A2-Polysys CryptoSigno Interop JAVA API minősített elektronikus aláíráshoz

Biztonsági előirányzat
Security Target
ST

Készült: PKE PP alapján
Public Key-Enabled Application
Family of Protection Profiles
USMC PKE PP with
<
Certification Path Validation (CPV) – Basic,
PKI Signature Generation,
PKI Signature Verification,
PKI Encryption using Key Transfer Algorithms,
PKI Decryption using Key Transfer Algorithms,
Certificate Revocation List (CRL) Validation
Online Certificate Status Protocol Client
>
at EAL <3> with augmentation
PP version: 2.5
PP date: October 31, 2002
PP prepared for: US Marine Corps

Kiegészítve: Időbélyeg kliens csomaggal

Verzió:	2.4
Dátum:	2009.03.10.
Készítette	Juhász Ágnes Polyák Ferenc

polysys®

A polysys® védjegyet az Országos Találmányi hivatal 129230/1989 szám alatt lajstromozva.
A polysys® védjegy hivatalos képviselője a Polysys Vállalkozó és Befektető Kft.

Java™

A Java™, valamint minden olyan védjegy, amely a Java szót tartalmazza a Sun Microsystems, Inc. védjegye vagy bejegyzett védjegye az Egyesült Államokban és egyéb országokban.

Ez a dokumentum a „JAVA” szóval szintén a Java védjegyre utal.

Változás kezelés

Verzió	Dátum	Leírás	Készítette
A1			
0.1	2004-05-11	Szerkesztés alatt	Juhász Ágnes, Polyák Ferenc
0.5	2004-07-15	Szerkesztés alatt	Juhász Ágnes, Polyák Ferenc
0.6	2004-07-24	Draft változat	Juhász Ágnes, Polyák Ferenc
0.7	2004-08-07	A TOE értékelés előzetes ST áttekintésének eredményeit figyelembe vevő változat	Juhász Ágnes, Polyák Ferenc
0.8	2004-10-11	Angolnyelvű összevetést segítő szövegek eltávolítása. 2.5 fejezet: pontosítás 6.2: fejezet: pontosítás 8.2.3: fejezet:magyarázat bővítés Előkészítés minősítésre.	Juhász Ágnes, Polyák Ferenc
0.9	2004-10-23	azonosító kulcs: javítva hitelesítő kulcsra 6.2.8: táblázatban dokumentum megnevezés és fejezet szám hivatkozás szövege javítva EAL 3+ kiterjesztve: javítva EAL3+ kibővítve Rövidítések,fogalmak, hivatkozott dokumentumok: AX-be átkerült	Juhász Ágnes, Polyák Ferenc
1.0	2004-11-22	minősítésre benyújtott, lezárt verzió	Juhász Ágnes, Polyák Ferenc
A2			
1.1	2005-05-13	Szerkesztés alatt	Juhász Ágnes, Polyák Ferenc
1.2	2005-09-13	ST áttekintés eredményeit figyelembe vevő változat	Juhász Ágnes, Polyák Ferenc
1.9	2005-11-20	minősítésre benyújtott, lezárt verzió	Juhász Ágnes, Polyák Ferenc
2.0	2005-12-30	„Egységes MELASZ formátum elektronikus aláírásokra” v1.0 hivatkozások kicserélésre kerültek **„**Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára (2005. november 22.)**”** hivatkozásra, mivel a két dokumentum azonos, csak ez utóbbi lett a miniszteri rendeletet követően a dokumentum hivatalos neve. tanúsításra benyújtott, lezárt verzió	Juhász Ágnes, Polyák Ferenc
2.1	2006-10-06	garancia folyamatosság biztosítással kísért aktuális változat	Juhász Ágnes, Polyák Ferenc
2.2	2007-01-27	garancia folyamatosság biztosítással kísért aktuális változat	Juhász Ágnes, Polyák Ferenc
2.3	2008-03-20	garancia folyamatosság biztosítással kísért aktuális változat	Juhász Ágnes, Polyák Ferenc
2.4	2009-03-10	garancia folyamatosság biztosítással kísért aktuális változat	Juhász Ágnes, Polyák Ferenc

Tartalomjegyzék

1 Bevezetés (ASE_INT)

Ez a fejezet azonosítja a biztonsági előirányzatot (ST), az értékelés tárgyát (TOE), ST konvenciókat, ST megfelelőséget, és az ST szervezését.

1.1 Azonosítás

ST cím: A2-Polysys CryptoSigno JAVA API minősített elektronikus aláíráshoz biztonsági előirányzata

ST készült:USMC PKE PP with <
Certification Path Validation (CPV) – Basic,
PKI Signature Generation,
PKI Signature Verification,
PKI Encryption using Key Transfer Algorithms,
PKI Decryption using Key Transfer Algorithms,
Certificate Revocation List (CRL) Validation >
at EAL <3> with augmentation
védelmi profil (PP) alapján

ST kiegészítés: Jelen ST-ben az eredeti PKE PP család választott csomagjain túl kiegészítésre került egy „Időbélyeg kliens” csomaggal, amely nem része az eredeti PKE PP családnak.

ST garancia szint: Evaluation Assurance Level (EAL) 3 with Augmentation

ST verzió: 2.4
ST dátum: 2009.03.10
ST szerzők: Juhász Ágnes, Polysys
Polyák Ferenc, Polysys

TOE azonosítás: A2-Polysys CryptoSigno Interop JAVA API minősített elektronikus aláíráshoz

CC azonosítás: Common Criteria for Information Technology Security Evaluation
CC verzió: 2.1, CCIMB-2004-01-002
CC dátum: 2004.január

