatos hitelesítés	Folyamatos hitelesítés végrehajtása	PKI alapú felhasználó hitelesítés, CPV - Alap
Kiegészítő csomag		
Időbélyeg kérés és ellenőrzése	Időbélyeget kér és ellenőriz az RFC 3161 szabványnak megfelelően.	CPV – Alap

1.3 Kapcsolódó dokumentumok

- Department of Defense (DoD) Class 3 Public Key Infrastructure (PKI) Public Key-Enabled Application Requirements," Version 1.0, 13 July 2000 PKE-PP
- RFC 3161 X.509 Internet Public Key Infrastructure - Time-Stamp Protocol, August 2001
- RFC 3280: X.509 Internet Public Key Infrastructure - Certificate and CRL Profile, April 2002
- RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol - OCSP, June, 1999
- International Organization for Standards/Internet Electrotechnical Committee (ISO/IEC) 9594-8:"Information Technology- Open Systems Interconnection-The Directory: Public Key and Attribute Certificate Frameworks" (X.509 Standard)
- International Standard ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security
- Common Methodology for Information Security Evaluation (CEM) Version 1.0, August 1999
- RFC 3275: (Extensible Markup Language) XML-Signature Syntax and Processing
- ITU-T X.680: Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation

1.4 A biztonsági előirányzat szerkezete

A 2., 3. és 4. fejezetek a XadesMagic 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. fejezeten belül az 5.1-5.2 alfejezetek az általános, illetve az egyes csomagokra vonatkozó funkcionális biztonsági követelményeket írják le. Az 5.3 alfejezet az EAL3 követelményeit írja le.

A 6. fejezet a XadesMagic 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 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 verziójával készült (ISO/IEC 15408 IT biztonság értékelési követelményei, 1. rész: Bevezetés és általános modell, 2. rész: Funkcionális biztonsági követelmények, 3. rész: Garanciális biztonsági követelmények.).
A TOE-ra (XadesMagic v1.0) a CC-nek való megfelelőség szempontjából az alábbi nyilatkozatok tehetők:

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

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

2 A TOE (XadesMagic) leírása

2.1 Áttekintés

A jelen biztonsági előirányzat követelményeinek megfelelő alkalmazás (XadesMagic v1.0 fejlesztői függvénykönyvtár) nyilvános kulcs szolgáltatásokkal rendelkezik (PK-szolgáltató), mivel:

- biztonságosan kezel kulcsokat, megbízható pontokat és tanúsítványokat;
- elfogad és feldolgoz X.509 v3 nyilvános kulcs tanúsítványokat;
- képes a szükséges tanúsítványok és visszavonási adatok megszerzésére;
- ellenőrzi minden tanúsítvány érvényességét, az X.509 szabványban [ISO 9594-8] leírt eljárások felhasználásával, beleértve a visszavonás ellenőrzését is;
- hozzáfér pontos és megbízható időforráshoz a tanúsítványok, visszavonási adatok és alkalmazási adatok dátumának, idejének ellenőrzése érdekében;
- beszerzi, tárolja (beágyazza az aláírás struktúrába) a digitális aláírás jövőbeni ellenőrzéséhez szükséges adatokat.

2.2 Megközelítés

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

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

A CC 2. részét felhasználva a biztonsági szempontból fontos követelmények kialakításához jelen biztonsági előirányzat csak a PKI szolgáltatás biztonsági szempontjaival foglalkozik. A PP nem (s így jelen ST sem) tárgyalja például a tanúsítványok és CRL-ek megszerzésének módját, mert ezek biztonsága nem függ attól, hogyan kerültek az alkalmazás birtokába; a biztonságukat a digitális aláírás ellenőrzése biztosítja.

A tanúsítási útvonal ellenőrzése terén a követelményeket a szerzők úgy adták meg, hogy azok megfeleljenek az ISO X.509-nek és az IETF PKIX RFC 3280-nak.

A CC hozzáférés ellenőrzéssel kapcsolatos összetevők nem alkalmasak tanúsítvány és visszavonási információkat (pl. CRL, OCSP válasz) feldolgozó követelményekként, így a CC 2. részét ki kellett terjeszteni.

2.3 A TOE (XadesMagic) meghatározása

2.3.1 A TOE (XadesMagic) típusa

A TOE szoftverfejlesztők számára készült, elektronikus aláírás létrehozás és –ellenőrzés szolgáltatásokat biztosító Microsoft .NET C# programozási nyelven megírt függvénykönyvtár.

A TOE (XadesMagic v1.0) az alábbi összetevőkből áll:

- függvénykönyvtár (4 darab .dll állomány)
  - SDA.XadesMagic.dll
  - SDA.Cryptography.dll
  - SDA.Cryptography.Framework.dll

SDA.TimestampProtocol.dll

- dokumentáció:
  "XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – A konfiguráció menedzselés dokumentációja"
  "XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – Szállítási dokumentáció"
  "XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – Funkcionális specifikáció"
  "XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – Magas szintű terv"
  "XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – Megfeleltetés elemzések"
  "XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – Fejlesztői útmutató"
  "XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – A fejlesztési biztonság dokumentációja"
  "XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – Tesztelési dokumentáció"
  "XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – Teszt lefedettség elemzés"
  "XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – Teszt mélység elemzés"
  "XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 - Sebezhetőség elemzés"

A TOE olyan funkcionalitást biztosít, amellyel elektronikus aláírások létrehozása, ellenőrzése, az ellenőrzéshez érvényesítő információk feldolgozása, tanúsítási útvonal felépítése, tanúsítványok érvényességének ellenőrzése, visszavonási információk érvényesség ellenőrzése, időbélyeg kérése és ellenőrzése, valamint PKI alapú felhasználói hitelesítés valósítható meg.

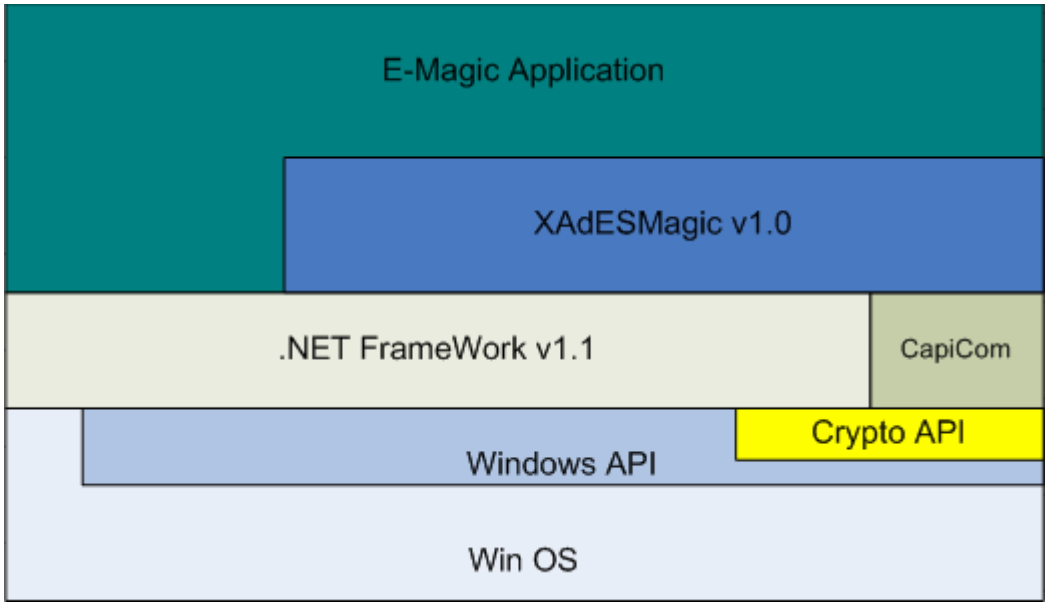
A TOE az MS CryptoAPI kriptográfiai, valamint a .NET Framework v1.1 XML-kezelő (pl. parser) függvényeit használja a saját függvényein kívül.

2.3.2 A TOE (XadesMagic) felépítése

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

A TOE (XadesMagic v1.0) függvénykönyvtárat felhasználva lehet kifejleszteni az IT környezet részét képező, a TOE függvényeit meghívó alkalmazást (pl. E-Magic Application). Szintén az IT környezethez tartoznak a .NET Framework v1.1, a CryptoAPI és a CAPICOM (CryptoAPI Component Object Model) kriptográfiai ActiveX vezérlő, illetve a Windows API és Windows OS (operációs rendszer) egyéb függvényei.

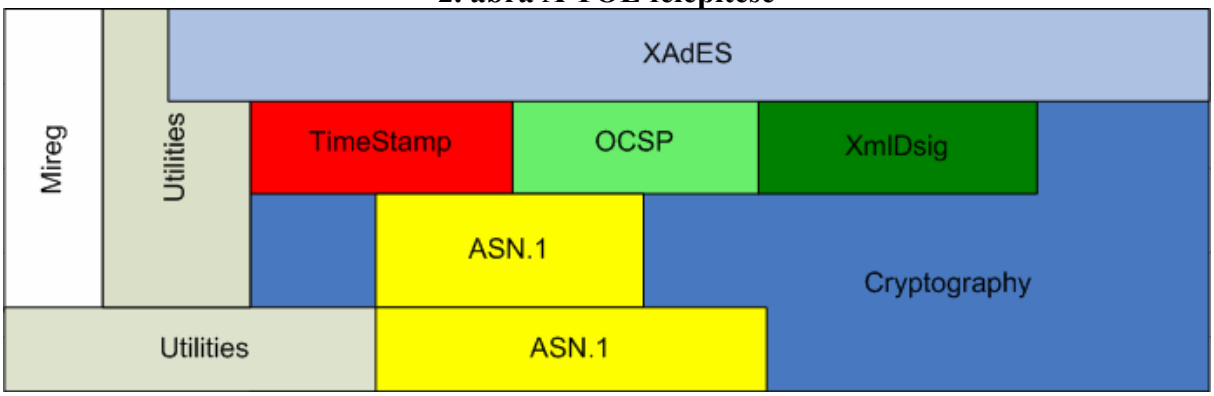
1. ábra A TOE és környezete



A 2. ábra a TOE (XadesMagic v1.0) függvénykönyvtár moduljait mutatja be:

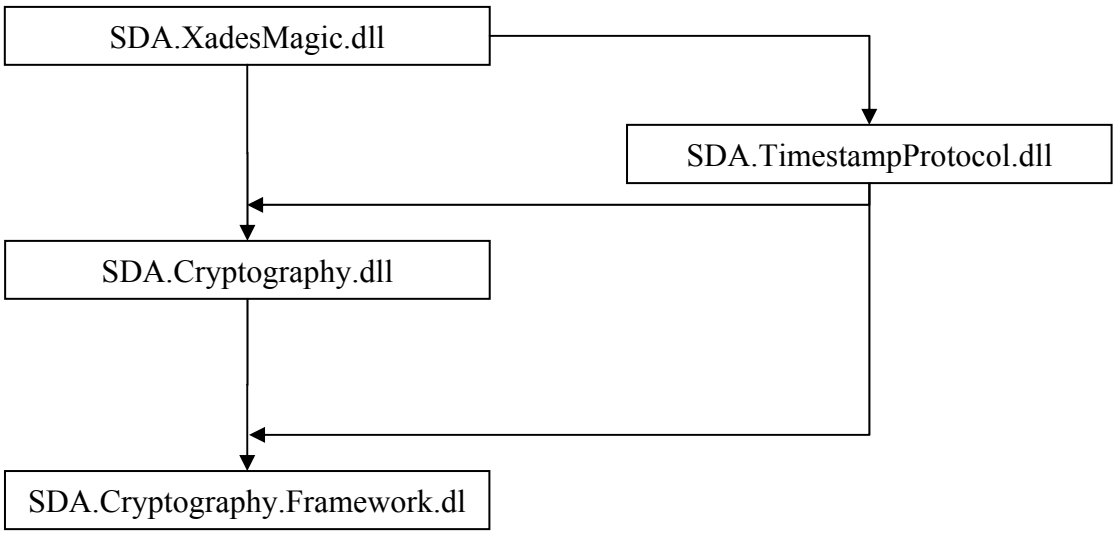
- XAdES (ETSI TS 101 903 v1.2.2 szabványon alapuló kibővített XML elektronikus aláírás struktúra kezelése);
- XmlDsig (RFC 3275 szabványon alapuló XML elektronikus aláírás struktúra kezelése);
- Timestamp (RFC 3161 szabványon alapuló időbélyegek kezelése);
- OCSP (RFC 2560 szabványon alapuló tanúsítvány visszavonási adatok kezelése);
- ASN.1 (ITU-T X.680 és kapcsolódó ajánlásain alapuló adatstruktúrák kezelése);
- Cryptography (a tanúsítványok, tanúsítványtár, tanúsítványláncok, CRL, lenyomatkészítő algoritmusok, tanúsítvány kiterjesztések kezelését végzi);
- MIReG (a Dublin Core elemeit kiegészítő, az Európai Unió IDABC által támogatott metaadat-készlet);
- Utilities (segédeszközök, amelyek többek közt a base64 kódolást, dekódolást, megkülönböztető nevek, MIME típusok kezelését, a naplózást végzik).

2. ábra A TOE felépítése



A 3. ábra a TOE (XadesMagic v1.0) belső függőségeit mutatja be:

3. ábra A TOE függvénykönyvtárainak függőségei



A TOE fokozott biztonságú elektronikus aláírás létrehozása esetén:

- biztonságos aláírás létrehozó eszköz nélkül tudja előállítani a szükséges adatokat.
  KHE (kriptográfiai hardver eszköz)
  PKCS#12 szoftveres kulcstároló állomány
  Windows tanúsítványtár

A TOE a fokozott biztonságú elektronikus aláírások mellett a minősített elektronikus aláírásokat is képes ellenőrizni (ellenőrzi a minősített elektronikus aláírásokra, minősített tanúsítványokra vonatkozó speciális követelményeket).

2.4 A TOE (XadesMagic) alkotóelemei

A 2.1 táblázat az alapul szolgáló PKE PP család által megvalósított csomag-elv alapján a XadesMagic v1.0-hoz kiválasztott funkciók összegzését adja, a táblázat után pedig a csomagok funkcionalitását találhatjuk.

Vannak csomagok, melyek más csomagoktól függnek, azaz amikor egy függő csomagot szerepeltetünk a biztonsági előirányzatban, akkor azt a csomagot is be kell venni teljes egészében, amelytől függ. A táblázat tartalmazza a csomagok közötti függéseket is.

2.1 táblázat – A csomagok áttekintése

Csomag neve	**Funkcionalitás**	**Függések**
Tanúsítási útvonal érvényesség ellenőrzése (CPV) – Alap	Végrehajtja az összes X.509 érvényesség ellenőrzést, kivéve a szabályzat és név megszorítás feldolgozását	Nincs
PKI aláírás létrehozás	Magánkulcs használata aláírás létrehozására Aláírási információk generálása (pl. Nyilvános kulcsú kriptográfiai szabvány)	Nincs
PKI aláírás ellenőrzés	Feldolgozza az aláírási információkat Nyilvános kulcsot használ az aláírás ellenőrzésére	CPV – Alap

Csomag neve	Funkcionalitás	Függések
PKI alapú felhasználó hitelesítés	Végrehajtja a „kijelölt” hitelesítési protokoll(oka)t Nyilvános kulcsot használ hitelesítéshez	CPV – Alap
Valós idejű tanúsítvány állapot protokoll kliens	OCSP kérést generál az RFC 2560-nak megfelelően	Nincs
CRL érvényesség ellenőrzés	CRL lehívása CRL feldolgozása	Nincs
Naplózás	Naplóadatok generálása napló védelme Ember számára olvasható naplójelentések generálása	Nincs
Folyamatos hitelesítés	Folyamatos hitelesítés végrehajtása	PKI alapú felhasználó hitelesítés, CPV - Alap
Időbélyeg kérés és ellenőrzése	Időbélyeget kér és ellenőriz az RFC 3161 szabványnak megfelelően.	CPV - Alap

2.4.1 Tanúsítási útvonal érvényességének ellenőrzése - Alap csomag

A Tanúsítási útvonal érvényesség ellenőrzése – Alap csomag (CPV - Alap) gondoskodik az összes X.509 érvényesség ellenőrzésről, leszámítva a szabályzat feldolgozást és névmegszorítások feldolgozását. 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. Ez a csomag megengedi a megbízható pont érvényességének ellenőrzését, beleértve az aláírás érvényességének ellenőrzését és annak az ellenőrzését, hogy a megbízható pont érvényességi ideje nem járt-e le.
- **Közbenső tanúsítványok**: Ezek a CA-k számára kibocsátott tanúsítványok. Egy tanúsítási útvonal minden tanúsítványa ennek tekintendő, kivéve az utolsót.
- **Végtanúsítvány:** A tanúsítási útvonal legutolsó tanúsítványa, melyet a szóban forgó egyed (előfizető) részére bocsátottak ki.

Jelen csomag a következő biztonsággal kapcsolatos tanúsítvány kiterjesztési ellenőrzéseket veszi számításba: keyUsage, extendedKeyUsage, basicConstraints, qCStatements (minősített elektronikus aláírás ellenőrzése esetében).

Az útvonal érvényesség ellenőrzése az aláírás önbevallott ideje (SigningTime) szerint történik, illetve ha rendelkezésre áll, akkor kizárólag az időbélyegből (SignatureTimeStamp) kinyert dátumot és időpontot veszi alapul.

2.4.2 PKI aláírás létrehozás csomag

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

A TOE az aláírás létrehozását és ellenőrzését az alábbi digitális aláírás sémák szerint valósítja meg:

- SHA-1 lenyomatkészítő algoritmus,
- RSA aszimmetrikus kódoló algoritmus,
- 1024 - 4096 bites kulcsok használata RSA aszimmetrikus kódolás esetén,
- http://www.w3.org/2000/01/xmldsig/rsa-sha1 azonosítóval ellátott aláírás struktúra létrehozása (RSASSA-PKCS-v1_5).

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

2.4.3 PKI aláírás ellenőrzés csomag

A PKI aláírás létrehozás csomag a CPV – Alap csomagtól függ. Aláírási információk, XML aláírás (XAdES) feldolgozására és egy aláírás ellenőrzésekor a nyilvános kulcs használatára tartalmaz funkciókat.

2.4.4 PKI alapú felhasználó hitelesítés csomag

A PKI alapú felhasználó hitelesítés csomag a CPV–Alap csomagtól függ, és lehetővé teszi a PKI használatát felhasználó hitelesítési szolgáltatásokban. A csomagban leírt követelmények azokra az esetekre vonatkoznak, amikor az aláírás létrehozása, ellenőrzése során olyan távoli kiszolgálóhoz fordul a TOE, amelynél a felhasználót tanúsítvánnyal hitelesítik. Ilyen szolgáltatás lehet az időbélyeg kiszolgálónál (pl. SSL, TLS protokollal védett kommunikációs csatorna).

2.4.5 Valós idejű tanúsítvány állapot protokoll kliens csomag

A valós idejű tanúsítvány állapot protokoll (OCSP) kliens csomag lehetővé teszi a TOE-nak, hogy OCSP kéréseket kezdeményezzen és ellenőrizze az OCSP válaszokat. Ez a csomag megengedi mindhárom típusú OCSP válaszadó használatát: OCSP válaszok aláírására jogosult megbízható pont, hitelesítés-szolgáltató, végfelhasználó.

2.4.6 Tanúsítvány visszavonási lista (CRL) érvényesség ellenőrzése csomag

A CRL érvényesség ellenőrzése csomag lehetővé teszi, hogy a TOE ellenőrizzen egy CRL-t.

Jelen csomag használható olyan CRL feldolgozására, amelyre egy CRL szétosztó pont (CRLDP) kiterjesztés mutat egy tanúsítványban, amennyiben a CRL teljes CRL, melyet jelez az IDP és deltaCRLIndicator kiterjesztések hiánya.

2.4.7 Naplózás menedzsment csomag

A naplózás menedzsment csomag a TOE szempontjából fontos eseményeket generálja és védi. Naplózott eseményekre néhány példa:
- megbízható pontok kezelése (hozzáadás, törlés)
- azonosítás és hitelesítés
- aláírás ellenőrzési sikeressége, dátum és idő, szabályok, melyek értelmében az aláírás érvényes
- aláírás ellenőrzés sikertelensége, dátum és idő, kudarc oka
- felhasználó által hatástalanított események (aktuális CRL hozzáférés, null szabályzat elfogadása, stb.)

2.4.8 Folyamatos hitelesítés csomag

Ez a csomag a PKI alapú felhasználó hitelesítéstől és a CPV–Alap csomagtól függ. A protokoll, parancs, csomagok stb. folyamatos hitelesítésére használt csomag.

2.4.9 Időbélyeg kérés és ellenőrzése csomag

Ez a csomag az időbélyeg kérések küldését és a válaszok fogadását, feldolgozását valósítja meg. A CPV – Alap csomagtól függ.

2.5 Garanciális követelmények

A TOE értékelésére vonatkozó garanciakövetelmény: EAL3

3 A TOE biztonsági környezete

3.1 A biztonságos használattal kapcsolatos feltételezések

3.1 táblázat – Feltételezések az IT környezetre

Sorszám	Feltételezés megnevezése	Leírás
1	AE.Authorized_Users	Az engedéllyel rendelkező felhasználók megbízhatók a tekintetben, hogy a számukra kijelölt funkciókat megfelelően hajtják végre.
2	AE.Configuration	A TOE-t megfelelően telepítik és konfigurálják.
3	AE.Crypto_Module	A TOE környezetről feltételezés, hogy tartalmaz egy megbízható kriptográfiai modult (CryptoAPI), mely modul a kriptográfiai műveleteket hajtja végre.
4	AE.Physical_Protection	A TOE környezete fizikailag megvédi a TOE-t a jogosulatlan fizikai hozzáféréssel szemben.
5	AE.PKI_Info	A tanúsítvány és tanúsítvány visszavonási információk a TOE rendelkezésére állnak.
6	AE.Time	A környezetről feltételezzük, hogy GMT formában és a megkívánt pontossággal gondoskodik a pontos rendszeridőről.
7	AE.TimeStamp	A környezetről feltételezzük, hogy biztosítja az időbélyegzés szolgáltatóhoz való hozzáférést.

3.2 Alap biztonsági fenyegetések

Ez az alfejezet a TOE-t fenyegető alap (csomagoktól független) fenyegetéseket azonosítja, míg a 3.3 alfejezet az egyes csomagokra vonatkozó biztonsági fenyegetéseket határozza meg. Mindkét alfejezetre érvényes, hogy a támadott érték a TOE-n valamilyen formában áthaladó információ, illetve a fenyegetés forrásai elsősorban az alábbiak lehetnek:

1) a TOE-hoz hozzáférő olyan egyének, akik alacsony támadási potenciállal rendelkeznek („átlagos” szakértelemmel, kevés erőforrással bírnak és közepes motiváció jellemzi őket); vagy
2) a TOE hibája.

3.2 táblázat – Alapvető biztonsági fenyegetések

Sorszám	Veszély megnevezése	Veszély leírása
1	T.Attack	A TOE értékek észrevétlen kompromittálódása következhet be egy (külső vagy belső) támadó jogosulatlan tevékenysége végzésének kísérlete miatt.
2	T.Audit_Excess	A biztonsági napló túl sok adatot tartalmaz az elemzéshez.
3	T.Audit_Fill	A biztonsági napló túl gyorsan telik meg, így gyakorlatilag nem használható.
4	T.Audit_Modify	A biztonsági napló tartalma nem megbízható, mivel jogosulatlan módosítás történhetett benne.
5	T.Audit_Unreadable	A napló nem olvasható és értelmezhető emberi felhasználó számára, így nem vizsgálhatók a biztonsági szempontból fontos események.
6	T.Bypass	Jogosulatlan egyed vagy felhasználó meghamisíthatja a biztonsági tulajdonságokat vagy más adatokat a TOE biztonsági funkcióinak kikerülése és a TOE értékekhez való jogosulatlan hozzáférés megszerzése érdekében.
7	T.Imperson	Jogosulatlan egyed megszemélyesíthet egy jogosult TOE felhasználót, és ezáltal hozzáféréshez jut a TOE adatokhoz, kulcsokhoz és műveletekhez.
8	T. Modify	Egy támadó módosíthatja a TSF-et vagy más adatokat, például a tárolt biztonsági beállításokat vagy kulcsokat, hogy hozzáférést szerezzen a TOE-hoz és annak adataihoz.
9	T.Object_Init	Egy támadó hozzáférhet jogosulatlanul egy objektumhoz annak létrehozása során, ha a biztonsági tulajdonságokat nem állítják be, vagy bárki megadhatja azokat az objektum létrehozás során.
10	T.Private_Key	Egy támadó felhasználónak adja ki magát a felhasználó magánkulcsának generálása vagy használata által.
11	T.Role	Egy felhasználó magasabb szintű jogosultságú szerepben jelenhet meg, mint amekkora neki megengedett, és ezt az emelt szintű jogosultságot használhatja fel jogosulatlan tevékenységekhez.
12	T.Secure_Attributes	Egy felhasználó módosíthatja egy objektum biztonsági tulajdonságait, ami által jogosulatlanul hozzáfér az objektumhoz.
13	T.Shoulder_Surf	Egy jogosulatlan felhasználó a jogosult felhasználó válla fölötti kémleléssel megismeri a hitelesítési információkat a hitelesítési folyamat során.
14	T.Tries	Egy jogosulatlan egyed próbálgatás és hiba következtében kitalálhatja a hitelesítési információt.

3.3 Az egyes csomagokra vonatkozó biztonsági fenyegetések

3.3.1 Tanúsítási útvonal érvényességének ellenőrzése – Alap csomag

Az alapveszélyeken kívül, az alábbi fenyegetések sorolandók a „Tanúsítási útvonal ellenőrzés – Alap” csomagjába.

3.3 táblázat– A „Tanúsítási útvonal érvényesség ellenőrzése – Alap” csomagot érintő veszélyek

Sorszám	Veszély megnevezése	Veszély leírása
1	T.Certificate_Modi	Egy jogosulatlan felhasználó tanúsítványt módosíthat, 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, és ezáltal ezek az egyedek jogosult felhasználónak adják 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 nem engedélyezett tanúsítványokat bocsát ki.

3.3.2 PKI aláírás létrehozás csomag

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

3.4 táblázat – A „PKI aláírás generálás” csomaggal kapcsolatos veszélyek

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

3.3.3 PKI aláírás ellenőrzés csomag

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

3.5 táblázat – A „PKI aláírás ellenőrzés” csomaggal kapcsolatos veszélyek

Sorszám	Veszély megnevezése	Veszély leírása
1	T.Assumed_Identity_PKI_Ver	Egy felhasználó egy másik felhasználónak adhatja ki magát, hogy ellenőrizhessen egy PKI aláírást.
2	T.Clueless_PKI_Ver	A felhasználó jelzés hiányában csak helytelen tanúsítványok felhasználásával próbál ellenőrizni.

3.3.4 PKI alapú felhasználó hitelesítés csomag

Az alábbi veszélyek a „PKI alapú felhasználó hitelesítés” csomagot jellemzik.

3.6 táblázat – A „PKI alapú felhasználó hitelesítés csomaggal” kapcsolatos veszélyek

Sorszám	Veszély megnevezése	Veszély leírása
1	T.Assumed_Identity_Auth	Egy felhasználó egy másik felhasználónak adja ki magát, hogy végrehajthasson egy PKI alapú felhasználó hitelesítést.
2	T.Replay_Entity	Egy jogosulatlan felhasználó visszajátszik egy érvényes hitelesítő adatot.

3.3.5 Valós idejű tanúsítvány állapot protokoll kliens csomag

Az alábbi veszélyek a „Valós idejű tanúsítvány állapot protokoll kliens” csomagot jellemzik.

3.7 táblázat
A „Valós idejű tanúsítvány állapot protokoll kliens” csomaggal kapcsolatos veszélyek

Sorszám	Veszély megnevezése	Veszély leírása
1	T.Replay_OCSP_Info	A felhasználó egy régi OCSP választ fogad el, amelynek következtében elfogad egy már visszavont tanúsítványt az OCSP tranzakcióhoz.
2	T.Wrong_OCSP_Info	A felhasználó elfogad egy visszavont tanúsítványt, vagy visszautasít egy érvényes tanúsítványt, egy helytelen OCSP válasz következtében.

3.3.6 Tanúsítvány visszavonási lista ellenőrzése (érvényesítése) csomag

Az alábbi veszélyek a „Tanúsítvány visszavonási lista (CRL) ellenőrzése” csomagot jellemzik.

3.8 táblázat – A „Tanúsítvány visszavonási lista (CRL) ellenőrzése” csomaggal kapcsolatos veszélyek

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

3.3.7 Naplózás csomag

Az alábbi veszélyek a „Naplózás” csomagot jellemzik.

3.9 táblázat – A „Naplózás” csomaggal kapcsolatos veszélyek

Sorszám	Veszély megnevezése	Veszély leírása
1	T.Accountability	A biztonsági szempontból fontos naplóadatok nem köthetők egyedek tevékenységéhez.
2	T.No_Audit	Nincs biztonsági napló a biztonsági szempontból fontos események vizsgálatához.

3.3.8 Folyamatos hitelesítés csomag

Az alábbi veszélyek a „Folyamatos hitelesítés” csomagot jellemzik.

3.10 táblázat – A „Folyamatos hitelesítés” csomaggal kapcsolatos veszélyek

Sorszám	Veszély megnevezése	Veszély leírása
1	T.Hijack	Egy jogosulatlan felhasználó eltérít egy hitelesített munkaszakaszt.

3.3.9 Időbélyeg kérése és ellenőrzése csomag

Az alábbi veszélyek az „Időbélyeg kérése és ellenőrzése” csomagot jellemzik.

3.11 táblázat – Az „Időbélyeg kérése és ellenőrzése” csomaggal kapcsolatos veszélyek

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 elfogad egy visszavont tanúsítványt vagy visszautasít egy érvényeset.

3.4 Szervezeti biztonsági szabályok

Ezen biztonsági előirányzat alapját képező védelmi profil (PKE PP) család nem tartalmaz szervezeti biztonsági szabályokat. Jelen biztonsági előirányzat sem tartalmaz szervezeti biztonsági szabályokat.

4. Biztonsági célok

Ez a fejezet a TOE biztonsági céljait határozza meg. A 4.1 alfejezet az alap (csomagtól független), míg a 4.2 az egyes csomagokra vonatkozó biztonsági célokat azonosítja.
A környezet által teljesítendő biztonsági célokat „OE” előtag, míg a TOE által teljesítendőket „O” előtag jelöli.

4.1 Alap biztonsági célok a TOE környezetére

4.1 táblázat – A TOE környezetére vonatkozó biztonsági célok

Sorszám	Cél megnevezése	Cél leírása
1	OE.Audit_Protect	Az IT környezet TSF-nek meg kell védenie a biztonsági naplófájlt a jogosulatlan módosítástól.
2	OE.Audit_Readable	Az IT környezet TSF-nek képesnek kell lennie humán felhasználó által olvasható formára hozni a naplórekordokat.
3	OE.Audit_Select	Az IT környezet TSF-nek lehetővé kell tennie a jogosult felhasználók számára a naplózandó események kiválasztását.
4	OE.DAC	Az IT környezet TSF-nek ellenőriznie és korlátoznia kell a felhasználók hozzáféréseit a TOE értékekhez, egy megadott hozzáférés ellenőrzési szabályzatnak megfelelően.
5	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.
6	OE.Init_Secure_Attr	Az IT környezet TSF-nek érvényes és helyes alapértelmezett biztonsági tulajdonságokról kell gondoskodnia egy objektum inicializálásakor.
7	OE.Invoke	Az IT környezet TSF-nek minden tevékenység esetén meg kell hívódnia.
8	OE.Limit_Actions_Auth	Az IT környezet TSF-nek korlátoznia kell azon tevékenységeket, melyeket egy felhasználó végrehajthat, mielőtt a TSF ellenőrzi a felhasználó kilétét.
9	OE.Limit_Tries	Az IT környezet TSF-nek korlátoznia kell az egymás utáni sikertelen hitelesítések számát.
10	OE.No_Echo	Az IT környezet TSF-nek nem szabad kijeleznie a hitelesítési információkat.
11	OE.Protect_I&A_Data	Az IT környezet TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie az I&A adatok módosítását.
12	OE.Secure_Attributes	Az IT környezet TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie a biztonsági tulajdonságok módosítását.
13	OE.Security_Roles	Az IT környezet TSF-nek karban kell tartania

Sorszám	Cél megnevezése	Cél leírása
		a biztonsági szempontból lényeges szerepköröket és a felhasználók ezen szerepkörökhöz való rendelését.
14	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.
15	OE.Trust_Anchor	Az IT környezet TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie a megbízható pontok karbantartását.
16	OE.TSF_Data	Az IT környezet TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie a TSF adatok módosítását.
17	OE.Authorized_Users	Az engedéllyel rendelkező felhasználók megbízhatók a tekintetben, hogy a számukra kijelölt feladatokat biztonsági szempontból korrekt módon hajtják végre.
18	OE.Configuration	A TOE-t úgy kell telepíteni és konfigurálni, hogy a TOE biztonságos állapotban kezdjen el üzemelni.
19	OE.Crypto	A környezetnek tartalmaznia kell egy vagy több megbízható kriptográfiai modult, mely modul vagy modulok a kriptográfiai műveleteket hajtják végre.
20	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 időzítés elemzés különböző formái.
21	OE.PKI_Info	Az IT környezetnek biztosítania kell a TOE számára a tanúsítvány és tanúsítvány visszavonási információkat.
22	OE.Time	A környezetnek hozzáférést kell biztosítania a pontos időhöz, megkívánt pontossággal, GMT formára alakítva.
23	OE.TimeStamp	Az IT környezetnek biztosítania kell a TOE számára az időbélyegzés szolgáltatóhoz való hozzáférést.

4.2 A csomagokra vonatkozó biztonsági célok

4.2.1 Tanúsítási útvonal érvényességének ellenőrzése - Alap csomag

4.2 táblázat – Biztonsági célok a CPV – Alap csomag esetén

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

4.2.2 PKI aláírás létrehozási csomag

4.3 táblázat – Biztonsági célok PKI aláírás létrehozási csomag esetén

sorszám	Cél megnevezése	Cél leírása
1	O.Give_Sig_Hints	A TSF-nek utalni kell arra, hogy melyik tanúsítványt vagy kulcsot kell kiválasztani a PKI aláíráshoz.

4.2.3 PKI aláírás ellenőrzési csomag

4.4 táblázat– Biztonsági célok a PKI aláírás ellenőrzési csomag esetén

Sorszám	Cél megnevezése	Cél leírása
1	O.Use_Sig_Hints	A TSF-nek utalni kell arra, hogy melyik tanúsítványt vagy kulcsot kell kiválasztani az aláírás ellenőrzéshez.
2	O.Linkage_Sig_Ver	A TSF-nek a megfelelő felhasználó nyilvános kulcsát kell használnia az aláírás ellenőrzéséhez.

4.2.4 PKI alapú felhasználó hitelesítés csomag

4.5 táblázat – Biztonsági célok a PKI alapú felhasználó hitelesítés csomag esetén

Sorszám	Cél megnevezése	Cél leírása
1	O.I&A_Remote	A TSF-nek egyértelműen azonosítania kell az összes távoli egyedet, és hitelesítenie kell azok állítólagos azonosságát, mielőtt egy távoli egyednek hozzáférést engedélyezne a TOE szolgáltatásokhoz és erőforrásokhoz.
2	O.Limit_Actions_Auth_Remote	A TSF-nek korlátoznia kell azokat a tevékenységeket, melyeket egy távoli egyed végrehajthat azelőtt, mielőtt a TSF ellenőrizné a távoli egyed azonosságát.
3	O.Linkage	A TSF-nek a megfelelő felhasználói nyilvános kulcsot kell használnia a hitelesítéshez.
4	O.Single_Use_I&A	A TSF-nek olyan azonosítási és hitelesítési (I&A) mechanizmusokat kell alkalmaznia, amelyek egyedi hitelesítési információkat követelnek meg minden egyes I&A esetén.

4.2.5 Valós idejű tanúsítvány állapot protokoll kliens csomag

4.6 táblázat – Biztonsági célok a valós idejű tanúsítvány állapot protokoll kliens csomag esetén

Sorszám	Cél megnevezése	Cél leírása
1	O.Accurate_OCSP_Info	A TSF-nek csak a pontos OCSP válaszokat szabad elfogadnia.
2	O.Auth_OCSP_Info	A TSF-nek el kell fogadnia a jogosult forrásból származó OCSP visszavonási információkat.
3	O.Fresh_OCSP_Info	A TSF-nek csak valószerűen aktuális visszavonási információkat szabad elfogadnia az OCSP tranzakciók esetén.

4.2.6 Tanúsítvány visszavonási lista ellenőrzése (érvényesítése) csomag

4.7 táblázat – Biztonsági célok a CRL érvényesség ellenőrzés csomag esetén

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

4.2.7 Naplózás menedzsment csomag

4.8 táblázat– Biztonsági célok a naplózás menedzsment csomag esetén

Sorszám	Cél megnevezése	Cél leírása
1	O.Audit	A TSF-nek naplóznia kell a biztonsági szempontból fontos eseményeket.
2	O.Audit_User	A TSF-nek képesnek kell lennie a naplózott eseményeket egyedi felhasználókhoz kötni.

4.2.8 Folyamatos hitelesítés csomag

4.9 táblázat – Biztonsági célok a folyamatos hitelesítés csomag esetén

Sorszám	Cél megnevezése	Cél leírása
1	O.Continuous_I&A	A TSF-nek folyamatosan hitelesítenie kell a felhasználót.

4.2.9 Időbélyeg kérése és ellenőrzése csomag

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

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

5. IT biztonsági követelmények

Ez a fejezet a TOE funkcionális és garanciális biztonsági követelményeit írja le, a védelmi profil család által lefedett összes védelmi profilra. A követelmények a CC 2. és 3. részéből származnak, illetve a 2. rész kiterjesztései. A kiterjesztésre azért volt szükség, mert a CC nem nyújt katalogizált követelményeket az X.509 feldolgozási szabályokra, melyek ebben a biztonsági előirányzatban kritikus jelentőségűek.
A jelölések a CC-nek megfelelnek.

Az alábbi táblázat összesíti a védelmi profil családba tartozó összes lehetséges PP funkcionális követelményét.