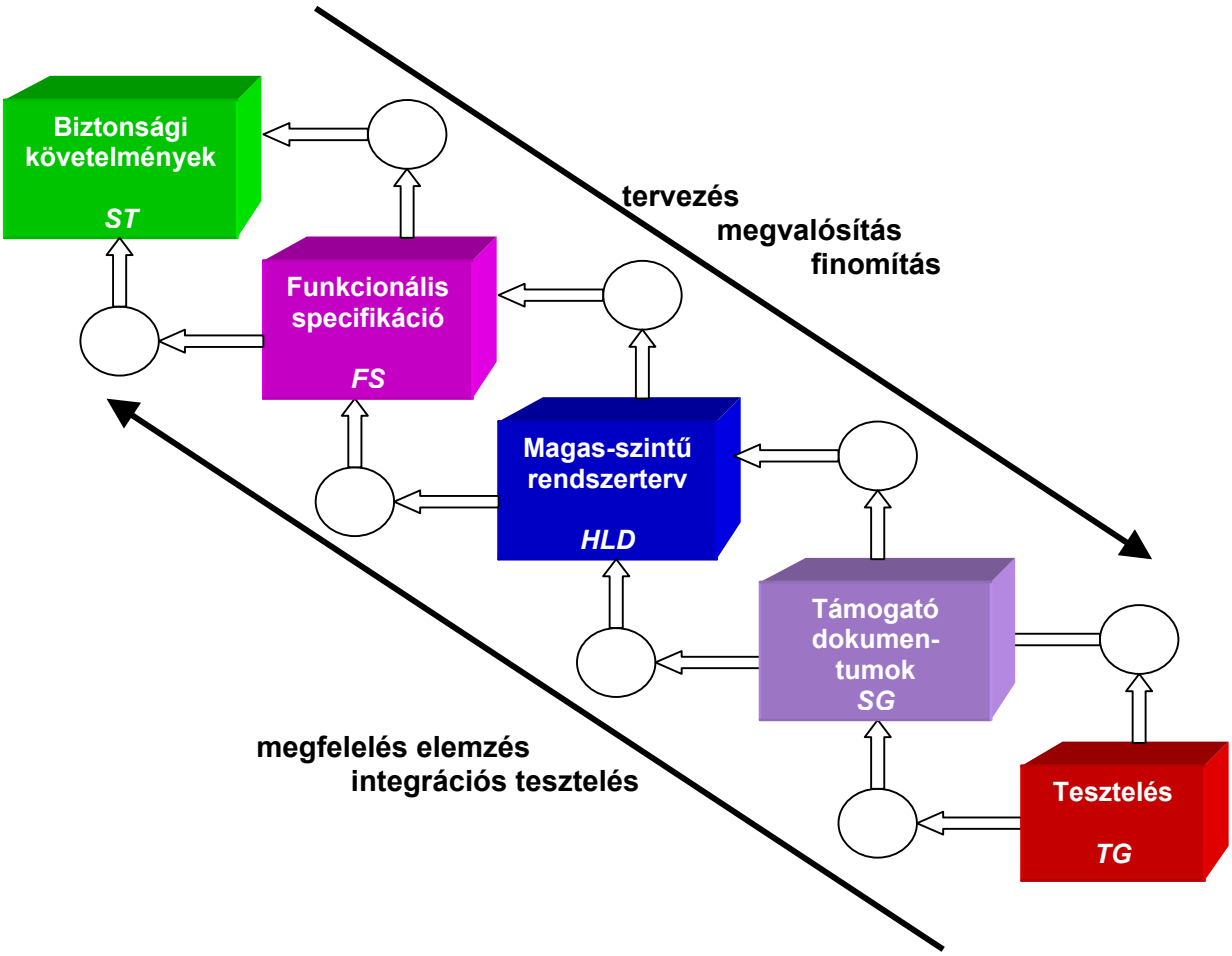
PP azonosítás: PKE PP (Public Key-Enabled Application Family of Protection Profiles)
with <
Certification Path Validation (CPV) – Basic,
PKI Signature Generation,
PKI Signature Verification,
PKI Encryption using Key Transfer Algorithms,
PKI Decryption using Key Transfer Algorithms,
Certificate Revocation List (CRL) Validation,
Online Certificate Status Protocol Client >
at EAL <3> with augmentation

PP verzió: 2.5
PP dátum: 2002.10.31

Kulcsszavak: Public Key Enabled (PKE), PKE, Public Key Infrastructure (PKI), PKI, minősített elektronikus aláírás, platform független, fejlesztő készlet, JAVA, API

Az alábbi ábra szemlélteti jelen dokumentum helyét a TOE fejlesztési modelljében.

1. ábra: A TOE fejlesztési modellje



A dokumentumokra történő hivatkozásokat egységes szín és rövidítés jelzi:

ST	Biztonsági előirányzat (Security Target)
FS	Funkcionális specifikáció (Functional Specification)
HLD	Magas-szintű terv (HighLevel Design)
SG	Támogató dokumentációk (Support Guides): JavaDoc / User Guide / Administrator Guide
TG	Teszt dokumentum (Test Guide)

1.2 Áttekintés

Ez a biztonsági előirányzat (ST) egy tanúsított védelmi profil családon (PKE PP) alapszik,amely csomag koncepción alapul, továbbá az ST kiegészítésre kerül egy csomaggal, amely az időbélyegek kliens oldali kezelését valósítja meg, mivel az eredeti PP csomagok közül ez a lehetőség hiányzik.

A PKE PP védelmi profil családot az USA Védelmi Minisztériuma (DoD) részére dolgozták ki. A védelmi profil család a csomagok koncepciójának bevezetésével alkalmas több ezer védelmi profil előállítására. Ezen nagyszámú variációk közül kiválasztásra került a csomagoknak egy olyan összeállítása, amely megfelel a jelen értékelés tárgyának (TOE). A kiválasztott PP összeállítás teljesen azonos a PKE PP, a kiválasztott csomagoknak a megfelelő szűkítésével, egy apró, de fontos finomítással. Az eltérés az amerikai és az európai, illetve hozzá kapcsolódva a magyar jogi szabályozásból adódó különbségből fakad. A magyar jogi szabályozás kétfajta elektronikus aláírást különböztet meg, a minősített és a fokozott biztonságú eletronikus aláírást. A magyar szabályozás a minősített elektronikus aláírás készítéséhez kötelező módon előírja a tanúsított biztonságos aláírási eszköz (BALE) használatát. A tanúsított BALE és a PP által feltételezett/előírt tanúsított FIPS140-1 level1 kriptográfiai modul egymásnak nem feleltethető meg. Az ST csak azokon a minimálisnak tekinthető pontokban tér el a PP-től, ahol azt a jogi szabályozás indokolja.

Az időbélyeg szolgáltatások kliens oldali igénybe vételének funkcionális követelményeit a szerzők úgy adják meg, hogy az, az RFC 3161-nek megfeleljen. Az időbélyeg kliens oldali kezelése nem tárgyalja az időbélyeg megszerzésének módját, mert annak biztonsága nem függ attól, hogyan kerül az alkalmazás birtokába, a biztonságot az időbélyeg ellenőrzése biztosítja. Ennek megfelelően az alábbi fő funkciókat biztosítja:

- Időbélyeg kérés előállítása pontosan meghatározott formában
- Időbélyeg válasz pontosan elvárt formájának ellenőrzése
- Időbélyeget szolgáltató szervezet hitelesítése
- működés fenntartásának biztosítása, bármely okból bekövetkező hiba esetén.