5.1 táblázat– Kiterjesztett 2. vagy 3. rész követelmények

Követelmény	**2. részből származó vagy kiterjesztett**
FAU_GEN.1	2. rész
FAU_GEN.2	2. rész
FAU_SAR.1	2. rész
FAU_SEL.1	2. rész
FAU_STG.1	2. rész
FDP_ACC.1	2. rész
FDP_ACF.1	2. rész
FDP_RIP.1	2. rész
FIA_AFL.1	2. rész
FIA_ATD.1	2. rész
FIA_UAU.1	2. rész
FIA_UAU.4	2. rész
FIA_UAU.6	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_INI.1	Kiterjesztett 2. rész
FDP_DAU_CPV_OUT.1	Kiterjesztett 2. rész
FDP_DAU_CRL.1	Kiterjesztett 2. rész
FDP_DAU_OCS.1	Kiterjesztett 2. rész
FDP_DAU_SIG.1	Kiterjesztett 2. rész
FDP_DAU_TS.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
FIA_UAU_SIG.1	Kiterjesztett 2. rész

5.1 A TOE környezet alap funkcionális biztonsági követelményei

Az 5.2–es táblázat az általános funkcionális biztonsági követelményeket írja le, a táblázat után pedig a funkcionális követelmények kibontása következik.

Ezen biztonsági célok IT környezeti célként való felvételét indokolja a TOE terméktípusa, a fejlesztői könyvtár jelleg. A TOE az alá, illetve a fölé épülő IT környezetre alapoz az alábbi általános biztonsági célok teljesítése érdekében.

Mivel jelen biztonsági előirányzat a PKE PP-t veszi alapul, ezért tartja magát a PP szemléletéhez.

5.2 táblázat – A TOE környezetére vonatkozó funkcionális biztonsági követelmények

Sorszám	Funkcionális követelmény	Cím
1	FAU_SAR.1	Naplók átnézése
2	FAU_SEL.1	Szelektív naplózás
3	FAU_STG.1	Védett naplóadat tárolás
4	FCS_CRM_FPS.1	Kriptográfiai modul
5	FDP_ACC.1	Részleges hozzáférés ellenőrzés - PKI engedélyek kezelése
6	FDP_ACF.1	Biztonsági tulajdonságokon alapuló hozzáférés ellenőrzés – PKI engedélyek kezelése
7	FDP_ITC_PKI_INF.1	PKI információk importálása a TSF-en kívülről
8	FDP_RIP.1	Részhalmazra vonatkozó maradványinformáció-védelem
9	FIA_AFL.1	Sikertelen hitelesítés kezelése
10	FIA_ATD.1	Felhasználói tulajdonságok megadása
11	FIA_UAU.1	Hitelesítés időzítése
12	FIA_UAU.7	Védett hitelesítés visszacsatolás
13	FIA_UID.1	Azonosítás időzítése
14	FMT_MSA.1	Biztonsági tulajdonságok kezelése
15	FMT_MSA.3	Statikus tulajdonság inicializálás
16	FMT_MTD.1	TSF adatok kezelése
17	FMT_SMF.1	Menedzsment funkciók specifikációja
18	FMT_SMR.2	Megszorítások a biztonsági szerepkörökre
19	FPT_RVM.1	A TSP megkerülhetetlensége
20	FPT_SEP.1	TSF tartomány szétválasztás
21	FPT_STM.1	Megbízható időbélyegzés

5.1.1 FAU osztály – Biztonsági naplózás

FAU_SAR.1 Naplók átnézése

Hierarchia szerint alárendelt-e más komponensnek: nem.

FAU_SAR.1.1 Az **IT környezet** TSF-nek biztosítania kell, hogy a ***TOE függvényeit meghívó alkalmazás használatára jogosult felhasználók*** olvasni tudják a naplóadatokból ***az összes naplóadatot.***

FAU_SAR.1.2 Az **IT környezet** TSF-nek a felhasználó által értelmezhető formában kell rendelkezésre bocsátania a naplórekordokat.

Függések: FAU_GEN.1 Naplóadatok generálása

FAU_SEL.1 Szelektív naplózás

Hierarchia szerint alárendelt-e más komponensnek: nem.

FAU_SEL.1.1 Az **IT környezet** TSF-nek képesnek kell lennie, hogy bevegyen vagy kizárjon a naplózott események készletéből naplózható eseményeket, az alábbiak szerint:

a) ***objektum identitás, felhasználó identitás, host identitás, esemény típus***

b) ***aláíró identitás, szabályzat azonosító, kulcs azonosító, megbízható pont.***

Függőségek: FAU_GEN.1 Naplóadatok generálása
FMT_MTD.1 TSF adatok kezelése

FAU_STG.1 Védett naplóadat tárolás

Hierarchia szerint alárendelt-e más komponensnek: nem.

FAU_STG.1.1 Az **IT környezet** TSF-nek meg kell védenie a tárolt naplórekordokat a jogosulatlan törléstől.

FAU_STG.1.2 Az **IT környezet** TSF-nek képesnek kell lennie, hogy ***észlelje*** a naplórekordok módosításait.

Függések: FAU_GEN.1 naplóadatok generálása

5.1.2 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 aláíró és ellenőrző folyamat (szubjektumok), az aláíró és ellenőrző folyamathoz szükséges adatok (objektumok), illetve az aláírás létrehozása, aláírás ellenőrzése, időbélyeg kérése, időbélyeg válasz ellenőrzése, tanúsítványlánc felépítése, tanúsítványlánc ellenőrzése, visszavonási adatok kérése, visszavonási adatok ellenőrzése (műveletek)*** vonatkozásában.

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, megengedett-e egy művelet az ellenőrzött szubjektumok és ellenőrzött objektumok között:

a) Magánkulcsok, importálhatók („soft token" esetén a memóriába), exportálhatók, használhatók a TOE függvényeit meghívó alkalmazás által.

b) Nyilvános kulcs tanúsítványok, exportálhatók, használhatók a TOE függvényeit meghívó alkalmazás által.

c) Nyilvános kulcs tanúsítványokat bárki felhasználhat.

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

FDP_ACF.1.4 Az **IT környezet** TSF-nek explicit módon le kell tiltania a szubjektumok objektumokhoz való hozzáféréseit: ***nincsenek további szabályok.***

Függések: FDP_ACC.1 Részleges hozzáférés ellenőrzés,
FMT_MSA.3 Statikus tulajdonságok inicializálása

FDP_RIP.1 Részhalmazra vonatkozó maradványinformáció-védelem

Hierarchikus alárendeltség más komponensekhez képest: nincs.

FDP_RIP.1.1 Az **IT környezet** TSF-nek biztosítania kell, hogy bármely előző forrásnak az információtartalma elérhetetlen legyen **magánkulcsot, PIN kódot** illetően a következő objektumokból: **memória, állomány.**

Függőség: Nincsenek.

5.1.3 FIA osztály – Azonosítás és hitelesítés

FIA_AFL.1 Sikertelen hitelesítések kezelése

Hierarchikus alárendeltség más komponensekhez képest: nincs.

FIA_AFL.1.1 Az **IT környezet** TSF-nek észlelnie kell, amikor ***a magánkulcs tároló eszköz vagy a TOE függvényeit meghívó alkalmazás által meghatározott számú*** sikertelen hitelesítési kísérlet történik a ***magánkulcshoz való hozzáférés*** eseményekkel kapcsolatban.

FIA_AFL.1.2 Amikor a definiált számú sikertelen hitelesítési kísérlet bekövetkezett, vagy a kísérletek száma meghaladta ezt az értéket, az **IT környezet** TSF-nek a következőket kell tennie: ***a magánkulcs tároló által meghatározottakat kell végrehajtania (pl. BALE esetén a magánkulcs 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 paraméterek továbbítását a TOE függvényeit meghívó alkalmazás által (pl. magánkulcs tároló eszköz paraméterei)***, mielőtt a felhasználó hitelesítésre kerül.

FIA_UAU.1.2 Az **IT környezet** TSF megköveteli, hogy minden felhasználó sikeresen hitelesítve legyen, mielőtt bármilyen más **IT környezet** TSF által közvetített tevékenység történne a kérdéses felhasználó nevében.

Függések: FIA_UID.1 Azonosítás időzítése

FIA_UAU.7 Védett hitelesítés visszacsatolás

Hierarchikus alárendeltség más komponensekhez képest: nincs.

FIA_UAU.7.1 Az **IT környezet** TSF csak ***fedőkaraktert (pl. * vagy ●)*** szolgáltat a felhasználónak a hitelesítési folyamat végrehajtása közben.

Függések: FIA_UAU.1 Hitelesítés időzítése

FIA_UID.1 Azonosítás időzítése

Hierarchikus alárendeltség más komponensekhez képest: nincs.

FIA_UID.1.1 Az **IT környezet** TSF-nek lehetővé kell tennie a felhasználó nevében végrehajtandó ***tevékenységeket: a paraméterek továbbítását a TOE függvényeit meghívó alkalmazás által (pl. magánkulcs tároló eszköz paraméterei)***, mielőtt a felhasználó azonosításra kerül.

FIA_UID.1.2 Az **IT környezet** TSF megköveteli, hogy minden felhasználó sikeresen azonosítva legyen, mielőtt bármilyen más **IT környezet** TSF által közvetített tevékenység történne a kérdéses felhasználó nevében.

Függések: nincsenek.

5.1.4 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 nyilvános kulcs tanúsítvány és a magánkulcs közötti kapcsolat, a TOE függvényeit meghívó alkalmazást azonosító adatok, a TOE biztonsági funkcióinak működését befolyásoló paraméterek*** biztonsági tulajdonsággal kapcsolatban a következő tevékenységeket korlátozzák: ***lekérdezés, módosítás, törlés*** képessége a ***TOE függvényeit meghívó alkalmazás*** szerepkörre.

Függések: FMT_SMF.1 Menedzsment funkciók megadása,
FMT_SMR.1 Biztonsági szerepkörök,
FDP_ACC.1 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 függvényeit meghívó alkalmazás*** 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 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, végfelhasználói tanúsítványok, CRL-ek, CRL használat konfigurációs paramétereinek, időbélyeg használat paramétereinek, megbízható időbélyeg kiszolgálók címeinek, OCSP használat konfigurációs paramétereinek, aláírásba ágyazandó egyéb adatoknak (ETSI TS 101 903 v1.2.2 szabványban szereplő választható elemek)*** a ***módosítását, törlését, tartalom törlését, hozzáadását*** a ***TOE függvényeit meghívó alkalmazás*** szerepkörre.

Függések: FMT_SMF.1 Menedzsment funkciók megadása,
FMT_SMR.1 Biztonsági szerepkörök

FMT_SMF.1 Menedzsment funkciók megadása

Hierarchikus alárendeltség más komponensekhez képest: nincs.

FMT_SMF.1.1 Az **IT környezet** TSF-nek képesnek kell lennie a következő biztonsági menedzsment funkciók végrehajtására: ***megbízható pontok karbantartása, közbenső tanúsítványok karbantartása, végfelhasználói tanúsítványok karbantartása, TOE függvényeit meghívó alkalmazás által beállítható paraméterek (pl. CRL, OCSP, időbélyeg elfogadásának feltételei) TOE felé történő megbízható továbbítása***.

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 függvényeit meghívó alkalmazás*** szerepköröket.

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 ***hozzáférési jogosultságok, műveletek végrehajtásának engedélyezései*** teljesülnek.

Függések: FIA_UID.1 Azonosítás időzítése

5.1.5 FPT osztály – A TOE biztonsági funkciók védelme

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 elkülönítés

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 szubjektumok biztonsági tartománya közötti elkülönítést a TSC-ben.

Függések: nincsenek.

5.1.6 FCS osztály – Kriptográfiai támogatás

FCS_CRM_FPS.1 Kriptográfiai modul

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 Minden kriptográfiai modulnak ***minősített elektronikus aláírás létrehozása esetén NHH által nyilvántartásba vett, tanúsított biztonságos aláírás létrehozó eszköznek (BALE)*** kell lennie.

Függések: nincsenek.

5.1.7 FDP osztály – Felhasználói adatok védelme

FDP_ITC_PKI_INF.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 eszközökhöz való interfészek, CRL-ek, OCSP-kiszolgálók, időbélyeg-kiszolgálók elérhetőségének*** rendelkezésre állását a TOE ***funkcióinak teljesítését biztosító időn belüli*** mérték szerint a következő feltételek figyelembe vétele alapján: ***hálózati kapcsolat rendelkezésre állása, információs szerver rendelkezésre állása, az alkalmazás protokollban információ rendelkezésre állása, az IT környezethez információ rendelkezésre állása.***

Függések: nincsenek.

5.1.8 FPT osztály – A TSF védelme

FPT_STM.1 Megbízható időbélyegzés

Hierarchikus alárendeltség más komponensekhez képest: nincs.

FPT_STM.1.1 Az IT környezetnek a TSF használathoz megbízható időbélyeget kell biztosítania.

Függések: nincsenek.

5.1.9 Funkció erősségre vonatkozó követelmény

A TOE funkcionális biztonsági követelményeire vonatkozó minimális funkcióerősségi szint: SOF-alap, bár megjegyzendő, hogy 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.

5.3 táblázat – A csomagokban szereplő funkcionális biztonsági követelmények összegzése

Csomag neve	Funkcionális követelmény	Függések
Tanúsítási útvonal érvényesség ellenőrzése – Alap	FDP_CPD.1	nincs
	FDP_DAU_CPV_INI.1	
	FDP_DAU_CPV_CER.1	
	FDP_DAU_CPV_CER.2	
	FDP_DAU_CPV_OUT.1	
PKI aláírás létrehozás	FDP_ETC_SIG.1	nincs
PKI aláírás ellenőrzés	FDP_ITC_SIG.1	Tanúsítási útvonal érvényesség ellenőrzése – Alap
	FDP_DAU_SIG.1	
PKI alapú felhasználó hitelesítés	FIA_UAU.1;1	Tanúsítási útvonal érvényesség ellenőrzése – Alap
	FIA_UAU.4	
	FIA_UAU_SIG.1	
	FIA_UID.1;1	
Valós idejű tanúsítvány állapot protokoll kliens	FDP_DAU_OCS.1	nincs
Tanúsítvány visszavonási lista érvényesség ellenőrzése	FDP_DAU_CRL.1	nincs
Naplózás menedzsment	FAU_GEN.1	nincs
	FAU_GEN.2	
Folyamatos hitelesítés	FIA_UAU.6;1	PKI alapú felhasználó hitelesítés, Tanúsítási útvonal érvényesség ellenőrzése – Alap
	FIA_UAU.6;2	
Kiegészítő csomag		
Időbélyeg kérése és ellenőrzése	FDP_DAU_TS.1	Tanúsítási útvonal érvényesség ellenőrzése – Alap

5.2.1 Tanúsítási útvonal érvényesség ellenőrzése - Alap csomag

5.2.1.1 FDP osztály – Felhasználói adatok védelme

FDP_CPD.1 Tanúsítási útvonal felépítése

Hierarchia szerint alárendelt-e más komponensnek: nem.

FDP_CPD.1.1 A TSF-nek fel kell építenie egy tanúsítási útvonalat a ***TOE függvényeit meghívó alkalmazás (ellenőrző fél)*** által biztosított megbízható ponttól az előfizetőig, a következő előfizetői tanúsítvány mezők vagy kiterjesztésekre vonatkozó illesztési szabályok felhasználásával: ***a tanúsítvány kibocsátója mezőben (issuer) levő megkülönböztető név (DN) megegyezik a tanúsítvány aláírásához használt tanúsítvány (subject) megkülönböztető nevével (DN).***

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

a) keyUsage kiterjesztésben az RFC 3280, RFC 3739, ETSI TS 101 862 v1.3.2, ETSI TS 102 280 v1.1.1, RFC 3161, RFC 2560 szabványokban leírtaknak megfelelő bit be van kapcsolva.

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

a) extKeyUsage kiterjesztésben az RFC 3280, RFC 3739, ETSI TS 101 862 v1.3.2, ETSI TS 102 280 v1.1.1, RFC 3161, RFC 2560 szabványokban leírtaknak megfelelő bit be van kapcsolva.

FDP_CPD.1.4 A TSF-nek mellőznie kell minden illesztési szabályt, kivéve a ***megkülönböztető néven alapuló szabályt***, ha további tanúsítási útvonalakra is szükség van.

Függések: nincsenek.

FDP_DAU_CPV_INI.1 Tanúsítási útvonal inicializálása -- alapelemek

Hierarchia szerint alárendelt-e más komponensnek: nem.

FDP_DAU_CPV_INI.1.1

A TSF-nek használnia kell a ***TOE függvényeit meghívó alkalmazás*** által megadott megbízható pontot.

FDP_DAU_CPV_INI.1.2

A TSF-nek meg kell kapnia az „aktuális” pontos időt egy megbízható forrásból a ***TOE függvényeit meghívó alkalmazás által megadott megbízható forrásból NTP (RFC 1305) vagy SNTP (RFC 1769) protokollon keresztül.***

FDP_DAU_CPV_INI.1.3

A TSF-nek végre kell hajtania az alábbi ellenőrzéseket a megbízható pontra:

a) alany megkülönböztető név (DN) és kibocsátó megkülönböztető név (DN) egyezés;

b) aláírás ellenőrzés az alany nyilvános kulcsának és paraméterének (ha van ilyen) felhasználásával a megbízható ponttól;

c) notBefore mező a megbízható pontban <= aktuális idő;

d) notAfter mező a megbízható pontban => aktuális idő.

FDP_DAU_CPV_INI.1.4

A TSF-nek származtatnia kell a megbízható pontból az alábbiakat: ***alany megkülönböztető név (DN), alany nyilvános kulcsa, alany nyilvános kulcs algoritmus objektum azonosító, alany nyilvános kulcs paraméterek.***

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

FDP_DAU_CPV_CER.1 Tanúsítvány feldolgozás -- alapelemek

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) szülő nyilvános kulcs és szülő nyilvános kulcs paraméterek használata a tanúsítványon lévő aláírás ellenőrzésére;

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

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

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

e) a TSF képes minden kritikusnak jelölt kiterjesztést feldolgozni.

FDP_DAU_CPV_CER.1.2

A TSF-nek csak akkor szabad elfogadnia egy tanúsítványt, ha a használt ***CRL, OCSP válasz*** azt mutatja, hogy a tanúsítvány nem visszavont.

FDP_DAU_CPV_CER.1.3

A TSF-nek a nyilvános kulcs paraméterek állapot-mechanizmust az alábbi szabályokat követve kell módosítania:

a) A paramétereket a tanúsítvány subjectPublickeyInfo mezőjéből nyeri ki, ha ez a mező tartalmazza a paramétereket, különben

b) a paramétereket RSA-SHA1 algoritmusra állítja be.

Függések: FCS_COP.1 Kriptográfiai művelet,
FPT_STM.1 Megbízható időbélyegek

FDP_DAU_CPV_CER.2 Közbenső tanúsítvány feldolgozás - alapelemek

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 basicConstraints mező jelen van a CA=TRUE értékkel;
b) a pathLenConstraint valóban teljesül;
c) ha egy kritikus keyUsage kiterjesztés szerepel, akkor a keyCertSign bit be van kapcsolva.

Függések: FDP_DAU_CPV_CER.1 Tanúsítvány feldolgozás -- alapelemek

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 ki kell jeleznie a tanúsítási útvonal érvényesség ellenőrzésének sikertelenségét, ha a tanúsítási útvonal bármelyik tanúsítványa érvénytelen.

FDP_DAU_CPV_OUT.1.2

A TSF-nek ki kell jeleznie a végtanúsítvány következő változóit: alany megkülönböztető neve (DN), alany nyilvános kulcs algoritmus azonosítója, alany nyilvános kulcsa, kritikus keyUsage kiterjesztés.

FDP_DAU_CPV_OUT.1.3

A TSF-nek ki kell jeleznie továbbá a következő változókat a végtanúsítványból: ***tanúsítvány*.**

FDP_DAU_CPV_OUT.1.4

A TSF-nek ki kell jeleznie az alany nyilvános kulcs paramétereit a tanúsítási útvonal paraméter állapotgépből.

Függések: nincsenek

5.2.2 PKI aláírás létrehozás csomag

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 magánkulcsot kell használnia digitális aláíráshoz.

FDP_ETC_SIG.1.2 A TSF-nek az alábbi információkat kell belefoglalnia a digitális aláírásba: ***hash algoritmus, aláírási algoritmus, aláíró nyilvános kulcs tanúsítványa, aláíró megkülönböztető neve (DN), aláírás dátuma és időpontja.***

Függések: FCS_COP.1 Kriptográfiai művelet

5.2.3 PKI aláírás ellenőrzési csomag

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, aláírási algoritmus, aláíró nyilvános kulcs tanúsítványa, aláíró megkülönböztető neve (DN), aláírás dátuma és időpontja*** az aláírás ellenőrzés során.

Függések: nincsenek

FDP_DAU_SIG.1 Aláírás-blob ellenőrzése

Hierarchia szerint alárendelt-e más komponensnek: nem.

FDP_DAU_SIG.1.1 A TSF-nek a „Tanúsítási útvonal érvényesség ellenőrzése” csomagból az alábbi információkat kell használnia az aláírt adatok digitális aláírásának ellenőrzéséhez: alany nyilvános kulcs algoritmusa, alany nyilvános kulcsa, alany nyilvános kulcs paraméterei.

FDP_DAU_SIG.1.2 A TSF-nek ellenőriznie kell, hogy a keyUsage kiterjesztés kimenetben, a „Tanúsítási útvonal érvényesség ellenőrzése” csomagból, a nonRepudiation bit **(minősített tanúsítványok esetén)** be van-e kapcsolva.

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

a) az alany megkülönböztető neve (DN) a tanúsítási útvonal ellenőrzéséből megegyezik az aláírt adatban lévővel;

b) keyUsage, extKeyUsage kiterjesztésben az RFC 3280, RFC 3739, ETSI TS 101 862 v1.3.2, ETSI TS 102 280 v1.1.1, RFC 3161, RFC 2560 szabványokban leírtaknak megfelelő bit be van kapcsolva (pl. minősített tanúsítvány, időbélyegző tanúsítványa);

c) qCStatements kiterjesztés QcCompliance és QcSSCD értékeiben az ETSI TS 101 862 v1.3.2 szabványban leírtaknak megfelelő bit be van kapcsolva.

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

5.2.4 PKI alapú felhasználó hitelesítés csomag

5.2.4.1 FIA osztály – Azonosítás és hitelesítés

FIA_UAU.1;1 Hitelesítés időzítése – Távoli felhasználó

Hierarchikus alárendeltség más komponensekhez képest: nincs.

FIA_UAU.1.1;1 A TSF-nek lehetővé kell tennie a ***távoli felhasználó*** nevében végrehajtandó ***tevékenységeket: a paraméterek továbbítását a TOE függvényeit meghívó alkalmazás által (pl. SSL, TLS protokollal védett csatornán időbélyeg-szolgáltató elérése)***, mielőtt a ***távoli felhasználó*** hitelesítésre kerül.

FIA_UAU.1.2 A TSF megköveteli, hogy minden ***távoli felhasználó*** sikeresen hitelesítve legyen, mielőtt bármilyen más TSF által közvetített tevékenység történne a szóban forgó ***távoli felhasználó*** nevében.

Függések: FIA_UID.1 Azonosítás időzítése

FIA_UAU.4 Egyszer használatos hitelesítési mechanizmusok

Hierarchikus alárendeltség más komponensekhez képest: nincs.

FIA_UAU.4.1 A TSF-nek meg kell akadályoznia a ***SSL v3, TLS v1*** mechanizmusokhoz kapcsolódó hitelesítési adatok újrafelhasználását.

Függések: nincsenek.

FIA_UAU_SIG.1 Felhasználó hitelesítés

Hierarchikus alárendeltség más komponensekhez képest: nincs.

FIA_UAU_SIG.1.1 A TSF-nek a „Tanúsítási útvonal érvényesség ellenőrzése” csomagból az alábbi információkat kell felhasználnia az aláírás ellenőrzéséhez, melyet a távoli egyed a TSF kezdeményezésére válaszként ad: alany nyilvános kulcs algoritmusa, alany nyilvános kulcsa, alany nyilvános kulcs paraméterei.

FIA_UAU_SIG.1.2 A TSF-nek ellenőriznie kell, hogy a keyUsage kimenet a tanúsítási útvonal érvényesség ellenőrzése után beállítva tartalmazza-e a digitalSignature bitet **(hitelesítéshez használandó tanúsítványok esetén)**.

FIA_UAU_SIG.1.3 A TSF-nek az alábbi egyéb ellenőrzéseket kell végrehajtania:

a) össze kell hasonlítania a „Tanúsítási útvonal érvényesség ellenőrzése” csomag alany megkülönböztető nevét (DN) a hitelesítés alatt álló egyed megkülönböztető nevével (DN);

b) el kell végezni a kriptográfiai és egyéb adatok ellenőrzését a hitelesítéshez használt protokoll előírásai alapján.

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

FIA_UID.1;1 Azonosítás időzítése – Távoli felhasználó

Hierarchikus alárendeltség más komponensekhez képest: nincs.

FIA_UID.1.1;1 A TSF-nek lehetővé kell tennie a ***távoli felhasználó*** nevében végrehajtandó ***tevékenységeket: a paraméterek továbbítását a TOE függvényeit meghívó alkalmazás által (pl. SSL, TLS protokollal védett csatornán időbélyeg-szolgáltató elérése)***, mielőtt a ***távoli felhasználó*** azonosításra kerül.

FIA_UID.1.2;1 A TSF megköveteli, hogy minden ***távoli felhasználó*** sikeresen azonosítva legyen, mielőtt bármilyen más TSF által közvetített tevékenység történne a szóban forgó ***távoli felhasználó*** nevében.

Függések: nincsenek.

5.2.5 Valós idejű tanúsítvány állapot protokoll kliens csomag

5.2.5.1 FDP osztály – Felhasználói adatok védelme

FDP_DAU_OCS.1 Alap OCSP kliens

Hierarchikus alárendeltség más komponensekhez képest: nincs.

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

FDP_DAU_OCS.1.2 Az OCSP kérésnek tartalmaznia kell a következő kiterjesztéseket: ***nonce (a requestExtensions elemben)***.

FDP_DAU_OCS.1.3 A TSF-nek meg kell ismernie az OCSP válaszadó nyilvános kulcsát, algoritmusát és nyilvános kulcs paramétereit a következő forrásokból: ***megbízható pont, tanúsítványt aláíró CA, OCSP válaszadó tanúsítványa.***

FDP_DAU_OCS.1.4 A TSF –nek a következő egyéb funkciókat kell végrehajtania:

a) az OCSP válaszadó megbízhatóságának megállapítása a „Tanúsítási útvonal érvényesség ellenőrzése – Alap" csomag felhasználásával.

FDP_DAU_OCS.1.5 A TSF-nek ellenőriznie kell az OCSP válaszon lévő aláírást az OCSP válaszadó megbízható nyilvános kulcsának, algoritmusának és nyilvános kulcs paramétereknek a segítségével.

FDP_DAU_OCS.1.6 A TSF-nek ellenőriznie kell, hogy ha az OCSP válaszadó tanúsítványa tartalmazza az extKeyUsage kiterjesztést, akkor a kiterjesztés tartalmazza-e a PKIX OID-t OCSP-aláírásra.

FDP_DAU_OCS.1.7 A TSF-nek össze kell hasonlítania az OCSP válaszban szereplő válaszadó ID-t a válaszadó tanúsítványban található megfelelő információval.

FDP_DAU_OCS.1.8 A TSF-nek össze kell hasonlítania egy kérés certID-jét a singleResponse certID-vel.

FDP_DAU_OCS.1.9 A TSF-nek aktuálisnak kell elfogadnia az OCSP választ minden esetben, ha az alábbi szabály fennáll: ***aktuális idő <= létrehozás_ideje+x, ahol x-et az alábbi felhasználó adja meg: TOE függvényeit meghívó alkalmazás (pl. a jogi szabályozás alapján).***

FDP_DAU_OCS.1.10 A TSF-nek aktuálisnak kell elfogadnia az OCSP választ, ha az alábbi szabály fennáll: ***aktuális idő <= thisUpdate a tételre+x, ahol x-et az alábbi felhasználó adja meg: TOE függvényeit meghívó alkalmazás (pl. a jogi szabályozás alapján).***

FDP_DAU_OCS.1.11

A TSF-nek aktuálisnak kell elfogadnia az OCSP választ, ha az alábbi szabály fennáll: ***aktuális idő <= nextUpdate a tételre+x, ahol x-et az alábbi felhasználó adja meg: TOE függvényeit meghívó alkalmazás (pl. a jogi szabályozás alapján).***

FDP_DAU_OCS.1.12

A TSF-nek el kell utasítania az OCSP választ, ha a válasz olyan kritikus kiterjesztést tartalmaz, amelyet a TSF nem képes feldolgozni.

FDP_DAU_OCS.1.13

A TSF-nek az alábbi ellenőrzéseket kell még végrehajtania:

a) nonce kérés = nonce válasz,

b) OCSP válasz formátumának ellenőrzése RFC 2560 alapján.

Függések: FCS_COP.1 Kriptográfiai művelet,
FPT_STM.1 Megbízható időbélyegek

5.2.6 Tanúsítvány visszavonási lista (CRL) érvényesség ellenőrzés csomag

5.2.6.1 FDP osztály – Felhasználói adatok védelme

FDP_DAU_CRL.1 Alap CRL ellenőrzés

Hierarchia szerint alárendelt-e más komponensnek: nem.

FDP_DAU_CRL.1.1 A TSF-nek meg kell kapnia a CRL-t az alábbi helyek valamelyikéről: ***a CRL DP által mutatott pont a szóban forgó nyilvános kulcs tanúsítványban, az aláírásba ágyazva (ha előzőleg, a megfelelő időben kibocsátott CRL már beágyazásra került).***

FDP_DAU_CRL.1.2 A TSF-nek meg kell kapnia a CRL kibocsátójára vonatkozóan a megbízható nyilvános kulcsot, algoritmust és nyilvános kulcs paramétereket.

FDP_DAU_CRL.1.3 A TSF-nek ellenőriznie kell a CRL-en az aláírást a CRL kibocsátójának megbízható nyilvános kulcsa, az algoritmus és a nyilvános kulcs paraméterek ismeretében.

FDP_DAU_CRL.1.4 A TSF-nek ellenőriznie kell, hogy ha egy kritikus keyUsage kiterjesztés a CRL kibocsátó tanúsítványban jelen van, akkor a kiterjesztés cRLSign bitje be van-e kapcsolva a tanúsítványban.

FDP_DAU_CRL.1.5 A TSF-nek egyeztetnie kell a CRL-ben lévő kibocsátó mezőt a CRL feltételezett kibocsátójával.

FDP_DAU_CRL.1.6 A TSF-nek az alábbi szabályok teljesülése esetén kell elfogadnia aktuálisként a CRL-t**:** ***aktuális idő <= thisUpdate+ x ahol x-et a TOE függvényeit meghívó alkalmazás (pl. a jogi szabályozás alapján)*** adja meg.

FDP_DAU_CRL.1.7 A TSF-nek csak akkor szabad érvényesnek elfogadnia a CRL-t, ha fennáll az alábbi szabály: ***aktuális idő <= nextUpdate + x ahol x-et a TOE függvényeit meghívó alkalmazás (pl. a jogi szabályozás alapján)*** adja meg.

FDP_DAU_CRL.1.8 A TSF-nek nem szabad elfogadnia a CRL-t, ha a CRL olyan kritikus kiterjesztéseket tartalmaz, melyeket a TSF nem dolgoz fel.

FDP_DAU_CRL.1.9 A TSF-nek a következő további ellenőrzéseket is el kell végeznie:

a) CRL formátumának ellenőrzése RFC 3280 alapján.

Függések: FCS_COP.1 Kriptográfiai művelet,
FPT_STM.1 Megbízható időbélyegek

5.2.7 Naplózási csomag

5.2.7.1 FAU osztály – Biztonsági naplózás

FAU_GEN.1 Naplóadatok generálása

Hierarchia szerint alárendelt-e más komponensnek: nem.

FAU_GEN.1.1 A TSF-nek képesnek kell lennie naplóadatok generálására az alábbi események esetén:

a) a naplózási funkciók indítása és lezárása;
b) minden naplózandó esemény a ***nem specifikált (felhasználó által beállítható)*** szintű naplózáshoz; és
c) magánkulcs használata;
d) időbélyeg kérés;
e) időbélyeg válasz;
f) OCSP kérés;
g) OCSP válasz;
h) CRL letöltés;
i) hibaüzenetek, figyelmeztetések;

FAU_GEN.1.2 A TSF-nek a naplórekordon belül legalább az alábbi információkat kell rögzítenie:

a) dátum, idő, esemény típusa, alany azonosítása, esemény kimenetele (siker vagy sikertelenség), és
b) minden naplóesemény típusnál a PP/ST-ben szereplő funkcionális komponensek naplóesemény definíciójából kiindulva, a ***sikertelenség oka, tanúsítványnál alany megkülönböztető neve (DN), alany nyilvános kulcsa, tanúsítványnál, CRL-nél kibocsátó megkülönböztető neve (DN), hash algoritmus, hash érték, sorszám, aláíró algoritmus, kulcsméret, bináris aláírás, időbélyeg válasz, OCSP válasz, CRL, időbélyeg esetén nonce, beágyazott tanúsítvány, kiszolgáló IP-címe, állapot, OCSP válasz esetén nonce, thisUpdate, nextUpdate, kiszolgáló URL-je, állapot, CRL esetén thisUpdate, nextUpdate.***

Függések: FPT_STM.1 Megbízható időbélyegek

FAU_GEN.2 Felhasználói identitás csatolása

Hierarchia szerint alárendelt-e más komponensnek: nem.

FAU_GEN.2.1 A TSF-nek képesnek kell lennie, hogy minden naplózandó eseményhez hozzárendelje az eseményt kiváltó felhasználót.

Függések: FAU_GEN.1 Naplóadatok generálása
FIA_UID.1 Azonosítás időzítése

5.2.8 Folyamatos hitelesítés csomag

5.2.8.1 FIA osztály – Azonosítás és hitelesítés

FIA_UAU.6;1 Távoli felhasználó újrahitelesítése

Hierarchia szerint alárendelt-e más komponensnek: nem.

FIA_UAU.6.1;1 A TSF-nek újra hitelesítenie kell a ***távoli felhasználó***t a következő feltételek mellett: ***tranzakciónként.***

Függések: nincsenek.

FIA_UAU.6;2 Felhasználó újrahitelesítése

Hierarchia szerint alárendelt-e más komponensnek: nem.

FIA_UAU.6.1;2 A TSF-nek újra hitelesítenie kell a ***felhasználó***t a következő feltételek mellett: ***nincs feltétel.***

Függések: nincsenek.

5.2.9 Időbélyeg kérése és ellenőrzése csomag

5.2.9.1 FDP osztály – Felhasználói adatvédelem

FDP_DAU_TS.1 Időbélyeg kérés és ellenőrzés

Hierarchia szerint alárendelt-e más komponensnek: nem.

FDP_DAU_TS.1.1 A TSF-nek időbélyeg kérést kell összeállítania az alábbi mértékadó útmutatóban specifikált: ***RFC 3161*** alábbi formátumnak megfelelően: ***TimeStampReq.***

FDP_DAU_TS.1.2 A TSF-nek az időbélyeg kérést a TOE függvényeit meghívó alkalmazás által megadott időbélyeg szolgáltató felé kell kibocsátania.

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

a) version elem;
b) messageImprint elem (hash algoritmus objektum azonosítója, aláírandó adat lenyomata);
c) nonce elem;
d) certReq elem „TRUE” értékkel.

FDP_DAU_TS.1.4 A TSF-nek ellenőriznie kell, hogy az időbélyeg válasz megfelel-e az alábbi mértékadó útmutatóban definiált: ***RFC 3161*** alábbi formátumnak: ***TimeStampResp.***

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

a) ha az állapot (status elem értéke) nem „granted” vagy „grantedWithMods”, akkor nem szerepelhet a válaszban TimeStampToken;
b) ha az állapot (status elem értéke) nem „granted” vagy „grantedWithMods”, akkor a válaszban szerepelnie kell PKIFailureInfo hiba információnak;
c) ha az állapot (status elem értéke) „granted” vagy „grantedWithMods”, akkor a válaszban szerepelnie kell TimeStampToken objektumnak.

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

FDP_DAU_TS.1.7 A TSF-nek a ***TSA megbízhatóságának megállapítására*** tanúsítási útvonal érvényesség ellenőrzést kell végrehajtania a ***Tanúsítási útvonal érvényesség ellenőrzése (CPV) - Alap csomag*** felhasználásával.

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

FDP_DAU_TS.1.9 A TSF-nek ellenőriznie kell, hogy az időbélyeg válasz aláírásához használt tanúsítvány tartalmaz-e kritikus extKeyUsage kiterjesztést, és annak értéke „timeStamping”.

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

a) messageImprint elem azonosságát az időbélyeg kérés messageImprint elemének értékével,
b) ha a kérés tartalmazott TSAPolicyId elemet, akkor az azonos-e a válaszban kapott TSAPolicyId elem értékével.

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

Függések: FCS_COP.1 Kriptográfiai műveletek

5.3 EAL3 garanciaszint

Az alábbi táblázat az EAL3 szint garanciális követelményeit sorolja fel.

5.4 táblázat – Emelt szintű EAL3

Garanciaösszetevő azonosító	Garanciaösszetevő megnevezés
ACM_CAP.3	Engedélyek kezelése
ACM_SCP.1	TOE CM lefedettség
ADO_DEL.1	Szállítási eljárások
ADO_IGS.1	Telepítési, generálási, indítási eljárások
ADV_FSP.1	Informális funkcionális specifikáció
ADV_HLD.2	A biztonsági magas szintű terv
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

ACM_CAP.3 A feljogosító óvintézkedések

Függőségek:

- ACM_SCP.1 A TOE CM-lefedettsége
- ALC_DVS.1 A biztonsági intézkedések azonosítása

Fejlesztői tevékenységelemek:

- ACM_CAP.3.1D A fejlesztőnek kell hivatkozással ellátnia a TOE-t.
- ACM_CAP.3.2D A fejlesztőnek CM-rendszert kell használnia.
- ACM_CAP.3.3D A fejlesztőnek kell CM-dokumentációt szolgáltatnia.