A csomagok funkcionális követelmények halmazaként is felfogható. A csomagokon belüli funkcionalitás nem „opcionális”. A csomagok más-más PKI funkcionalítást adnak meg, melyet egy alkalmazás, a TOE igényelhet vagy sem. Ha egy adott alkalmazás tartalmazza egy csomagban leírt funkcionalítást, akkor a TOE-nak maradéktalanul teljesítenie kell a csomag követelményeket.

A csomag nem foglalkozik az időbélyeg szerver funkciókkal, mivel az alapvetően infrastruktúra funkció.

Az alábbi összefoglaló táblázatban felsorolásra kerülnek a PKE PP védelmi profil családból kiválasztásra került csomagok, kiegészítve az időbélyeg kliens csomaggal.

1. táblázat: Felhasznált csomagok

Csomagnév	Funkcionalitás	Függőség
PKE PP csomag		
Tanúsítási útvonal érvényesítése (CPV) - Alap	Minden X.509 érvényesítési ellenőrzés elvégzése, a policy és name constraints feldolgozások kivételével	Tanúsítvány visszavonási lista (CRL) érvényesítés
PKI aláírás készítés	Magán kulcsot használ az aláírás elkészítéséhez	Nincs
PKI aláírás ellenőrzés	Aláírási információk feldolgozása Nyilvános kulcsot használ az aláírás ellenőrzésére	Tanúsítási útvonal érvényesítése (CPV) - Alap
PKI titkosítás kulcs átviteli algoritmusokkal	Elkészíti egy titkosítást kísérő információkat Nyilvános kulcsot használ a titkosításhoz	Tanúsítási útvonal érvényesítése (CPV) - Alap
PKI visszafejtés kulcs átviteli algoritmusokkal	Feldolgozza a titkosítást kísérő információkat Magán kulcsot használ a visszafejtéshez	nincs
Valós idejű tanúsítvány állapot protokoll (OCSP) kliens	OCSP kérést állít elő és OCSP választ ellenőriz az RFC 2560-nak megfelelően	Tanúsítási útvonal érvényesítése (CPV) - Alap
Tanúsítvány visszavonási lista (CRL) érvényesítés	Megszerzi a CRL-t Feldolgozza a CRL-t	nincs
ST csomag		
Időbélyeg kliens	Időbélyeget kér és ellenőriz az RFC 3161-nek megfelelően	Tanúsítási útvonal érvényesítése (CPV) - Alap

1.3 Megfelelőség a Common Criteria-hoz

Jelen dokumentumban használt CC (Common Criteria) rövídítés minden esetben azonosnak tekintendő a Magyar Szabványügyi Testület által magyar szabványként közzétett MSZ ISO/IEC 15408-2:2003 szabvánnyal, amely a CC 2.1 verziójával azonos. Minden olyan CC hivatkozás esetén, amely nem a 2.1 verzióra vonatkozik, ott a CC verzió számot külön jelölik a szerzők.

A TOE megfelel az alábbi CC specifikációknak:

- Az informatikai biztonságértékelés közös szempontjai, 2. kötet: A biztonság funkcionális követelményei, MSZ ISO/IEC 15408-2:2003
  - 2. kötet kiterjesztett
  - FMT biztonságirányítás osztály kiegészítve az FMT_SMF (Specification of management function) családdal, amely megtalálható a CC 2.2 verzióban (CCIMB-2004-01-002).
- Az informatikai biztonságértékelés közös szempontjai, 3. kötet: A biztonság garanciális követelményei, MSZ ISO/IEC 15408-3:2003
  - 3. kötet konform
  - értékelési garanciaszint EAL 3+ kibővítve az ALC_FLR.1 (A biztonsági rések alapszintű javítása) összetevővel.

A CC az időbélyeggel/időponttal kapcsolatos összetevői nem alkalmasak időbélyeg kliens követelményként, így a CC 2. részét ki kell terjeszteni. A kiterjesztett 2. rész definiciója, a CC 1. rész 5.2 szakasz alapján; egy PP vagy TOE kiterjesztett, ha a funkcionális követelmények, a 2. részben nem szereplő funkcionális összetevőket is tartalmaznak.

A TOE megfelel az alábbi PP-nek:

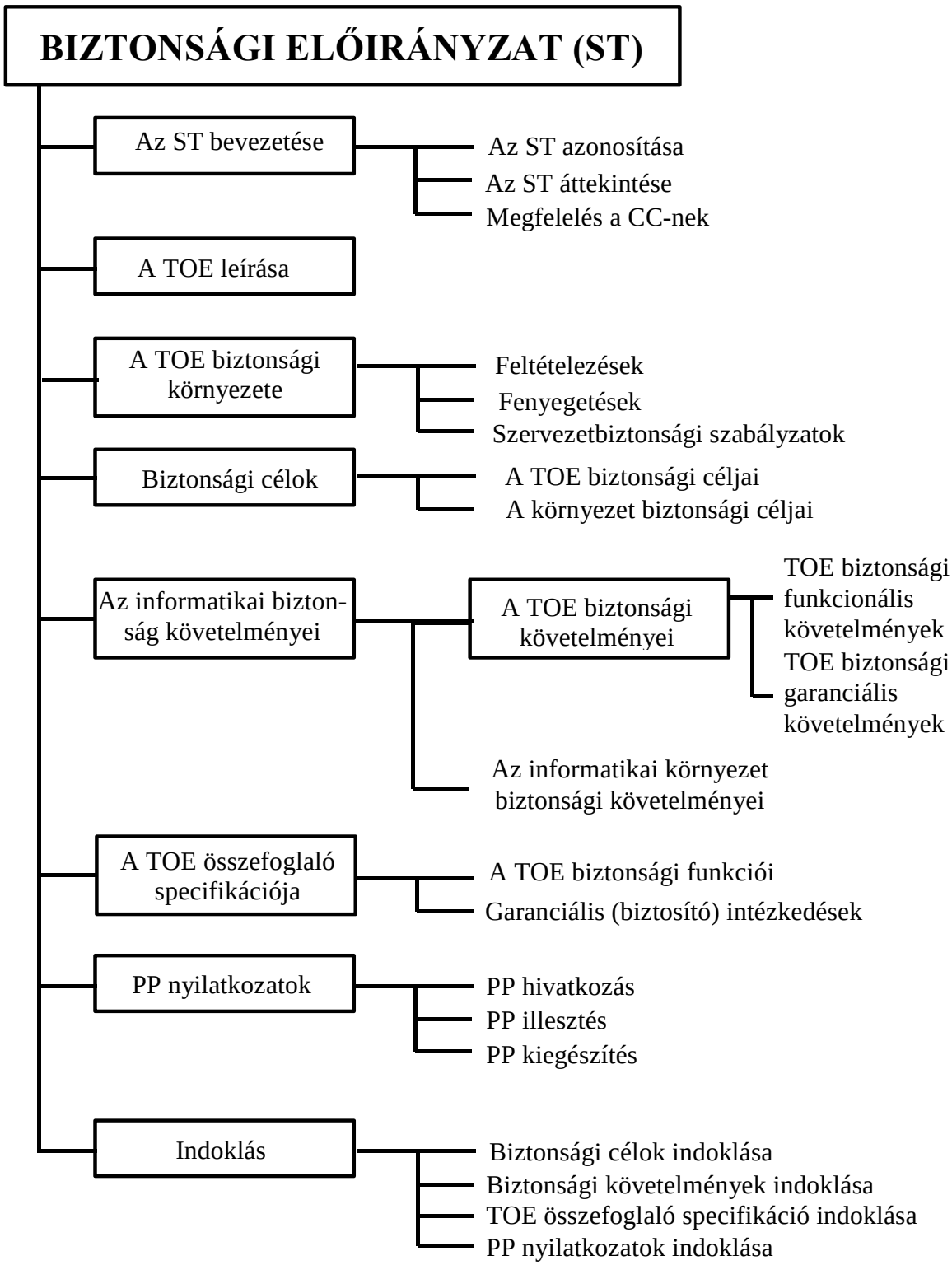
PKE PP (Public Key-Enabled Application Family of Protection Profiles), verzió: 2.5, dátum: 2002.10.31
with <
Certification Path Validation (CPV) – Basic,
PKI Signature Generation,
PKI Signature Verification,
PKI Encryption using Key Transfer Algorithms,
PKI Decryption using Key Transfer Algorithms,
Certificate Revocation List (CRL) Validation,
Online Certificate Status Protocol Client >
at EAL <3> with augmentation