Bizonyítékelemek tartalma és megjelenésmódja:

- ACM_CAP.3.1C A TOE hivatkozásának a TOE minden változatára egyedinek kell lennie.
- ACM_CAP.3.2C A TOE-t saját hivatkozásának megfelelő címkével kell ellátni.
- ACM_CAP.3.3C A CM dokumentációjának tartalmaznia kell egy konfigurációs listát és egy CM-tervet.
- ACM_CAP.3.4C A konfigurációs listának kell leírnia azokat a konfigurációs egységeket, amelyekből a TOE áll.
- ACM_CAP.3.5C A CM dokumentációjának kell leírnia azt a módszert, amelyet a TOE egyedi azonosítására használnak.
- ACM_CAP.3.6C A CM-rendszernek kell egyértelműen azonosítania minden konfigurációs egységet.
- ACM_CAP.3.7C A CM-tervnek kell leírnia azt, hogy hogyan lehet a CM-rendszert használni.
- ACM_CAP.3.8C A bizonyítéknak kell szemléltetnie, hogy a CM-rendszer a CM-terv szerint működik.
- ACM_CAP.3.9C A CM dokumentációjának kell bizonyítékot szolgáltatnia arról, hogy minden konfigurációs egységet hatékonyan tartottak és tartanak karban a CM-rendszer szerint.
- ACM_CAP.3.10C A CM-rendszernek úgy kell intézkedéseket tennie, hogy a konfigurációs egységeken csak feljogosított változtatásokat lehessen végezni.

Értékelői tevékenységelemek:

- ACM_CAP.3.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.

ACM_SCP.1 A TOE CM-lefedettsége

Függőségek:

- ACM_CAP.3 A feljogosító óvintézkedések

Fejlesztői tevékenységelemek:

- ACM_SCP.1.1D A fejlesztőnek kell a CM dokumentációjáról gondoskodnia.

Bizonyítékelemek tartalma és megjelenésmódja:

- ACM_SCP.1.1C A CM dokumentációjának kell megmutatnia, hogy a CM-rendszer legalább a következőket követi nyomon: a TOE kivitelezésének ábrázolása, tervezési dokumentáció, vizsgálati dokumentáció, felhasználói dokumentáció, adminisztrátori dokumentáció és CM dokumentáció.
- ACM_SCP.1.2C A CM dokumentációjának kell leírnia, hogy a konfigurációs egységeket a CM-rendszer hogyan követi nyomon.

Értékelői tevékenységelemek:

- ACM.SCP.1.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.

ADO_DEL.1 A kiszállítás eljárásai

Függőségek:

- Nincsenek függőségek.

Fejlesztői tevékenységelemek:

- ADO_DEL.1.1D A használó számára a fejlesztőnek kell dokumentálnia a TOE kiszállításának eljárásait vagy annak részeit.
- ADO_DEL.1.2D A fejlesztőnek használnia kell a kiszállítási eljárásokat.

A bizonyítékelemek tartalma és megjelenésmódja:

- ADO_DEL.1.1C A kiszállítási dokumentációnak kell leírnia minden olyan eljárást, amely a biztonság fenntartásához szükséges a TOE-nak a felhasználó telephelyére történő kiszállítása során.

Értékelői tevékenységelemek:

- ADO_DEL.1.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.

ADO_IGS.1 Hv-telepítés, Sv-telepítés, beindítás eljárásai

Függőségek:

- AGD_ADM.1 Az adminisztrátori útmutató

Fejlesztői tevékenységelemek:

- ADO_IGS.1.1D A fejlesztőnek kell dokumentálnia a biztonságos HV-telepítéshez, SV-telepítéshez és beindításhoz szükséges eljárásokat.

A bizonyítékelemek tartalma és megjelenésmódja:

- ADO_IGS.1.1C A dokumentációnak kell leírnia a biztonságos HV-telepítéshez, SV-telepítéshez és beindításhoz szükséges lépéseket.

Értékelői tevékenységelemek:

- ADO_IGS.1.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.
- ADO_IGS.1.2E Az értékelőnek úgy kell meghatároznia a HV-telepítés, az SV-telepítés és a beindítás eljárásait, hogy azok biztonságos konfigurációt eredményezzenek.

ADV_FSP.1 Informális funkcionális előírás

Függőségek:

- ADV_RCR.1 A kölcsönös megfelelés informális szemléltetése

Fejlesztői tevékenységelemek:

- ADV_FSP.1.1D A fejlesztőnek kell gondoskodnia a funkcionális előírásról.

Bizonyítékelemek tartalma és megjelenésmódja:

- ADV_FSP.1.1C A funkcionális előírásnak informális stílusban kell leírnia a TSF-et és annak külső interfészeit.
- ADV_FSP.1.2C A funkcionális előírásnak belsőleg ellentmondásmentesnek kell lennie.
- ADV_FSP.1.3C A funkcionális előírásnak kell leírnia valamennyi külső TSF interfész használatának célját és módszerét azzal, hogy alkalmas módon, kellő részletességel megadja a következmények, kivételek és hibaüzenetek részleteit.
- ADV_FSP.1.4C A funkcionális előírásnak teljes mértékben ábrázolnia kell a TSF-et.

Értékelői tevékenységelemek:

- ADV_FSP.1.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.
- ADV_FSP.1.2E Az értékelőnek kell meghatároznia, hogy a funkcionális előírás a TOE biztonsága funkcionális követelményeinek pontos és teljes megjelenítése.

ADV_HLD.2 Felsőszintű tervet érvényesítő biztonság

Függőségek:

- ADV_FSP.1 Informális funkcionális előírás
- ADV_RCR.1 A kölcsönös megfelelés informális szemléltetése

Fejlesztői tevékenységelemek:

- ADV_HLD.2.1D A fejlesztőnek kell gondoskodnia a TSF felsőszintű tervéről.

Bizonyítékelemek tartalma és megjelenésmódja:

- ADV_HLD.2.1C A felsőszintű terv ábrázolásának informálisnak kell lennie.
- ADV_HLD.2.2C A felsőszintű tervnek belsőleg ellentmondásmentesnek kell lennie.
- ADV_HLD.2.3C A felsőszintű tervnek kell leírnia a TSF alrendszerekkel kifejezett szerkezetét.
- ADV_HLD.2.4C A felsőszintű tervnek kell leírnia a TSF valamennyi alrendszere által ellátott biztonsági funkcionalitást.
- ADV_HLD.2.5C A felsőszintű tervnek kell azonosítania a TSF által megkövetelt valamennyi alárendelt hardvert, förmvert és/vagy szoftvert, a hardverben, förmverben vagy szoftverben kivitelezett támogató védelmi mechanizmusok által ellátott funkciók megjelenítésével.
- ADV_HLD.2.6C A felsőszintű tervnek kell azonosítania a TSF valamennyi alrendszerének interfészeit.
- ADV_HLD.2.7C A felsőszintű tervnek kell azonosítania a TSF alrendszereinek azokat az interfészeit, amelyek kívülről láthatók.
- ADV_HLD.2.8C A felsőszintű tervnek kell leírnia a TSF alrendszerei interfészei használatának célját és módszerét azzal, hogy alkalmas módon, kellő részletességel megadja a következmények, kivételek és hibaüzenetek részleteit.
- ADV_HLD.2.9C A felsőszintű tervnek kell leírnia a TOE felosztását TSP-t érvényesítő és más alrendszerekre.

Értékelői tevékenységelemek:

- ADV_HLD.2.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.
- ADV_HLD.2.2E Az értékelőnek kell meghatároznia, hogy a felsőszintű terv a TOE biztonsága funkcionális követelményeinek pontos és teljes megjelenítése.

ADV_RCR.1 A kölcsönös megfelelés informális szemléltetése

Függőségek:

- Nincsenek függőségek.

Fejlesztői tevékenységelemek:

- ADV_RCR.1.1D A fejlesztőnek kell gondoskodnia valamennyi redelkezésre bocsátott szomszédos TSF ábrázoláspár között a kölcsönös megfelelés elemzéséről.

Bizonyítékelemek tartalma és megjelenésmódja:

- ADV_RCR.1.1C Az elemzésnek kell szemléltetnie valamennyi redelkezésre bocsátott szomszédos TSF ábrázoláspár esetére, hogy a kevésbé elvont TSF ábrázolásban az elvontabb TSF ábrázolás valamennyi fontos biztonsági funkcionalitását helyesen és teljesen finomították.

Értékelői tevékenységelemek:

- ADV_RCR.1.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.

AGD_ADM.1 Az adminisztrátori útmutató

Függőségek:

- ADV_FSP.1 Informális funkcionális előírás

Fejlesztői tevékenységelemek:

- AGD_ADM.1.1D A fejlesztőnek kell szolgáltatnia az adminisztrátori útmutatót a rendszeradminisztrátori szervezetnek címezve.

A bizonyítékelemek tartalma és megjelenésmódja:

- AGD_ADM.1.1C Az adminisztrátori útmutatónak kell leírnia a TOE adminisztrátora számára elérhető adminisztratív funkciókat és interfészeket.
- AGD_ADM.1.2C Az adminisztrátori útmutatónak kell leírnia a TOE biztonságos adminisztrálásának módjait.
- AGD_ADM.1.3C Az adminisztrátori útmutatónak figyelmeztetéseket kell tartalmaznia azokra a funkciókra és jogosultságokra, amelyeket egy biztonságos feldolgozási környezetben ellenőrizni kell.
- AGD_ADM.1.4C Az adminisztrátori útmutatónak kell írnia az összes olyan feltevést, amely a TOE biztonságos működésének szempontjából fontos használói viselkedéshez kapcsolódik.

- AGD_ADM.1.5C Az adminisztrátori útmutatónak kell leírnia az összes, az adminisztrátor ellenőrzése alá tartozó paramétert, a megfelelő biztonságos értékek megjelölésével együtt.
- AGD_ADM.1.6C Az adminisztrátori útmutatónak kell leírnia minden egyes biztonsági szempontból fontos eseményt az adminisztratív funkciók viszonylatában, amelyeket el kell végezni, ideértve a TSF ellenőrzése alá tartozó entitások biztonsági jellemzőinek megváltoztatását is.
- AGD_ADM.1.7C Az adminisztrátori útmutatónak összhangban kell lennie a többi értékeléshez tartozó dokumentummal.
- AGD_ADM.1.8C Az adminisztrátori útmutatónak kell leírnia minden, az adminisztrátor szempontjából fontos követelményt, amely az IT környezetre vonatkozik.

Értékelői tevékenységelemek:

- AGD_ADM.1.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.

AGD_USR.1 A használói útmutató

Függőségek:

- ADV_FSP.1 Informális funkcionális előírás

Fejlesztői tevékenységelemek:

- AGD_USR.1.1D A fejlesztőnek kell szolgáltatnia a használói útmutatót.

A bizonyítékelemek tartalma és megjelenésmódja:

- AGD_USR.1.1C A használói útmutatónak kell leírnia a TOE nem-adminisztrátori használói számára elérhető funkciókat és interfészeket.
- AGD_USR.1.2C A használói útmutatónak kell leírnia A TOE által nyújtott, a használók számára elérhető biztonsági funkciókat.
- AGD_USR.1.3C A használói útmutatónak figyelmeztetéseket kell tartalmaznia azokra a funkciókra és jogosultságokra, amelyeket egy biztonságos feldolgozási környezetben ellenőrizni kell.
- AGD_USR.1.4C A használói útmutatónak világosan be kell mutatnia a használók minden felelősségét, amely a TOE biztonságos működéséhez kapcsolódik, ideértve azokat, amelyek a TOE biztonsági környezetének közleményében szerepelnek és a használó viselkedésével kapcsolatosak.
- AGD_USR.1.5C A használói útmutatónak összhangban kell lennie a többi értékeléshez tartozó dokumentummal.
- AGD_USR.1.6C A használói útmutatónak kell leírnia minden, a használó szempontjából fontos követelményt, amely az IT környezetre vonatkozik.

Értékelői tevékenységelemek:

- AGD_USR.1.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.

ALC_DVS.1 A biztonsági intézkedések azonosítása

Függőségek:

- Nincsenek függőségek.

Fejlesztői tevékenységelemek:

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

A bizonyítékelemek tartalma és megjelenésmódja:

- ALC_DVS.1.1C A fejlesztés biztonságáról szóló dokumentumnak kell leírnia azokat a fizikai, eljárásbeli, személyi és egyéb biztonsági intézkedéseket, amelyek szükségesek a TOE sértetlenségének és hitelességének védelméhez 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 a karbantartása során.

Értékelői tevékenységelemek:

- ALC_DVS.1.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.
- ALC_DVS.1.1E Az értékelőnek kell megerősítenie, hogy a biztonsági intézkedéseket betartják.

ALC_FLR.1 Alapszintű hibajavítás

Függőségek:

- Nincsenek függőségek.

Fejlesztői tevékenységelemek:

- ALC_FLR.1.1D A fejlesztőnek kell szolgáltatnia a hibajavítási eljárásokat tartalmazó dokumentációt.

A bizonyítékelemek tartalma és megjelenésmódja:

- ALC_FLR.1.1C A hibajavítási dokumentációnak kell leírnia a teendőket az azonosított biztonsági rések nyomon követéséhez a TOE minden egyes változatában.
- ALC_FLR.1.2C A hibajavítási eljárásoknak tartalmazniuk kell a biztonsági rések tulajdonságait és hatásait, valamint a rés kijavításának státuszát tartalmazó leírás meglétét.

- ALC_FLR.1.3C A hibajavítási eljárásoknak tartalmazniuk kell, hogy minden egyes biztonsági réshez javítási lépéseket kell azonosítani.
- ALC_FLR.1.4C A hibajavítási eljárásoknak kell leírniuk azokat a módszereket, amelyek a résekkel kapcsolatos információ, hibajavítások és a TOE használói számára szükséges hibajavítási és útmutató jellegű lépések biztosítására használatos.

Értékelői tevékenységelemek:

- ALC_FLR.1.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.

ATE_COV.2 A lefedettség elemzése

Függőségek:

- ADV_FSP.1 Informális funkcionális előírás
- ATE_FUN.1 Funkcionális vizsgálat

Fejlesztői tevékenységelemek:

- ATE_COV.2.1D A fejlesztőnek elemzést kell adnia a vizsgálat lefedettségére.

A bizonyítékelemek tartalma és megjelenésmódja:

- ATE_COV.2.1C A vizsgálat lefedettség elemzésének kell szemléltetnie, hogy a vizsgálati dokumentációban szereplő vizsgálat megfelel a TSF-nek a funkcionális előírásban leírtak szerint.
- ATE_COV.2.2C A vizsgálat lefedettség elemzésének kell szemléltetnie, hogy funkcionális előírásban leírtak szerinti TSF megfelel a vizsgálati dokumentációban leírt vizsgálatoknak, és hogy a vizsgálati dokumentáció teljes.

Értékelői tevékenységelemek:

- ATE_COV.2.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.

ATE_DPT.1 A felsőszintű terv vizsgálata

Függőségek:

- ADV_HLD.1 A felsőszintű terv leírása
- ATE_FUN.1 Funkcionális vizsgálat

Fejlesztői tevékenységelemek:

- ATE_DPT.1.1D A fejlesztőnek szolgáltatnia kell a vizsgálat alaposságének elemzését.

A bizonyítékelemek tartalma és megjelenésmódja:

- ATE_DPT.1.1C Az alaposságvizsgálatnak meg kell mutatnia, hogy a vizsgálati dokumentációban szereplő vizsgálatok elegendőek annak demonstráláshoz, hogy a TSF a saját felsőszintű tervének megfelelően működik.

Értékelői tevékenységelemek:

- ATE_DPT.1.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.

ATE_FUN.1 Funkcionális vizsgálat

Függőségek:

- Nincsenek függőségek.

Fejlesztői tevékenységelemek:

- ATE_FUN.1.1D A fejlesztőnek vizsgálnia kell a TSF-et és dokumentálnia kell az eredményeket.
- ATE_FUN.1.2D A fejlesztőnek szolgáltatnia kell a vizsgálati dokumentációt.

A bizonyítékelemek tartalma és megjelenésmódja:

- ATE_FUN.1.1C A vizsgálati dokumentációnak tartalmaznia kell a vizsgálati terv, a vizsgálati eljárások leírását, a várható és valós vizsgálati eredményeket.
- ATE_FUN.1.2C A vizsgálati tervnek azonosítania kell a vizsgálni kívánt funkciókat és le kell írnia a végrehajtandó vizsgálatok céljait.
- ATE_FUN1.3C A vizsgálati eljárások leírásának azonosítania kell a végrehajtandó vizsgálatokat és le kell írnia a vizsgálat forgatókönyvét minden egyes funkció esetében. Ezeknek a forgatókönyveknek tartalmazniuk kell a további vizsgálatok eredményeivel kapcsolatos soros függőségeket.
- ATE_FUN.1.4C A várható vizsgálati eredmények a vizsgálatok sikeres futtatása során keletkező várható kimeneti értékeket mutassák.
- ATE_FUN.1.5C A fejlesztő által végrehajtott vizsgálatok eredményeinek meg kell mutatniuk, hogy minden funkció előírás szerint működik.

Értékelői tevékenységelemek:

- ATE_FUN.1.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.

ATE_IND.2 Független vizsgálat – mintán

Függőségek:

- ADV_FSP.1 Informális funkcionális előírás
- AGD_ADM.1 Az adminisztrátori útmutató
- AGD_USR.1 A használói útmutató
- ATE_FUN.1 Funkcionális vizsgálat

Fejlesztői tevékenységelemek:

- ATE_IND.2.1D A fejlesztőnek kell szolgáltatnia a TOE-t a vizsgálathoz.

A bizonyítékelemek tartalma és megjelenésmódja:

- ATE_IND.2.1C A TOE-nek alkalmasnak kell lennie a vizsgálatra.
- ATE_IND.2.2C A fejlesztőnek a TSF funkcionális vizsgálata során használt erőforráskészlettel megegyező erőforráskészletet kell nyújtania.

Értékelői tevékenységelemek:

- ATE_IND.2.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.
- ATE_IND.2.2E Az értékelőnek meg kell vizsgálnia a TSF egy részhalmazát annak igazolására, hogy a TOE előírás szerint működik.
- ATE_IND.2.3E Az értékelőnek végre kell hajtania egy mintavizsgálatot a vizsgálati dokumentáción azért, hogy ellenőrizze a fejlesztői vizsgálati eredményeket.

AVA_MSU.1 Az útmutatós vizsgálata

Függőségek:

- ADO_IGS.1 A Hv-telepítés, a Sv-telepítés és a beindítás eljárásai
- ADV_FSP.1 Informális funkcionális előírás
- AGD_ADM.1 Az adminisztrátori útmutató
- AGD_USR.1 A használói útmutató

Fejlesztői tevékenységelemek:

- AVA_MSU.1.1D A fejlesztőnek kell szolgáltatnia az útmutatói dokumentációt.

A bizonyítékelemek tartalma és megjelenésmódja:

- AVA_MSU.1.1C Az útmutatói dokumentációnak azonosítania kell a TOE minden lehetséges műveleti módozatát (köztük azokat a műveleteket, amelyek egy hibát vagy működési rendellenességet követnek), a következményüket és a biztonságos működés karbantartására vonatkozó javaslatokat.