kibővítve az Időbélyeg kliens csomaggal

1.4 A dokumentum szerkezete

Jelen dokumentum az MSZ ISO/IEC 15408 Az informatikai biztonságértékelés közös szempontjai szabvány 1. kötet C mellékletében meghatározott szerkezetet követi.

2. ábra: Az ST szerkezete



2 Az értékelés tárgyának (TOE) leírása (ASE_DES)

Ez a fejezet az értékelés tárgyát (TOE) képező A2-Polysys CryptoSigno Interop JAVA API minősített elektronikus aláíráshoz fejlesztő készlet leírása. Leírja a TOE típusát, üzemmódjait, szolgáltatásait, a TOE határait és működési környezetét.

A TOE a tanúsított „A1-Polysys CryptoSigno JAVA API minősített elektronikus aláíráshoz v1.1.0” aláíró alkalmazás fejlesztő készlet terméknek a továbbfejlesztett és kibővített változata. A TOE felülről kompatíbilis az A1-API-val, amely azt jelenti, hogy képes az annak megfelelő aláírások létrehozására és ellenőrzésére (deprecated). Ugyanakkor az aláírás létrehozására és ellenőrzésére a XAdES formátumok teljes palettáját felölelő és az interoperabilitást biztosító, aláírás létrehozó és ellenőrző funkciók állnak rendelkezésre.

2.1 A termék típusa

A TOE egy fejlesztő készlet (könyvtár), amely platform független Java technológiával készülő, a TOE-t használó alkalmazások (AHA) számára támogatást nyújt:

- minősített vagy fokozott biztonságú elektronikus aláírás létrehozására és ellenőrzésére
- titkosításra és visszafejtésre
- tanúsítványok és visszavonási információk ellenőrzésére, a tanúsítási útvonal felépítésére és érvényesítésére
- azonosításra (identification), hitelesítésre (authentication) és jogosultság ellenőrzésre (authorization)

Elektronikus aláírás
A TOE az XML-Signature Syntax and Processing (XMLDSIG) szabvány és az XML Advanced Electronic Signature (XAdES) v1.2.2, valamint a v1.3.2 szabvány BES, EPES, T, C, X, X-L, A formátumai szerint készít és ellenőriz elektronikus aláírásokat. Az A2-API az interoperabilitás biztosítására támogatja **„**Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára (2005. november 22.)**”** változatát, valamint az „Egységes MELASZ formátum elektronikus aláírásokra” v2.0 változatát. Az A2-API az aláírás létrehozása és ellenőrzése során a TSP, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (RFC 3161) szerint kér és ellenőriz időbélyegeket. Az A2-API az aláírás létrehozása és ellenőrzése során az OCSP, X.509 Internet Public Key Infrastucture Online Certificate Status Protocol (RFC 2560) szerint készít OCSP kérést és ellenőrzi az OCSP válaszokat.

Titkosítás és visszafejtés
Az A2-API hibrid típusú (PKI alapú, kulcsátviteli algoritmus és szimmetrikus titkosító algoritmus kombinációjára épülő) titkosítást és visszafejtést végez. A szimmetrikus titkosítás algoritmusa AES/256, amelynek titkos kulcsát aszimmetrikus RSA/1024 vagy RSA/2048 bites titkosítás védi.

Tanúsítványok és visszavonási információk ellenőrzése
A TOE a PKIX, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 5280) szerint végzi a tanúsítványok és tanúsítvány visszavonási listák ellenőrzését, a tanúsítási útvonal felépítését és érvényesítését.

Azonosítás, hitelesítés és jogosultság ellenőrzés
A TOE PKI alapú azonosítás, hitelesítés és jogosultság ellenőrzés szolgáltatást nyújt, a Java Authentication and Authorization Service (JAAS) architektúrának megfelelően.

2.2 A TOE üzemmódjai

A TOE-nak két használati módja különböztethető meg:

- szigorú üzemmód: - minősített elektronikus aláírás létrehozására alkalmas
- normál üzemmód: - fokozott biztonságú elektronikus aláírás létrehozására alkalmas

A TOE a szigorú üzemmódjában egy NHH által nyilvántartásba vett, tanúsított biztonságos aláírás-létrehozó eszközzel és minősített tanúsítvánnyal használva megfelel a magyar elektronikus aláírásról szóló XXXV. törvény (Eat.) minősített elektronikus aláírásra vonatkozó előírásainak.

A TOE a normál üzemmódjában megfelel a törvénynek, a fokozott biztonságú elektronikus aláírásra vonatkozó előírásainak.

2.3 A TOE szolgáltatásai

2.3.1 Önteszt

A TOE öntesztet hajt végre, amelynek fő feladata a TOE hitelességének ellenőrzése, annak sértetlenségének és változatlanságának fenntartása. Használatának fő célja, hogy megakadályozza a TOE szándékos megváltoztatását vagy nem szándékos megváltozását.
Az önteszt során a TOE futtatható kódjának a csatolt, elektronikus aláírását ellenőrzi, azaz

- a futó kódot valóban a feltételezett gyártó írta-e alá
- az aláírás hiteles-e

Sikeres önteszt esetén engedélyezésre kerül az AHA számára a TOE használata.

2.3.2 Felhasználó hitelesítés és azonosítás

Az AHA felhasználója, a TOE szolgáltatásait igénybe venni kívánó személy. A TOE biztosítja, hogy a szolgáltatásait csak az AHA azonosított, hitelesített és jogosult felhasználója, illetve annak nevében eljáró folyamat vehesse igénybe. A TOE biztonsági funkciója minden szolgáltatás igénybe vétele előtt és után működésbe lép. A biztonsági funkció a szolgáltatás kérésekor a folyamatot (annak felhasználóját) azonosítja, hitelesíti és jogosultságát ellenőrzi. Használatának fő célja, hogy a hozzáférést kérő személy, az AHA felhasználója bizonyítsa, hogy birtokol egy olyan kulcstárolót, amelyben a személyes tanúsítványa és az ahhoz tartozó azonosító magánkulcsa rendelkezésre áll, és azokat használni tudja.

A felhasználó hitelesítéséhez és jogosultság ellenőrzéséhez szükséges információk bekéréséhez elengedhetetlen információk bekérését a TOE biztosítja. Az első alkalommal mindenképpen a teljes hitelesítés és jogosultság ellenőrző eljárásra kerül sor, a továbbiakban opcionálisan gyorsított eljárás is választható. A gyorsított eljárás lényege, hogy az AHA felhasználó nevében eljáró folyamat azonosítása, hitelesítése és jogosultságának ellenőrzése olyan módon lesz megismételve, amely a felhasználói ismételt közreműködését nem igényeli.

2.3.3 PKI biztonsági, működési jellemzők menedzsmentje

A TOE lehetővé teszi a TOE által azonosított, hitelesített és jogosult felhasználó nevében eljáró AHA folyamat számára a PKI biztonsági jellemzők és a TOE működését befolyásoló biztonsági jellemzők menedzsmentjét.

A PKI biztonsági jellemzői a következők:
- tanúsítvány jellegű:
  - megbízható legfelső szintű hitelesítő tanúsítványok (trust anchor)
  - közbenső tanúsítványok (intermediate certificate)
  - saját tanúsítványok (personal end entity certificate)
  - más személyek tanúsítványai (other end entity certificate)
- CRL jellegű:
  - visszavonási információk

A TOE működését befolyásoló biztonsági jellemzők a következőek:
- a CRL a kibocsátást követő hány napig tekinthető aktuálisnak (CRLAfterThisUpdateLimit)
- a CRL a következő kibocsátási dátumot követő hány napig tekinthető aktuálisnak (CRLAfterNextUpdateLimit)
- a CRL frissesség ellenőrzés engedélyezése
- visszavonás ellenőrzés kihagyhatóságának engedélyezése
- megbízható időszerverek
- szolgáltatás igénybevétele utáni kényszerített kijelentkeztetés engedélyezése
- az OCSP válasz az előállítást követő hány percig tekinthető aktuálisnak (OCSPAfterProducedAtLimit)
- az OCSP válasz a kibocsátás követő hány percig tekinthető aktuálisnak (OCSPAfterThisUpdateLimit)
- az OCSP válasz a következő kibocsátást követő hány percig tekinthető aktuálisnak (OCSPAfterNextUpdateLimit)
- OCSP válasz frissesség ellenőrzés engedélyezése
- Időbélyeg szolgáltatás elérhetősége
- OCSP szolgáltatás elérhetősége
- szervezeti aláírási szabályzat

A PKI szolgáltatások a következők lehetnek:
- tanúsítvány ellenőrzés jellegű:
  - megbízható legfelső szintű tanúsítvány ellenőrzése
  - közbenső tanúsítvány ellenőrzése
  - végtanúsítvány (saját vagy más személy) ellenőrzése
  - kulcshasználat ellenőrzése
- tanúsítási útvonal felépítés és érvényesítés jellegű:
  - tanúsítási útvonal felépítése
  - tanúsítási útvonal érvényesítése
  - tanúsítási útvonal együttes felépítése és érvényesítése

Az AHA részére biztosítva van a TOE működését befolyásoló biztonsági jellemzők alapértelmezett értékeinek beállítási és lekérdezési lehetősége.

2.3.4 Elektronikus aláírás, ellenőrzés

A TOE biztosítja a TOE által azonosított, hitelesített és jogosult felhasználó nevében eljáró AHA folyamat számára:
- az AHA felhasználó aláíró magánkulcsával elektronikus aláírás és kiegészítő aláírási információk létrehozását
- elektronikus aláírás és az azt kiegészítő aláírási információk ellenőrzését az aláíró tanúsítványának felhasználásával

A TOE az elektronikus aláírás létrehozását és ellenőrzését az XMLDSIG szabványra épülő XAdES v1.2.2, valamint a v1.3.2 szabvány XAdES-BES, EPES, T, C, X, X-L, A formátumainak és „Az

Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára (2005. november 22.)**”** ajánlásnak, vagy az „Egységes MELASZ formátum elektronikus aláírásokra” v2.0 dokumentumnak megfelelően végzi.

A TOE az A1-API-val való kompatibilitás fenntartására biztosítja az annak megfelelő elektronikus aláírás létrehozására és ellenőrzésére irányuló szolgáltatásokat. Azonban az új fejlesztésű alkalmazásokban ezeknek a szolgáltatásoknak a használata nem javasolt (deprecated). Helyettük az új aláírás létrehozó és ellenőrző szolgáltatások használata javasolt.