- AVA_MSU.1.2C Az útmutatói dokumentációnak teljesnek, érthetőnek, konzisztensnek és értelmesnek kell lennie.
- AVA_MSU.1.3C Az útmutatói dokumentációnak a várható környezettel kapcsolatban minden feltételezést tartalmaznia kell.
- AVA_MSU.1.4C Az útmutatói dokumentációnak tartalmaznia kell minden követelményt a külső biztonsági intézkedésekkel kapcsolatban (köztük az eljárási, fizikai és személyi vezérlőkkel).

Értékelői tevékenységelemek:

- AVA_MSU.1.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.
- AVA_MSU.1.2E Az értékelőnek meg kell ismételnie minden konfigurációs és telepítési eljárást annak megerősítésére, hogy a TOE konfigurálható és biztonságosan használható csupán a csatolt útmutatói dokumentáció használatával.
- AVA_MSU.1.3E Az értékelőnek meg kell határoznia, hogy az útmutatói dokumentáció lehetővé teszi az összes nem biztonságos állapot érzékelését.

AVA_SOF.1 A TOE biztonsági funkciója erősségének értékelése

Függőségek:

- ADV_FSP.1 Informális funkcionális előírás
- ADV_HLD.1 A felsőszintű terv leírása

Fejlesztői tevékenységelemek:

- AVA_SOF.1.1D A fejlesztőnek a TOE biztonsági funkcióerősség-elemzését minden olyan mechanizmuson el kell végeznie, amelyet az ST a TOE biztonsági funkcióerősség-igényként azonosít.

A bizonyítékelemek tartalma és megjelenésmódja:

- AVA_SOF.1.1C Minden olyan mechanizmus esetében, amely rendelkezik egy TOE biztonsági funkcióerősség-igénnyel, a TOE funkcióerősség-elemzésnek ki kell mutatni, hogy a mechanizmus eléri vagy túllépi a PP/ST-ben meghatározott legkisebb erősségi szintet.
- AVA_SOF.1.2C Minden egyes mechanizmus esetében, amely rendelkezik külön TOE biztonsági funkcióerősség-igénnyel, a TOE funkcióerősség-elemzésnek ki kell mutatni, hogy a mechanizmus eléri vagy túllépi a PP/ST-ben meghatározott legkisebb erősségi szintet.

Értékelői tevékenységelemek:

- AVA_SOF.1.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.
- AVA_SOF.1.2E Az értékelőnek kell megerősítenie, hogy az erősségi igények megfelelőek.

AVA_VLA.1 A sebezhetőség fejlesztői elemzése

Függőségek:

- ADV_FSP.1 Informális funkcionális előírás
- ADV_HLD.1 A felsőszintű terv leírása
- AGD_ADM.1 Az adminisztrátori útmutató
- AGD_USR.1 A használói útmutató

Fejlesztői tevékenységelemek:

- AVA_VLA.1.1D A fejlesztőnek végre kell hajtania és dokumentálnia kell a TOE szállítható elemeinek elemzését a TSP megsértésének nyilvánvaló módozatait kutatva.
- AVA_VLA.1.2D A fejlesztőnek dokumentálnia kell a nyilvánvaló sebezhetőségi pontok természetét.

A bizonyítékelemek tartalma és megjelenésmódja:

- AVA_VLA.1.1C A dokumentációnak meg kell mutatnia, hogy egyik azonosított sebezhetőségi pont sem használható ki a TOE várható környezetében.

Értékelői tevékenységelemek:

- AVA_VLA.1.1E Az értékelőnek kell megerősítenie, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó minden követelménynek.
- AVA_VLA.1.2E Az értékelőnek a fejlesztő sebezhetőségi elemzésén alapuló behatolási vizsgálatot kell végrehajtania annak biztosítására, hogy a nyilvánvaló sebezhetőségi pontok tárgyalásra kerültek.

6 TOE összefoglaló előírás

A TOE összefoglaló előírás a TOE által teljesítendő biztonsági követelményeket teljesítő biztonsági funkciókat tartalmazza. Leírja a TOE összes biztonsági funkcióját és garanciális intézkedését, amelyek a TOE biztonsági követelményeinek a kielégítéséhez járulnak hozzá.

6.1 A TOE biztonsági funkciói

A biztonsági funkciók (BF) 6 csoportba lettek sorolva:

- BF1 Lenyomat és digitális aláírás kezelése
- BF2 Tanúsítvány kezelése
- BF3 Időbélyeg kezelése
- BF4 OCSP kezelése
- BF5 CRL kezelése
- BF6 A TSF védelme és kezelése

6.1.1 BF1 Lenyomat és digitális aláírás kezelése

A „BF1 Lenyomat és digitális aláírás kezelése” biztonsági funkció végzi el a lenyomat készítésének, aszimmetrikus kódolás elkészítését, ellenőrzését.

A BF1 biztonsági funkció a kriptográfiai függvények meghívása előtt előkészíti az adatokat, a megfelelő formázásokat elvégzi rajtuk. A XAdES aláírások (ETSI TS 101 903 v1.2.2) esetében az XML struktúrába van beágyazva (pl. base64 kódoltan) az aláírásra megadott, tetszőleges formátumú állomány, adat, és emiatt csak a kanonikalizációs függvény, a C14N (W3C Canonical XML v1.0) meghívása után kerülhetnek átadásra az aláírandó adatok a lenyomatkészítő függvény számára.

Aláírás létrehozása esetén az eszköztől függően különböző módon történik meg a lenyomat elkészítése és az aszimmetrikus kódolás. A PKCS#12 állományok, mint „szoftver tokenek” (tanúsítvány és a hozzá tartozó magánkulcs egy csomagban, állomány formájában tárolódik a számítógépen) használata esetén a CryptoAPI bonyolítja le a titkos kulcshoz való hozzáférés engedélyezését (PIN kód bekérése külön ablakban). A TOE „hardver tokenek” esetén a CryptoAPI függvényein keresztül adja át az előkészített adatot az aláírás-létrehozó eszköznek (pl. intelligens kártya), és a CryptoAPI bonyolítja le az eszközön tárolt magánkulcshoz való hozzáférés engedélyezését (PIN kód bekérése külön ablakban). A hozzáférések engedélyezése után a CryptoAPI vagy az aláírás-létrehozó eszköz lefuttatja a megkapott aláírandó adaton a lenyomatkészítő függvényt (SHA-1), illetve a magánkulcs segítségével az aszimmetrikus kódolást (RSA). A szabványban leírtaknak megfelelően (IETF 3275) az http://www.w3.org/2000/09/xmldsig#rsa-sha1 (RSASSA-PKCS1-v1_5) azonosítóval ellátott aláírás-létrehozó algoritmust elsődlegesen támogatja a TOE. A CryptoAPI („szoftveres token” és „hardveres token” esetében egyaránt) ennek a folyamatnak az eredményét adja vissza a TOE-nak. A részfolyamat a memóriába esetlegesen bekerült bizalmas adatok (pl. PKCS#12 állományok esetén PIN kód, magánkulcs) memóriából való törlésével végződik.

Aláírás ellenőrzése során a lenyomat elkészítését a CryptoAPI végzi el a megadott azonosítóval ellátott lenyomatkészítő függvény alapján (pl. SHA-1), illetve szintén a CryptoAPI dekódolja a digitális aláírást (pl. RSA) a megadott tanúsítványból kinyert nyilvános kulcs révén. A lenyomatok összehasonlításával, az eredmény kiértékelésével a részfolyamat lezárul.

6.1.2 BF2 Tanúsítvány kezelése

A „BF2 Tanúsítványok kezelése” biztonsági funkció végzi el a tanúsítványok sértetlenségének és hitelességének, a tanúsítványlánc, illetve tartalmi megfelelőségének ellenőrzését.

A tanúsítványokat a kibocsátó ellátja saját titkos kulcsával létrehozott digitális aláírással, amely biztosítja a kibocsátott tanúsítvány sértetlenségét és hitelességét. A digitális aláírás és az érvényesség ellenőrzése a „BF1 Lenyomat és digitális aláírás kezelése”, „BF4 OCSP kezelése”, „BF5 CRL kezelése” biztonsági funkcióknál leírtak alapján történik.

A hitelesség ellenőrzését nemcsak a végfelhasználói tanúsítványra kell elvégezni, hanem a tanúsítványláncban szereplő összes elemre. A szolgáltatói tanúsítványoknál a visszavonási adatok ellenőrzése – az archív aláírások kivételével – nem szükséges, ezért a digitális aláírás és az érvényesség ellenőrzése a „BF1 Lenyomat és digitális aláírás kezelése” biztonsági funkcióknál leírtak alapján történik.

A tartalmi megfelelőség esetében a TOE megkülönbözteti az előírásoknak megfelelően a fokozott biztonságú és minősített tanúsítványt. A tanúsítványoknál a TOE figyeli az RFC 3280 szabványnak való (ASN.1 struktúra) megfelelőséget. A fokozott biztonságú tanúsítványoknál az alapvető elemek szükségesek az ellenőrzéshez, a „subject” és „issuer” mező (pl. a végfelhasználói tanúsítványban szereplő kibocsátó megkülönböztető neve megegyezik-e a kibocsátó tanúsítványában feltüntetett tulajdonosi megkülönböztető névvel), illetve a „validity” mező (pl. aláírás létrehozásának dátuma és időpontja a tanúsítvány érvényességi idején történt-e). Bizonyos esetekben más elemeket is kell vizsgálni, mint az „extKeyUsage” (pl. „timeStamping” bit) kiterjesztés. Minősített tanúsítvány esetén az alapvető elemeken kívül a „keyUsage” (pl. „nonRepudiation” bit), és „qCStatements” (pl. „QcCompliance” bit) kiterjesztéseket, illetve a „critical” jelzőket is kell az előírásoknak megfelelően ellenőrizni.

6.1.3 BF3 Időbélyeg kezelése

A „BF3 Időbélyeg kezelése” biztonsági funkció az időbélyeg kérések és válaszok létrehozását, küldését, fogadását, feldolgozását foglalja magában.

Az időbélyeg kéréseknél és válaszoknál a TOE figyeli az RFC 3161 szabványnak való (ASN.1 struktúra) megfelelőséget. Az időbélyeg kérések paraméterezése miatt a válaszban elvárt, hogy szerepeljen az időbélyeg szolgáltató tanúsítványa beágyazva. Az időbélyeg válaszon és a beágyazott időbélyeg tanúsítványon levő digitális aláírás ellenőrzése a „BF1 Lenyomat és digitális aláírás kezelése”, „BF2 Tanúsítvány kezelése” biztonsági funkcióknál leírtak alapján történik.

Az időbélyeg szolgáltatóhoz a távoli hozzáférés során a TOE támogatja a tanúsítványon alapuló felhasználó hitelesítést (pl. SSL v3.0, TLS v1.0).

6.1.4 BF4 OCSP kezelése

A „BF4 OCSP kezelése” biztonsági funkció az OCSP kérések és válaszok létrehozását, küldését, fogadását, feldolgozását foglalja magában.

Az OCSP kéréseknél és válaszoknál a TOE figyeli az RFC 2560 szabványnak való (ASN.1 struktúra) megfelelőséget. Az OCSP válaszon levő digitális aláírás ellenőrzése a „BF1 Lenyomat és digitális aláírás kezelése”, „BF2 Tanúsítvány kezelése” biztonsági funkcióknál leírtak alapján történik. A visszavonási adatoknál külön meg kell vizsgálni, hogy azok kiadásának dátuma és időpontja megfelelő-e. A visszavonási adatnak az aláírás létrehozásának dátumában és időpontjában kell tartalmaznia információt a kérdéses tanúsítványokról, amit az előírásokban a „kivárási idő” fogalmának betartása jelöl a visszavonási adatok beszerzésére vonatkozólag.

Az OCSP szolgáltatóhoz a távoli hozzáférés során a TOE támogatja a tanúsítványon alapuló felhasználó hitelesítést (pl. SSL v3.0, TLS v1.0).

6.1.5 BF5 CRL kezelése

A „BF5 CRL kezelése” biztonsági funkció a CRL elérését, lekérését, feldolgozását foglalja magában.

A CRL adatoknál a TOE figyeli az RFC 3280 szabványnak való (ASN.1 struktúra) megfelelőséget. A CRL adaton levő digitális aláírás ellenőrzése a „BF1 Lenyomat és digitális aláírás kezelése”, „BF2 Tanúsítvány kezelése” biztonsági funkcióknál leírtak alapján történik. A visszavonási adatoknál külön meg kell vizsgálni, hogy azok kiadásának dátuma és időpontja megfelelő-e. A visszavonási adatnak az aláírás létrehozásának dátumában és időpontjában kell tartalmaznia információt a kérdéses tanúsítványokról, amit az előírásokban a „kivárási idő” fogalmának betartása jelöl a visszavonási adatok beszerzésére vonatkozólag.

A CRL adatokat tároló hitelesítés-szolgáltatóhoz a távoli hozzáférés során a TOE támogatja a tanúsítványon alapuló felhasználó hitelesítést (pl. SSL v3.0, TLS v1.0).

6.1.6 BF6 A TSF védelme és kezelése

A „BF6 A TSF védelme és kezelése” biztonsági funkció a bizalmas adatok memóriában, tárolón való kezelését, a különböző biztonsági beállításokat és az események naplózását foglalja magában.

A memóriába esetlegesen bekerült bizalmas adatok (pl. PKCS#12 állományok esetén PIN kód, magánkulcs) memóriából való törlését külön függvények biztosítják, amelyek a használat után közvetlenül meghívódnak (a lenyomatkészítés és aszimmetrikus kódolás után, de a távoli hozzáférések, mint az időbélyeg szolgáltató elérése előtt).

A biztonsági beállítások között szerepelnek a kriptográfiához kötődő elemek, mint a támogatott, elvárt kulcshosszok, algoritmusok, illetve az egyéb, de a kriptográfiai adatok feldolgozása szempontjából alapvető elemek, mint a visszavonási adatokhoz kapcsolódó kivárási idő, távoli hozzáférések, szolgáltatók elérhetőségeinek beállításai.

A naplózásnál a titkos kulcshoz való hozzáféréshez, az időbélyeg kérések küldéséhez, válaszok fogadásához, az OCSP kérések küldéséhez, válaszok fogadásához, a CRL adatok letöltéséhez, illetve a különböző hibajelenségekhez kapcsolódó üzenetek kerülnek biztonságos módon tárolásra.

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

A XadesMagic 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;
- fejlesztői útmutató;
- konfiguráció menedzselés dokumentáció;
- teszt dokumentáció és teszt szoftver.

A XadesMagic fejlesztése egy változáskezelő szoftver segítségével történik, mely egy szervergépen keresztül érhető el. Ennek védelme biztosítja, hogy csak engedélyezett módosítások történhessenek a fejlesztés alatt álló szoftveren. A XadesMagic termékhez verziószámot rendelnek, az értékelés során egyértelműen látható, hogy mely verzió értékelését végzik az értékelők.

A konfiguráció kezelési tervről készült leírás:

"XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – A konfiguráció menedzselés dokumentációja"

6.2.2 Kiszállítás és működtetés

A XadesMagic szállításával és használatával kapcsolatos eljárások leírását a "XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – Szállítási dokumentáció" című dokumentum tartalmazza.

6.2.3 Fejlesztés

Az informális funkcionális specifikáció megfogalmazza a XadesMagic fő biztonsági funkcióit, a külső interfészeket, ezek célját. Az informális specifikációt leíró dokumentum:
"XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – Funkcionális specifikáció"

A magas szintű terv informális eszközökkel leírja a fejlesztés alatt álló rendszer fő elemeit, a közöttük lévő kapcsolatokat. Az erről készült leírás:
"XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – Magas szintű terv"

Az informális megfelelés elemzés bemutatja, hogy a magasabb szintű informális leírásokban megadott biztonsági funkciókat hogyan valósítják meg az alacsonyabb szinteken, azaz hogyan felel meg egymásnak például a funkcionális specifikáció és a magas szintű terv. Az erről készült leírás:
"XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – Megfeleltetés elemzések"

6.2.4 Útmutató dokumentumok

A TOE felhasználói (alkalmazásfejlesztők) számára készült dokumentumok:
"XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – Fejlesztői útmutató"

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 "XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – A fejlesztési biztonság dokumentációja" leírás tartalmazza a fejlesztők által az értékelés tárgya fejlesztése során alkalmazott szabályok leírását.

6.2.6 Tesztelés

A XadesMagic teszteléséhez az alábbi, teszteléssel kapcsolatos dokumentumok készültek:
"XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – Tesztelési dokumentáció"

"XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – Teszt lefedettség elemzés"

"XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 – Teszt mélység elemzés"

6.2.7 Sebezhetőségek felmérése

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

A fejlesztői sebezhetőségi elemzést az alábbi dokumentum tartalmazza:
"XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 - Sebezhetőség elemzés"

7 PP megfelelőség

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

8 Indoklások

Ez a fejezet tartalmazza azon indoklásokat, melyek megmutatják, hogy a TOE valóban kivédi a számításba vett veszélyeket és teljesíti a biztonsági céljait. Mivel a TOE 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 a KHE eszköz és annak meghajtó programjai.

8.1 A biztonsági célok indoklása

8.1.1 Az alap (egyúttal a környezetre vonatkozó) biztonsági célok indoklása

A 8.1 táblázat a feltételezéseket és az alap fenyegetéseket képezi le a (környezetre vonatkozó) alap biztonsági célokra, megmutatva, hogy minden feltételezéshez és fenyegetéshez tartozik legalább egy biztonsági cél. A 8.2 táblázat az alap biztonsági célokat rendeli a feltételezésekhez és a fenyegetésekhez, bizonyítván, hogy minden biztonsági célhoz tartozik legalább egy feltételezés vagy fenyegetés.

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

Feltételezés/veszély	**Célok**
AE.Authorized_Users	OE.Authorized_Users
AE.Configuration	OE.Configuration
AE.Crypto_Module	OE.Crypto
AE.PKI_Info	OE.PKI_Info
AE.Physical_Protection	OE.Physical_Security
AE.Time	OE.Time
AE.Timestamp	OE.TimeStamp
T.Attack	OE.DAC
T.Audit_Excess	OE.Audit_Select
T.Audit_Fill	OE.Audit_Select
T.Audit_Modify	OE.Audit_Protect
T.Audit_Unreadable	OE.Audit_Readable
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 fg
T.Private_Key	OE.DAC
T.Role	OE.Security_Roles
T.Secure_Attributes	OE.Secure_Attributes
T.Shoulder_Surf	OE.No_Echo
T.Tries	OE.Limit_Tries

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

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

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

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

AE.Crypto_Module: a TOE környezetről feltételezzük, hogy tartalmaz egy vagy több megbízható kriptográfiai modult (pl. CryptoAPI, OpenSSL), mely modul vagy modulok a kriptográfiai műveleteke hajtják végre. A feltételezésből származtatott biztonsági cél:

- **OE.Crypto**: a környezetnek tartalmaznia kell egy vagy több kriptográfiai modult (pl. CryptoAPI, OpenSSL), mely modul vagy modulok a kriptográfiai műveleteket hajtjk végre.

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 megvédi a TOE-t 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: az időbélyeg válasz a TOE rendelkezésére állnak A feltételezésből származtatott biztonsági cél:

- **OE.TimeStamp**: az IT környezetnek biztosítania kell a TOE számára az időbélyegzés szolgáltatóhoz való hozzáférését.

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.Audit_Excess: a biztonsági napló túl sok adatot tartalmaz az értékelhető elemzéshez. A veszélyből származtatott biztonsági cél:

- **OE.Audit_Select**: a TSF-nek lehetővé kell tennie a jogosult felhasználók számára a naplózandó események kiválasztását.