Aláírás létrehozása, A1-kompatíbilis (deprecated)
Az elektronikus aláírás létrehozás bemenete:

- az aláírandó tartalmak egységes erőforrás azonosítói (Uniform Resource Identifier - URI) és/vagy a szöveges tartalom
- aláírás külső dokumentumként vagy Base64 kódolással beágyazva jelzés
- aláírás helye
- aláíró szerepköre
- aláírásba befoglalandó XML gyermek vagy szülő csomópont (opcionális)

A sikeres aláírás létrehozás előfeltételei:

- az AHA felhasználójának az aláírás létrehozásához használt tanúsítványa a tanúsítási útvonal felépítése és ellenőrzése által sikeresen érvényesíthető legyen
- az AHA felhasználójának az aláírás létrehozásához használt tanúsítványra, a kulcshasználat ellenőrzése az aláírás létrehozása művelet típusra nézve sikeresen megtörténjen

Az előfeltételek teljesülése esetén az aláírás létrehozásának főbb lépései:

- aláírási algoritmus (RSA-SHA1 vagy DSA-SHA1) kiválasztása az aláíró kulcs algoritmusának megfelelően
- aláírást kísérő információk összeállítása
- az aláírás elkészítése
- az elkészített aláírás automatikus ellenőrzése, a tanúsítási útvonal felépítése és ellenőrzése funkciójának kimenetéből származó nyilvános kulccsal
- a XAdES BES formátum kiírása

A sikeres aláírás létrehozás hatására létrejön az aláírást és az aláírást kísérő információkat tartalmazó XAdES BES formátumú fájl.

Elektronikus aláírás létrehozása fájlként
A TOE az elektronikus aláírás létrehozását a XAdES v1.2.2 vagy v1.3.2 BES, EPES, T vagy C formátumának, illetve **„**Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára (2005. november 22.)**”** ajánlásnak, vagy az „Egységes MELASZ formátum elektronikus aláírásokra” v2.0 dokumentumnak megfelelően végzi, a kimenetet fájlként adja vissza.

Elektronikus aláírás létrehozása fájlként bemenete:

- aláírás létrehozási környezet

A sikeres aláírás létrehozás előfeltételei:

- az AHA felhasználójának az aláírás létrehozásához használt tanúsítványa a tanúsítási útvonal felépítése és ellenőrzése által sikeresen érvényesíthető legyen
- az AHA felhasználójának az aláírás létrehozásához használt tanúsítványra, a kulcshasználat ellenőrzése az aláírás létrehozása művelet típusra nézve sikeresen megtörténjen

Az előfeltételek teljesülése esetén az aláírás létrehozásának főbb lépései:
- annak ellenőrzése, hogy az aláírás létrehozási környezetben megadott paraméterek összhangban vannak-e választott formátummal (szabványos vagy MMM)
- aláírást kísérő aláírt információk összeállítása
- aláírás elkészítése
- aláírást kísérő aláíratlan információk összeállítása, az aláírás létrehozási környezetben megadott paraméterektől függően
- XAdES v1.2.2 vagy v.1.3.2 BES, EPES, T, C szabványos vagy MMM v1.0 vagy v2.0 formátum kimenetként történő visszaadása, a fájl kiírásával

Elektronikus aláírás létrehozása XML dokumentumként
A TOE létrehozza az elektronikus aláírást, ez előzőekben leírtak szerint, azzal a különbséggel, hogy a kimenetet XML dokumentumként adja vissza.

Párhuzamos aláírás hozzáadása
A TOE egy kész (egyszeres vagy többszörös) aláíráshoz egy újabb aláírást ad hozzá. A párhuzamos aláírás kifejezés azt jelenti, hogy az újonnan hozzáadott aláírás nem ellenjegyző (CounterSignature), hanem a meglevőkkel egyenrangú aláírás, amely az aláírásba befoglalhat, nulla, egy vagy több az XML dokumentumban jelen levő tetszőleges elemet. A TOE-nak ez a funkciója egymás után többször is használható.

Ellenjegyző aláírás hozzáadása
A TOE egy kész (egyszeres vagy többszörös) aláíráshoz egy ellenjegyző aláírást (CounterSignature) ad hozzá. Az ellenjegyző aláírás egy referenciát fog tartalmazni, amely a beágyazó aláírás SignatureValue elemére mutat. A TOE-nak ez a funkciója egymás után többször is használható.

Aláírás ellenőrzés, A1 kompatíbilis (deprecated)
Az elektronikus aláírás ellenőrzés bemenete:
- aláírást tartalmazó XML formátum

A sikeres aláírás ellenőrzés előfeltételei:
- az aláíró tanúsítványára, a tanúsítvány a tanúsítási útvonal felépítése és ellenőrzése által sikeresen hitelesíthető legyen
- az aláíró tanúsítványára, a tanúsítvány a kulcshasználat ellenőrzése az aláírás ellenőrzés művelet típusra nézve sikeresen megtörténjen

Az előfeltételek teljesülése esetén az aláírás ellenőrzésének főbb lépései:
- az URI-val hivatkozott aláírt tartalmak beolvasása
- az aláírást kísérő információk formai és tartalmi megfelelőségének elemzése
- az aláírás ellenőrzése

Az aláírás ellenőrzés kimenete az, hogy az elektronikus aláírás érvényes vagy az elektronikus aláírás nem érvényes.

Egyszeres aláírás fájl ellenőrzése
A TOE ellenőrzi a fájlban található első aláírást, valamint kialakítja az ellenőrző szándéka szerinti T, C, X, X-L vagy A formátumot.
Az egyszeres aláírás fájl ellenőrzés bemenete:
- az aláírást tartalmazó fájl
- aláírás ellenőrzési környezet

Főbb lépések:
- aláírást kísérő információkból az aláírói tanúsítvány meghatározása
- előzetes ellenőrzés az aláírót tanúsítványból a nyilvános kulccsal
- XML aláírás tartalmi és formai elemzése, a megadott formátum típusnak megfelelően
- aláírást kísérő aláíratlan információk bővítése a paraméterezéstől függően
- az aláírói tanúsítványra a tanúsítási útvonal felépítése és érvényesítése az aláírás ellenőrzés művelet típussal
- aláírás ellenőrzése a tanúsítási útvonal felépítés kimenetéből származó nyilvános kulccsal
- időbélyegek ellenőrzése, ha az aláírás tartalmaz időbélyegeket
- OCSP válaszok ellenőrzése, ha az aláírás tartalmaz OCSP válaszokat

Egyszeres aláírás XML dokumentum ellenőrzése
A TOE ellenőrzi az elektronikus aláírást, az előzőekben leírtak szerint, azzal a különbséggel, hogy a bemenet XML dokumentum.

Többszörös aláírás megadott elemének ellenőrzése
A TOE ellenőrzi a többszörös aláírásban a megadott aláírást.

A többszörös aláírás ellenőrzés bemenete:
- aláírás ellenőrzési környezet
- a többszörös aláírást leíró objektum, amely létrehozható:
  - fájlból
  - XML dokumentum objektumból
  - stream olvasásával
  - egy többszörös aláírást leíró objektum másolataként
- az ellenőrizendő Signature elem

Többszörös aláírás ellenőrzése
A TOE a többszörös aláírásban fellelt összes aláírást ellenőrzi, ugyanazon aláírás ellenőrzési környezettel.

2.3.5 Titkosítás és visszafejtés

A TOE biztosítja a TOE által azonosított, hitelesített és jogosult felhasználó nevében eljáró AHA folyamat számára a titkosítás és visszafejtés szolgáltatásokat, azaz:
- a címzett(ek) nyilvános kulcsát tartalmazó tanúsítvány(ok) felhasználásával titkosítja a címzett(ek)nek továbbítandó információkat
- a titkosított információkat az AHA felhasználó visszafejtő magánkulcsának felhasználásával visszafejti
- a titkosított információkat az AHA felhasználó visszafejtő magánkulcsának felhasználásával visszafejti, majd egy megadott címzett részére újratitkosítja

Titkosítás
A titkosítás két szolgáltatást nyújt az AHA számára:
- stream titkosítást
- fájl titkosítás

A titkosítás bemenete:
- címzett(ek) tanúsítványai
- titkosítandó stream és annak hossza vagy a titkosítandó fájl

A sikeres titkosítás előfeltételei:
- minden egyes címzett tanúsítványra, a tanúsítványra a tanúsítási útvonal felépítése és ellenőrzése által sikeresen érvényesíthető legyen
- minden egyes címzett tanúsítványra, a tanúsítványra a kulcshasználat ellenőrzése a titkosítás művelet típusra nézve sikeresen megtörténjen

Az előfeltételek teljesülése esetén a titkosítás főbb lépései:
- az input stream vagy fájl tartalmára AES/256 szimmetrikus titkosítás elvégzése
- minden egyes címzett számára a leíró információ létrehozása

A sikeres titkosítás hatására létrejön a titkosított stream vagy fájl a következő formátumban:
- leíró információk 1…n címzett számára:
  - címzett tanúsítványa
  - titkosítás időpontja
  - fájl név vagy annak megfelelője
  - digest a titkosítatlan tartalomra
  - a címzett nyilvános kulcsával, RSA algoritmussal csomagolt AES titkos kulcs
- titkosított tartalom
  - AES algoritmussal titkosított tartalom

Visszafejtés
A visszafejtés két szolgáltatást nyújt az AHA számára:
- stream visszafejtés
- fájl visszafejtés

A visszafejtés bemenete:
- a titkosított stream és annak hossza vagy a titkosított fájl

A sikeres visszafejtés előfeltételei:
- a titkosítási formátum a TOE által titkosított formátum legyen
- az AHA felhasználó szerepeljen a titkosítás címzettjei között
- az AHA felhasználó tanúsítványára a tanúsítvány tanúsítási útvonal felépítése és ellenőrzése által, az ellenőrzés időpontjában sikeresen érvényesíthető legyen
- az AHA felhasználó tanúsítványára a tanúsítvány a kulcshasználat ellenőrzése a visszafejtés művelet típusra nézve sikeresen megtörténjen

Az előfeltételek teljesülése esetén megkezdődik a visszafejtés, amelynek lépései:
- a leíró információból az AHA felhasználó számára csomagolt AES kulcs kicsomagolása
- az AES/256 szimmetrikus visszafejtés elvégzése, egyidejűleg a visszafejtett tartalomra digest képzés
- a leíró információból a titkosítatlan tartalomra képzett digest kiolvasása, és annak egyezőségének vizsgálata a visszafejtett tartalomra képzett digesttel

A sikeres visszafejtés során létrejön a visszafejtett, az eredetivel azonos tartalmú stream vagy fájl.

Visszafejtés és újratitkosítás
A TOE biztosítja, a TOE által azonosított, hitelesített és jogosult felhasználó nevében eljáró AHA folyamat számára a visszafejtés és újratitkosítás szolgáltatást. A szolgáltatás célja az, hogy az AHA felhasználója a titkosított információt egy olyan címzett számára újratitkosítsa, aki eredetileg nem szerepelt a titkosítás címzettjei között.

A visszafejtés és újratitkosítás bemenete:
- a címzett tanúsítványa
- a titkosított stream és annak hossza

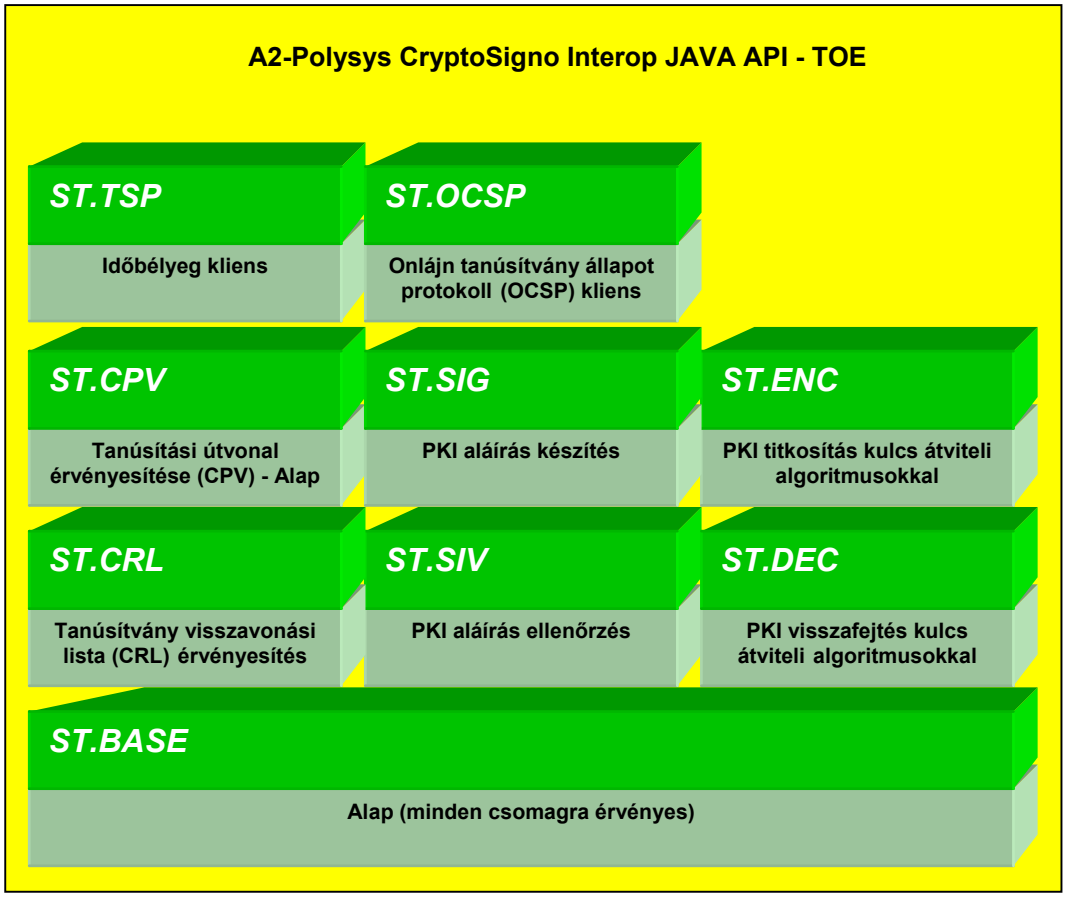
Az előfeltételek, lépések az általános titkosítással és visszafejtéssel egyezők.