T.Audit_Fill: a biztonsági napló túl gyorsan betelik, így nem tölti be célját. A veszélyből származtatott biztonsági cél:

- **OE.Audit_Select**: a TSF-nek lehetővé kell tennie a jogosult felhasználók számára a naplózandó események kiválasztását.

T.Audit_Modify a biztonsági naplórekordok nem megbízhatóak, mert jogosulatlan módosításnak lehetnek kitéve. A veszélyből származtatott biztonsági cél:

- **OE.Audit_Protect**: a TSF-nek meg kell védenie a biztonsági naplófájlt a jogosulatlan módosítástól. Az IT környezet által nyújtott védelmen túlmenően a TOE is biztosítja a naplórekordok módosításának észlelhetőségét kriptográfiai lenyomatképző (hash) algoritmusok használata révén.

T.Audit_Unreadable a biztonsági naplóállomány nem olvasható és értelmezhető emberi felhasználó számára, így nem lehet a biztonsági szempontból fontos eseményeket vizsgálni. A veszélyből származtatott biztonsági cél:

- **OE.Audit_Readable**: a TSF-nek képesnek kell lennie humán felhasználó által olvasható formára hozni a naplórekordokat.

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

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

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

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

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

- **OE.Self_Protect:** a TSF-nek a saját futásához egy tartományt kell kezelnie, melyet és melynek értékeit védi a külső beavatkozástól, hamisítástól vagy jogosulatlan felfedéstől.
- **OE.DAC**: a TSF-nek ellenőriznie és korlátoznia kell a felhasználók hozzáféréseit a TOE értékekhez, egy megadott hozzáférés ellenőrzési szabályzatnak megfelelően.

- **OE.Protect_I&A_Data**: a TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie az I&A adatok módosítását.
- **OE.Trust_Anchor**: a TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie a megbízható pontok karbantartását.
- **OE.TSF_Data**: a TSF-nek csak a jogosult felhasználók számára szabad lehetővé tennie a TSF adatok módosítását.

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

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

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

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

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

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

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

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

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

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

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

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

A 8.2 táblázat a környezetre vonatkozó biztonsági célokat visszavezeti a feltételezésekre és a efnyegetésekre, ami azt mutatja meg, hogy minden biztonsági cél visszavezethető legalább egy feltételezésre vagy veszélyre. Az indoklás az előző, itt már nem ismételjük meg.

8.2 táblázat – A környezeti biztonsági célok leképezése feltételezésekre és fenyegetésekre

Cél	**Feltételezés/veszély**
OE.Audit_Protect	T.Audit_Modify
OE.Audit_Readable	T.Audit_Unreadable
OE.Audit_Select	T.Audit_Excess T.Audit_Fill
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.I&A,	T.Imperson
OE.Limit_Actions_Auth	T.Imperson
OE.Protect_I&A_Data	T.Modify
OE.Init_Secure_Attr	T.Object_Init
OE.Security_Roles	T.Role
OE.Secure_Attributes	T.Secure_Attributes
OE.No_Echo	T.Shoulder_Surf
OE.Limit_Tries	T.Tries
OE.Self_Protect	T.Modify
OE.Trust_Anchor	T.Modify
OE.TSF_Data	T.Modify

8.1.2 A biztonsági célok indoklása a csomagokra

A csomagokban szereplő alábbi biztonsági célok kivétel nélkül mind a TOE-ra vonatkoznak.

8.1.2.1 CPV – Alap csomag biztonsági céljainak indoklása

8.3 táblázat – A veszélyek leképezése célokra a CPV – Alap csomag esetén

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

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

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

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

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

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

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

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

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

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

- **O.Path_Find**: a TSF-nek képesnek kell lennie a tanúsítási útvonal felépítésére egy megbízható ponttól az előfizetőig.

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.

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

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

8.1.2.2 PKI aláírás létrehozás csomag biztonsági céljainak indoklása

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

Sorszám	Veszély	Célok
1	T.Clueless_PKI_Sig	O.Give_Sig_Hints

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

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

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

Sorszám	Célok	Veszély
1	O.Give_Sig_Hints	T.Clueless_PKI_Sig

8.1.2.3 PKI aláírás ellenőrzési csomag biztonsági céljainak indoklása

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

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

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

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

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

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

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

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

8.1.2.4 A PKI alapú felhasználó hitelesítés csomag biztonsági céljainak indoklása

8.9 táblázat A veszélyek leképezése célokra a PKI alapú felhasználó hitelesítés csomag esetén

Sorszám	Veszély	Célok
1	T.Assumed_Identity_Auth	O.Linkage, O.I&A_Remote, O.Limit_Actions_Auth_Remote
2	T.Replay_Entity	O.Single_Use_I&A

T.Assumed_Identity_Auth: Egy felhasználó egy másik felhasználónak adja ki magát, hogy végrehajthasson egy PKI alapú felhasználó hitelesítést. A veszélyből származtatott biztonsági cél:

- **O.Linkage:** A TSF-nek a megfelelő felhasználói nyilvános kulcsot kell használnia a hitelesítéshez.
- **O.I&A_Remote**: A TSF-nek egyértelműen azonosítania kell az összes távoli egyedet, és hitelesítenie kell azok állítólagos azonosságát, mielőtt egy távoli egyednek hozzáférést engedélyezne a TOE szolgáltatásokhoz és erőforrásokhoz.
- **O.Limit_Actions_Auth_Remote**: A TSF-nek korlátoznia kell azokat a tevékenységeket, melyeket egy távoli egyed végrehajthat az előtt, mielőtt a TSF ellenőrizné a távoli egyed azonosságát.

T.Replay_Entity: Egy jogosulatlan felhasználó visszajátszik egy érvényes hitelesítő adatot. A veszélyből származtatott biztonsági cél:

- **O.Single_Use_I&A**: A TSF-nek olyan azonosítási és hitelesítési (I&A) mechanizmusokat kell alkalmaznia, amelyek egyedi hitelesítési információkat követelnek meg minden egyes I&A esetén.

8.10 táblázat A célok leképezése veszélyekre a PKI alapú felhasználó hitelesítés csomag esetén

Sorszám	Célok	Veszélyek
1	O.I&A_Remote	T.Assumed_Identity_Auth
2	O.Limit_Actions_Auth_Remote	T.Assumed_Identity_Auth
3	O.Linkage	T.Assumed_Identity_Auth
4	O.Single_Use_I&A	T.Replay_Entity

8.1.2.5 A valós idejű tanúsítvány állapot protokoll kliens csomag biztonsági céljainak indoklása

8.11 táblázat A veszélyek leképezése célokra az OCSP csomag esetén

Sorszám	Veszély	Célok
1	T.Replay_OCSP_Info	O.Fresh_OCSP_Info
2	T.Wrong_OCSP_Info	O.Accurate_OCSP_Info, O.Auth_OCSP_Info

T.Replay_OCSP_Info: A felhasználó egy régi OCSP választ fogad el, amelynek következtében elfogad egy már visszavont tanúsítványt az OCSP tranzakcióhoz. A veszélyből származtatott biztonsági cél:

- **O.Fresh_OCSP_Info:** A TSF-nek csak valószerűen aktuális OCSP válaszokat szabad elfogadnia.

T.Wrong_OCSP_Info: A felhasználó elfogad egy visszavont tanúsítványt, vagy visszautasít egy érvényes tanúsítványt, egy helytelen OCSP válasz következtében. A veszélyből származtatott biztonsági cél:

- **O.Accurate_OCSP_Info:** A TSF-nek csak a pontos OCSP válaszokat szabad elfogadnia.
- **O.Auth_OCSP_Info:** A TSF-nek el kell fogadnia a jogosult forrásból származó OCSP válaszokat.

8.12 táblázat A célok leképezése veszélyekre az OCSP csomag esetén

Sorszám	Célok	Veszélyek
1	O.Accurate_OCSP_Info	T.Wrong_OCSP_Info
2	O.Auth_OCSP_Info	T.Wrong_OCSP_Info
3	O.Fresh_OCSP_Info	T.Replay_OCSP_Info

8.1.2.6 A CRL ellenőrzés csomag biztonsági céljainak indoklása

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

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

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

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

T.Wrong_Revoc_Info_CRL: a felhasználó elfogadhat lejárt tanúsítványt vagy visszautasíthat érvényes tanúsítványt helytelen visszavonási információk miatt. A veszélyből származtatott biztonsági cél:

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

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

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

8.1.2.7 A naplózás menedzsment csomag biztonsági céljainak indoklása

8.15 táblázat – A veszélyek leképezése célokra a naplózás menedzsment csomag esetén

Sorszám	Veszély	Célok
1	T.Accountability	O.Audit_User
2	T.No_Audit	O.Audit

T.Accountability: a biztonsági szempontból fontos naplózott események nem köthetők egyedi tevékenységhez. A veszélyből származtatott biztonsági cél:

- **O.Audit_User**: a TSF-nek képesnek kell lennie a naplózott eseményeket egyedi felhasználókhoz kötni.

T.No_Audit: nincs biztonsági napló a biztonsági szempontból jelentőséggel bíró események vizsgálatához. A veszélyből származtatott biztonsági cél:

- **O.Audit:** a TSF-nek naplóznia kell a biztonsági szempontból fontos eseményeket.

8.16 táblázat – A célok visszavezetése veszélyekre a Naplózás menedzsment csomag esetén

Sorszám	Célok	Veszélyek
1	O.Audit	T.No_Audit
2	O.Audit_User	T.Accountability

8.1.2.8 A folyamatos hitelesítés csomag biztonsági céljainak indoklása

8.17 táblázat – A veszélyek leképezése célokra a folyamatos hitelesítés csomag esetén

Sorszám	Veszély	Célok
1	T.Hijack	O.Continuous_I&A

T.Hijack: Egy jogosulatlan felhasználó eltérít egy hitelesített munkaszakaszt. A veszélyből származtatott biztonsági cél

- **O.Continuous_I&A**: A TSF-nek folyamatosan hitelesítenie kell a felhasználót.

8.18 táblázat – A célok visszavezetése veszélyekre a folyamatos hitelesítés csomag esetén

Sorszám	Célok	Veszélyek
1	O.Continuous_I&A	T.Hijack

8.1.2.9 Az időbélyeg kérése és ellenőrzése csomag biztonsági céljainak indoklása

8.19 táblázat – A veszélyek leképezése célokra az időbélyeg kérése és ellenőrzése csomag esetén

Sorszám	Célok	Veszélyek
1	T.Replay_TimeStamp	O.Fresh_TimeStamp_Info
2	T.Wrong_TimeStamp_Info	O.Accurate_TimeStamp_Info O.Auth_TimeStamp_Info

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

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

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

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

8.19 táblázat – A célok visszavezetése veszélyekre az időbélyeg kérése és ellenőrzése csomag esetén

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

8.2 A biztonsági követelmények indoklása

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

8.2.1 A funkcionális biztonsági követelmények indoklása

Az összes biztonsági cél funkcionális követelményekre vagy feltételezésekre való leképezését mutatja a 8.19 táblázat. Az alap TOE funkcionális követelmények leképezéséhez és a csomagokhoz az indoklásokat külön alfejezetek tartalmazzák. Az explicit módon megfogalmazott követelmények jellegükben hasonlóak a CC 2. rész követelményeihez, így a CC 3. rész garanciális követelményei alkalmazhatók ezek tesztelésére is, a CC 3. részén kívüli garanciális követelményre nincs szükség.

8.20 táblázat – A biztonsági célok leképezése funkcionális követelményekre

Sorszám	Biztonsági cél	Funkcionális komponens
A környezetre vonatkozó biztonsági célok leképezése		
1	OE.Audit_Protect	FAU_STG.1
2	OE.Audit_Readable	FAU_SAR.1
3	OE.Audit_Select	FAU_SEL.1
4	OE.DAC	FDP_ACC.1, FDP_ACF.1
5	OE.Invoke	FPT_RVM.1
6	OE.I&A	FIA_ATD.1, FIA_UAU.1, FIA_UID.1
7	OE.Init_Secure_Attr	FMT_MSA.3
8	OE.Limit_Actions_Auth	FIA_UAU.1, FIA_UID.1
9	OE.Limit_Tries	FIA_AFL.1
10	OE.No_Echo	FIA_UAU.7
11	OE.Protect_I&A_Data	FMT_MTD.1, FMT_SMF.1
12	OE.Secure_Attributes	FMT_MSA.1, FMT_SMF.1
13	OE.Security_Roles	FMT_SMR.2
14	OE.Self_Protect	FPT_SEP.1
15	OE.Trust_Anchor	FMT_MTD.1, FMT_SMF.1
16	OE.TSF_Data	FMT_MTD.1, FMT_SMF.1
17	OE.Authorized_Users	Az adminisztrátori és felhasználói útmutatóban megadva (AGD_ADM.1 és AGD_USR.1) – nem a TOE-ra vonatkozólag
18	OE.Configuration	Az indítási és telepítési útmutatóban megadva (ADO_IGS.1) – nem a TOE-ra vonatkozólag
19	OE.Crypto	FCS_CRM_FPS.1
20	OE.Physical_Security	A fizikai biztonsági szabályok részeként definiálva az AGD_ADM.1 és AGD_USR.1 összetevőkben.
21	OE.PKI_Info	FDP_ITC_PKI_INF.1
22	OE.Time	FPT_STM.1
23	OE.TimeStamp	FDP_ITC_PKI_INF.1.1

CPV – Alap csomag céljainak leképezése		
1	O.Correct_Time	FDP_DAU_CPV_INI.1
2	O.Current_Certificate	FDP_DAU_CPV_CER.1
3	O.Get_KeyInfo	FDP_DAU_CPV_OUT.1
4	O.Path_Find	FDP_CPD.1
5	O.Trusted_Keys	FDP_DAU_CPV_INI.1
6	O.User	FDP_DAU_CPV_CER.2
7	O.Verified_Certificate	FDP_DAU_CPV_CER.1
8	O.Valid_Certificate	FDP_DAU_CPV_CER.1
A PKI aláírás létrehozás csomag céljainak leképezése		
1	O.Give_Sig_Hints	FDP_ETC_SIG.1
A PKI aláírás ellenőrzés csomag céljainak leképezése		
1	O.Use_Sig_Hints	FDP_ITC_SIG.1,
2	O.Linkage_Sig_Ver	FDP_DAU_SIG.1
A PKI alapú felhasználó hitelesítés céljainak leképezése		
1	O.I&A_Remote	FIA_UAU.1;1, FIA_UID.1;1
2	O.Limit_Actions_Auth_Remote	FIA_UAU.1;1, FIA_UID.1;1
3	O.Linkage	FIA_UAU_SIG.1
4	O.Single_Use_I&A	FIA_UAU.4
Az OCSP kliens csomag céljainak leképezése		
1	O.Accurate_OCSP_Info	FDP_DAU_OCS.1
2	O.Auth_OCSP_Info	FDP_DAU_OCS.1
3	O.Fresh_OCSP_Info	FDP_DAU_OCS.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
A naplózás menedzsment csomag céljainak leképezése		
1	O.Audit	FAU_GEN.1
2	O.Audit_User	FAU_GEN.2
A folyamatos hitelesítés csomag céljainak leképezése		
1	O.Continuous_I&A	FIA_UAU.6:1, FIA_UAU.6:2
Az időbélyeg kérése és ellenőrzése csomag céljainak leképezése		
1	O.Fresh_TimeStamp_Info	FDP_DAU_TS.1
2	O.Accurate_TimeStamp_Info	FDP_DAU_TS.1
3	O.Auth_TimeStamp_Info	FDP_DAU_TS.1

8.2.1.1 Biztonsági célok a környezetre - indoklás

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.

O.Audit_Protect: a TSF-nek meg kell védenie a biztonsági naplófájlt a jogosulatlan módosítástól. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FAU_STG.1, Védett naplóállomány tárolás: a TSF-nek meg kell védenie a naplórekordokat a jogosulatlan törléstől és módosítástól, ahogyan azt az ST írója meghatározza.

O.Audit_Readable: a TSF-nek képesnek kell lennie humán felhasználó számára olvasható formára hozni a naplórekordokat. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FAU_SAR.1, napló megtekintés: a TSF-nek képesnek kell lennie a naplóadatokból jelentés készítésére, mely egy felhasználó számára olvasható formátumú, és értelmezhetőek a benne szereplő adatok.

O.Audit_Select: a TSF-nek lehetővé kell tennie a jogosult felhasználók számára a naplózandó események kiválasztását. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FAU_SEL.1, Szelektív napló: a TSF a jogosult felhasználók számára biztosítja, hogy azok kiválaszthassák a naplózandó eseményeket.

OE.DAC: a 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 azon szubjektumokra, objektumokra és műveletekre, melyeket az ST szerzője megadott. Az objektum és szubjektum a TOE általános elemeit jelentik. Egy megvalósítandó biztonsági szabály esetén ezeket az egyedeket az ST írójának egyértelműen azonosítani kell. A legtöbb rendszernél csak egyféle szubjektum típus van, melyet általában folyamatnak vagy feladatnak (process, task) hívnak, melyet az ST-ben specifikálni kell. Az ST szerzőjének meg kell adnia az SFP által értelmezett szubjektumok, objektumok és a közöttük lévő műveletek listáját. Ez a követelmény egy hozzáférés ellenőrzési szabályzat specifikálását igényli.
- 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.
- FDP_RIP.1, Részhalmazra vonatkozó maradványinformáció-védelem, amely megköveteli, hogy a bizalmas adatok a használat után elérhetetlenné váljanak, az esetlegesen (pl. PKCS#12 állomány esetén) memóriába kerülő magánkulcs, PIN kód az aszimmetrikus kódolás után törlődik.

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. 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_UAU.1, Hitelesítés időzítése, amely megköveteli, hogy a TSF tegye lehetővé azt, hogy az ST szerzője megadja azon TSF által közvetített tevékenységek listáját, 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.
- FIA_UID.1, Azonosítás időzítése, amely megköveteli, hogy a TSF tegye lehetővé azt, hogy az ST szerzője megadja azon TSF által közvetített tevékenységek listáját, 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.

OE.Init_Secure_Attr: a 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. A TSF-nek lehetővé kell tennie, hogy az ST írója által megadott szerepkörök alternatív kezdeti értékkel írják felül az alapértelmezett értékeket egy objektum vagy információ létrehozásakor. Ez a követelmény azt biztosítja, hogy egy objektum létrejöttekor érvényes alapértelmezett biztonsági tulajdonságok legyenek megadva.

OE.Invoke: kimondja, hogy a TSF-nek minden tevékenység esetén meg kell hívódnia. 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: a 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_UAU.1, Hitelesítés időzítése, amely megköveteli, hogy a TSF tegye lehetővé azt, hogy az ST szerzője megadja azon TSF által közvetített tevékenységek listáját, 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.

- FIA_UID.1, Azonosítás időzítése, amely megköveteli, hogy a TSF tegye lehetővé azt, hogy az ST szerzője megadja azon TSF által közvetített tevékenységek listáját, 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.

OE.Limit_Tries: a 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 (ST szerző által definiált) sikertelen hitelesítési kísérlet történik az ST írója által megadott hitelesítési folyamatban. Amikor a megadott darabszámot eléri vagy meghaladja a sikertelen kísérletek száma, a TSF az ST szerzője által előírt műveletet hajtja végre. Ez a PKE PP követelmény korlátozza az egymás utáni sikertelen hitelesítési próbálkozások számát.

OE.No_Echo: a 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 az ST szerzője által megadott 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, amely megköveteli, hogy a TSF az ST írója által definiált szerepkörökre korlátozza az ST szerzője által megadott műveletek végrehajtását az ST írója által definiált adatokon. A követelmény célja, hogy a jogosult felhasználók és műveleteik megadott TSF adatokra (beleértve az azonosítási és hitelesítési adatokat) legyenek megadva.
- FMT_SMF.1, Menedzsment funkciók megadása, amely megköveteli, hogy a TSF képes legyen biztonsági menedzsment funkciók végrehajtására.

OE.Secure_Attributes: a 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 az ST szerzője által megadott műveletek végrehajtásának az ST író által megadott szerepkörökre való korlátozása érdekében az ST szerzője által definiált biztonsági tulajdonságok vonatkozásában. 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: a 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 a 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 kezel saját futásához egy biztonsági tartományt, 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 a 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, amely megköveteli, hogy a TSF az ST írója által definiált szerepkörökre korlátozza az ST szerzője által megadott műveletek végrehajtását az ST írója által definiált adatokon. 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, amely megköveteli, hogy a TSF az ST írója által definiált szerepkörökre korlátozza az ST szerzője által megadott műveletek végrehajtását az ST írója által definiált adatokon. 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.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 környezetnek tartalmaznia kell egy vagy több megbízható kriptográfiai modult (pl. CryptoAPI), mely modul vagy modulok a kriptográfiai műveleteket hajtják végre.
Ezt a célt az AE.Crypto_Module elégíti ki, azaz egy feltételezés, amely kimondja, hogy a környezet tartalmaz egy vagy több megbízható kriptográfiai modult, mely modul vagy modulok a kriptográfiai műveleteket hajtják végre. Az alábbi követelmény valósítja meg a cél teljesülését:

- FCS_CRM_FPS.1, Az IT környezet TSF számára minden kriptográfiai modulnak minősített elektronikus aláírás létrehozása esetén NHH által nyilvántartásba vett, 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 e 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, CRL-ek, OCSP válaszok és időbélyeg válaszok igény esetén 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: az IT környezetnek biztosítania kell a TOE számára az időbélyegzés szolgáltatóhoz való hozzáférést. 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, CRL-ek, OCSP válaszok és időbélyeg válaszok igény esetén a TOE rendelkezésére álljanak.

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_DAU_CPV_INI.1, Tanúsítási útvonal inicializálás – alapkövetelmény: 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, mely megköveteli, 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 egy megbízható ponttól az előfizetőig. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FDP_CPD.1, Tanúsítási útvonal felépítése: megköveteli, hogy a TSF egy megbízható ponttól az előfizetőig felépíti 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_INI.1, Tanúsítási útvonal inicializálás - alapkövetelmény: megköveteli, 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, Tanúsítvány feldolgozás – alapkövetelmény: megköveteli, hogy TSF 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 utalni 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 utalni kell arra, 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 felhasználó nyilvános kulcsát kell használnia az aláírás ellenőrzéséhez. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FDP_DAU_SIG.1, Aláírási blob 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 a TSF-nek végre kell hajtania az ST szerzője által megadott egyéb ellenőrzéseket is.

8.2.1.5 Biztonsági célok a „PKI alapú felhasználó hitelesítés" csomagra - indoklás

O.I&A_Remote A TSF-nek egyértelműen azonosítania kell az összes távoli egyedet, és hitelesítenie kell azok állítólagos azonosságát, mielőtt egy távoli egyednek hozzáférést engedélyezne a TOE szolgáltatásokhoz és erőforrásokhoz:

- FIA_UAU.1;1, Hitelesítés időzítése – távoli egyed: a TSF-nek lehetővé kell tennie az ST írója által megadott TSF által közvetített tevékenységekre, hogy a felhasználó hitelesítése előtt melyek hajtódhatnak végre a felhasználó nevében, továbbá, a TSF-nek meg kell követelnie, hogy minden felhasználó sikeresen hitelesítve lett, mielőtt bármilyen más TSFel kapcsolatos tevékenységbe kezdhetne. Ez a követelmény biztosítja, hogy minden felhasználó hitelesítve lesz. A felhasználó jelen esetben a távoli entitás.
- FIA_UID.1;1, Azonosítás időzítése – távoli egyed: a TSF-nek lehetővé kell tennie az ST írója által megadott TSF által közvetített tevékenységekre, hogy a felhasználó azonosítása előtt melyek hajtódhatnak végre a felhasználó nevében, továbbá, a TSF-nek meg kell követelnie, hogy minden felhasználó sikeresen azonosítva lett, mielőtt bármilyen más TSFel kapcsolatos tevékenységbe kezdhetne. Ez a követelmény biztosítja, hogy minden felhasználó azonosítva lesz. A felhasználó jelen esetben a távoli entitás.

O.Limit_Actions_Auth_Remote A TSF-nek korlátoznia kell azokat a tevékenységeket, melyeket egy távoli egyed végrehajthat az előtt, mielőtt a TSF ellenőrizné a távoli egyed azonosságát:

- FIA_UAU.1;1, Hitelesítés időzítése – távoli egyed: a TSF-nek lehetővé kell tennie az ST írója által megadott TSF által közvetített tevékenységekre, hogy a felhasználó hitelesítése előtt melyek hajtódhatnak végre a felhasználó nevében, továbbá, a TSF-nek meg kell követelnie, hogy minden felhasználó sikeresen hitelesítve lett, mielőtt bármilyen más TSFel kapcsolatos tevékenységbe kezdhetne. Ez a követelmény biztosítja, hogy minden felhasználó hitelesítve lesz. A felhasználó jelen esetben a távoli entitás.
- FIA_UID.1;1, Azonosítás időzítése – távoli egyed: a TSF-nek lehetővé kell tennie az ST írója által megadott TSF által közvetített tevékenységekre, hogy a felhasználó azonosítása előtt melyek hajtódhatnak végre a felhasználó nevében, továbbá, a TSF-nek meg kell követelnie, hogy minden felhasználó sikeresen azonosítva lett, mielőtt bármilyen más TSFel kapcsolatos tevékenységbe kezdhetne. Ez a követelmény biztosítja, hogy minden felhasználó azonosítva lesz. A felhasználó jelen esetben a távoli entitás.

O.Linkage A TSF-nek a megfelelő felhasználói nyilvános kulcsot kell használnia a hitelesítéshez. A célt teljesíti:

- FIA_UAU_SIG.1, Felhasználó hitelesítés, amely megköveteli, hogy a TSF a tanúsítási útvonal érvényesség ellenőrzéséből a következő információkat használja az aláírt adatok aláírásának ellenőrzésére: alany nyilvános kulcs algoritmusa, alany nyilvános kulcsa, alany nyilvános kulcs paraméterek, és a TSF az ST írója által definiált egyéb ellenőrzéseket végrehajtja.

O.Single_Use_I&A A TSF-nek olyan azonosítási és hitelesítési (I&A) mechanizmusokat kell alkalmaznia, amelyek egyedi hitelesítési információkat követelnek meg minden egyes I&A esetén. A célt teljesíti:

- FIA_UAU.4, Egyszer használatos hitelesítési mechanizmusok: a TSF-nek meg kell akadályoznia a hitelesítési adatok ismételt felhasználását.

8.2.1.6 Biztonsági célok a „Valós idejű tanúsítvány állapot protokoll” csomagra - indoklás

O.Accurate_OCSP_Info A TSF-nek csak a pontos OCSP válaszokat szabad elfogadnia. A célt teljesíti:

- FDP_DAU_OCS.1, Alap OCSP kliens, amely megköveteli, hogy az OCSP válaszadótól csak a pontos visszavonási információkat fogadja el a TSF.

O.Auth_OCSP_Info A TSF-nek el kell fogadnia a jogosult forrásból származó OCSP információkat. A célt teljesíti:

- FDP_DAU_OCS.1, Alap OCSP kliens, amely megköveteli, hogy az OCSP válaszadóval szemben ellenőrzés történjen, hogy jogosult forrásnak számít-e.

O.Fresh_OCSP_Info A TSF-nek csak valószerűen aktuális OCSP információkat szabad elfogadnia. A célt teljesíti:

- FDP_DAU_OCS.1, Alap OCSP kliens, amely megköveteli, hogy csak a valószerűen aktuális visszavonási információkat fogadja el a TSF, szabályzatok összessége és paraméter ellenőrzések végrehajtása után.

8.2.1.7 Biztonsági célok a „CRL érvényesség ellenőrzés" csomagra - 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 valószerű aktuális (friss) CRL szabad csak elfogadnia. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

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

8.2.1.8 Biztonsági célok a „Naplózás menedzsment" csomagra - indoklás

O.Audit: a TSF-nek naplóznia kell a biztonsági szempontból fontos eseményeket. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FAU_GEN.1, Naplóadatok generálása: a TSF-nek képesnek kell lennie naplóadatok generálására a megadott naplózandó események körére, és a napló bizonyos specifikált adatokat kell, hogy tartalmazzon.

O.Audit_User: a TSF-nek képesnek kell lennie a naplózott eseményeket egyedi felhasználókhoz kötni. A biztonsági célt az alábbi követelmény(ek) teljesíti(k):

- FAU_GEN.2, Felhasználó azonosságának hozzárendelése: a TSF-nek képesnek kell lennie, hogy a naplózott eseményt kiváltó egyed azonosságát az eseményhez rendelje.

8.2.1.9 Biztonsági célok a „Folyamatos hitelesítés" csomagra - indoklás

O.Continuous_I&A: A TSF-nek folyamatosan hitelesítenie kell a felhasználót. A célt teljesíti:

- FIA_UAU.6:1, Távoli felhasználó újrahitelesítése: a TSF-nek ismételten hitelesítenie kell a távoli egyedet az ST írója által megadott feltételek szerint.
- FIA_UAU.6:2, Felhasználó újrahitelesítése: a TSF-nek ismételten hitelesítenie kell a távoli egyedeken kívüli felhasználókat, az ST írója által megadott feltételek szerint.

8.2.1.10 Biztonsági célok az „Időbélyeg kérése és ellenőrzése” csomagra - indoklás

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

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

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

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

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

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

8.2.2 A garanciális követelmények indoklása

EAL3-as garanciaszint olyan TOE-kre alkalmas, amelyek közepes szintű független garanciát igényelnek és megkövetelik a TOE és fejlesztésének alapos vizsgálatát, alapvető átdolgozás nélkül. Az EAL3 a biztonsági funkciók elemzése által nyújt garanciát, melyhez felhasználják a funkcionális és interfész specifikációt, az útmutató leírásokat és a TOE magas szintű tervét a biztonsági funkciók megértéséhez. Az elemzést kiegészíti a TOE biztonsági funkcióinak független tesztje, a funkcionális specifikáción és a magas szintű terven alapuló fejlesztői tesztelési bizonyítékok, a fejlesztői tesztek szelektív független megerősítése, a funkcióerősség elemzése, továbbá a nyilvánvaló sebezhetőségek keresésére irányuló bizonyíték.

8.3 A függőségek teljesítésének indoklása

8.20 táblázat – Funkcionális követelmények közötti függések

Sorszám	**Követelmény**	**Függések**
IT környezet funkcionális követelményei		
1	FAU_SAR.1	FAU_GEN.1
2	FAU_SEL.1	FAU_GEN.1, FMT_MTD.1 (ld. 3. megjegyzést)
3	FAU_STG.1	FAU_GEN.1
4	FDP_ACC.1	FDP_ACF.1
5	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
6	FDP_RIP.1	Nincs
7	FIA_AFL.1	FIA_UAU.1
8	FIA_ATD.1	Nincs
9	FIA_UAU.1	FIA_UID.1
10	FIA_UAU.7	FIA_UAU.1
11	FIA_UID.1	Nincs
12	FMT_MSA.1	FDP_ACC.1, FMT_SMF.1, FMT_SMR.1
13	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
14	FMT_MTD.1	FMT_SMF.1, FMT_SMR.1
15	FMT_SMF.1	Nincs
16	FMT_SMR.2	FIA_UID.1
17	FPT_RVM.1	Nincs
18	FPT_SEP.1	Nincs
19	FCS_CRM_FPS.1	Nincs
20	FDP_ITC_PKI_INF.1	Nincs
21	FPT_STM.1	Nincs

CPV – Alap csomag		
1	FDP_CPD.1	Nincs
2	FDP_DAU_CPV_INI.1	FCS_COP.1 (ld. 4. megjegyzést), FPT_STM.1 (ld. 1. megjegyzést)
3	FDP_DAU_CPV_CER.1	FCS_COP.1 (ld. 4. megjegyzést), FPT_STM.1 (ld. 1. megjegyzést)
4	FDP_DAU_CPV_CER.2	FDP_DAU_CPV_CER.1
5	FDP_DAU_CPV_OUT.1	Nincs
PKI aláírás létrehozás		
1	FDP_ETC_SIG.1	FCS_COP.1 (ld. 4. megjegyzést)
PKI aláírás ellenőrzés		
1	FDP_ITC_SIG.1	Nincs
2	FDP_DAU_SIG.1	FCS_COP.1 (ld. 4. megjegyzést), FDP_DAU_CPV_OUT.1 (ld. 5. megjegyzést)
PKI alapú felhasználó hitelesítés csomag		
1	FIA_UAU.1 (iteráció)	FIA_UID.1
2	FIA_UAU.4	Nincs
3	FIA_UAU_SIG.1	FCS_COP.1 (ld. 4. megjegyzést), FDP_DAU_CPV_OUT.1 (ld. 5. megjegyzést)
4	FIA_UID. (iteráció)	Nincs
OCSP kliens		
1	FDP_DAU_OCS.1	FCS_COP.1 (ld. 4. megjegyzést), FPT_STM.1 (ld. 1. megjegyzést)
CRL ellenőrzés		
1	FDP_DAU_CRL.1	FCS_COP.1, FPT_STM.1
Naplózás menedzsment		
1	FAU_GEN.1	FPT_STM.1 (ld. 1. megjegyzést)
2	FAU_GEN.2	FAU_GEN.1, FIA_UID.1 (ld. 2. megjegyzést)
Folyamatos hitelesítés csomag		
1	FIA_UAU.6	Nincs
Időbélyeg kérés és ellenőrzés csomag		
1	FDP_DAU_TS.1	FCS_COP.1 (ld. 4 megjegyzés)

1. megjegyzés: Az FPT_STM.1 függést teljesíti az IT környezetre vonatkozó FPT_STM.1 követelmény.
2. megjegyzés: Az FIA_UID.1 függést teljesítik az alap TOE követelmények.
3. megjegyzés: Az FMT_MTD.1 függést teljesítik az alap TOE követelmények.
4. 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.
5. megjegyzés: A függést teljesíti CPV – Alap csomag szerepeltetése.

8.4 A TOE összefoglaló előírás indoklása

8.4.1 A TOE funkcionális biztonsági követelményeinek leképezése a biztonsági funkciókra

Az alábbi táblázat felsorolja a XadesMagic v1.0 összes biztonsági követelményét, és megmutatja, hogy minden követelményt teljesít egy vagy több biztonsági funkció, illetve egy biztonsági funkció visszavezethető egy vagy több biztonsági követelményre.

	BF1 Lenyomat és digitális aláírás kezelése	**BF2 Tanúsítvány kezelése**	**BF3 Időbélyeg kezelése**	**BF4 OCSP kezelése**	**BF5 CRL kezelése**	**BF6 A TSF védelme és kezelése**
FAU_GEN.1						X
FAU_GEN.2						X
FDP_CPD.1		X				
FDP_DAU_CPV_CER.1		X				
FDP_DAU_CPV_CER.2		X				
FDP_DAU_CPV_INI.1		X				
FDP_DAU_CPV_OUT.1		X				
FDP_ETC_SIG.1	X					
FDP_ITC_SIG.1	X					
FDP_DAU_SIG.1	X					
FDP_DAU_OCS.1				X		
FDP_DAU_CRL.1					X	
FDP_DAU_TS.1			X			
FIA_UAU.1						X
FIA_UAU.4						X
FIA_UAU.6						X
FIA_UAU_SIG.1	X					
FIA_UID.1						X

9. Fogalmak, rövidítések

9.1 Fogalmak

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9.2 Rövidítések

BALE		**Biztonságos aláírás-létrehozó eszköz**
CA	**Certification Authority**	**Hitelesítés-szolgáltató**
CC	**Common Criteria**	**Közös szempontok**
EAL	**Evaluation Assurance Level**	**Értékelési garanciaszint** /A CC 3. rész olyan garanciális összetevőiből álló csomag, amely a CC előre meghatározott garanciális skáláján egy szintet képvisel./
KHE		**Kriptográfiai hardver eszköz**
PP	**Protection Profile**	**Védelmi profil** /Megvalósítástól független, olyan biztonsági követelményrendszer az értékelés tárgyainak (TOE-k) egy kategóriájára, amely adott fogyasztói igényeket elégít ki./
SF	**Security Function**	**Biztonsági funkció** /Az értékelés tárgyának (TOE) olyan része vagy részei, amelyekben meg kell bízni ahhoz, hogy a vonatkozó biztonsági szabályzatból (TSP) egy szorosan összefüggő szabályhalmaznak érvényt lehessen szerezni./
SFP	**Security Function Policy**	**Biztonsági funkció szabályzata** /A biztonsági funkció (SF) által érvényre juttatott biztonsági szabályzat./
ST	**Security Target**	**Biztonsági előirányzat** /Biztonsági követelmények és előírások olyan összessége, amelyet egy adott értékelés tárgyának (TOE) értékelésének alapjaként használnak./
SOF	**Strength of Function**	**Funkcióerősség** /Az értékelés tárgya (TOE) valamelyik biztonsági funkciójának minősítése, amely azt fejezi ki, hogy minimálisan mekkora erőkifejtést tartanak szükségesnek az elvárt biztonsági működés legyőzéséhez a mögöttes biztonsági mechanizmusok közvetlen megtámadása esetén./
TOE	**Target of Evaluation**	**Az értékelés tárgya** /Az az informatikai termék vagy rendszer, valamint a hozzákapcsolódó (rendszer) adminisztrátori és felhasználói útmutatók, amelyre az értékelés irányul./
TSF	**TOE Security Functions**	**TOE biztonsági funkciói** /Az értékelés tárgyát (TOE) képező minden olyan hardver, szoftver és förmver összessége, amelyben meg kell bízni ahhoz, hogy a vonatkozó biztonságpolitikát (TSP-t) megfelelő módon érvényre lehessen juttatni./
TSP	**TOE Security Policy**	**TOE biztonsági szabályzata** /Szabályok olyan összessége, amely szabályozza a vagyontárgyak kezelését, védelmét, elosztását az értékelés tárgyán (TOE-n) belül./
TSF data	**TSF data**	**TSF adat** /Az értékelés tárgya (TOE) által és részére létrehozott adat, amely befolyásolhatja annak (TOE) működését./
TSC	**TSF Scope of Control**	**TSF ellenőrzési kör** /Azon kölcsönhatások összessége, amelyek az értékelés tárgyán (TOE-n) belül vagy azzal kapcsolatban felléphetnek, és amelyeknek a vonatkozó biztonsági szabályzat (TSP) szabályait be kell tartaniuk./