A sikeres visszafejtés során létrejön az AHA felhasználójának magánkulcsával visszafejtett tartalomnak a most megadott új címzett részére történt titkosítása.

2.4 A TOE határai

A TOE szolgáltatások nagyobb egységekbe, csomagokba vannak szervezve. Ezek a csomagok alkotják a TOE-t. Az alábbi ábrákon a sárga színnel jelzett terület a TOE, a zöld szín jelzi az összetevő csomagokat.

3. ábra: A TOE felosztása csomagokra

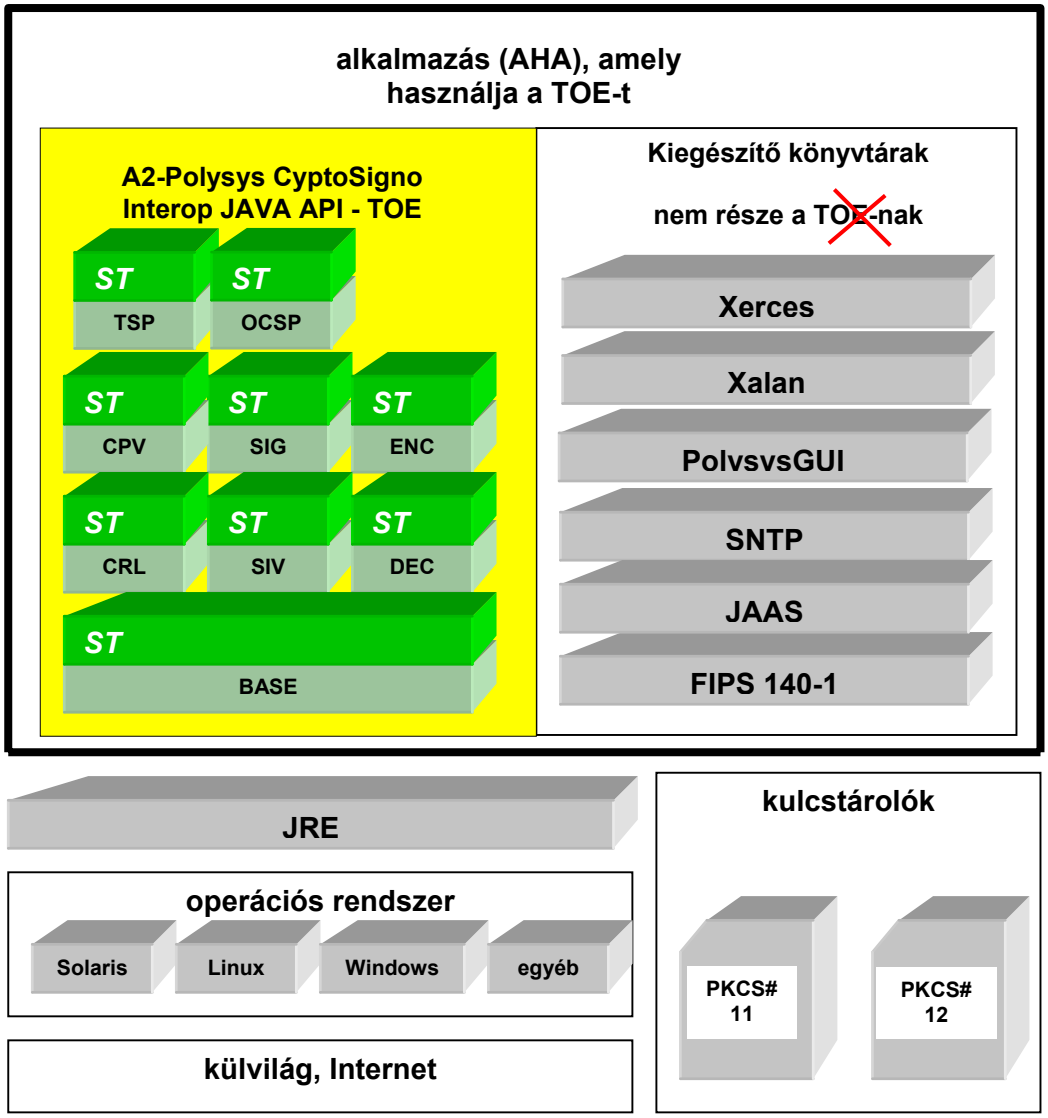


A TOE egy platform független, Java nyelven írt fejlesztő készlet. A TOE célja, hogy Java nyelven fejlesztendő alkalmazások (AHA) számára azt a PKI biztonsági magot biztosítsa, amely felhasználásával az AHA alkalmassá válik minősített és fokozott biztonságú elektronikus aláírás létrehozására, ellenőrzésére, valamint titkosításra és visszafejtésre, felhasználó azonosításra (identification), hitelesítésre (authentication) és jogosultság ellenőrzésre (authorization).

A TOE elektronikusan aláírt JAR fájl formájában létezik. A TOE a Java Language Specification 2.0, és Java Virtual Machine, Second Edition specifikációknak megfelelő Java környezetet feltételez.

A TOE-nak két határa van. Az első határa a Java virtuális gép és annak a futtató környezetet alkotó osztályai, a következő ábrán a JRE felirat jelzi. A második határ a TOE (az ábrán sárga szín jelzi) és az AHA között van. A második határ egy közvetett határ, mivel az AHA és a TOE ugyanazon a Java virtuális gépen belül fut. A TOE közvetlen környezetét a Java virtuális gép alkotja. A TOE és az AHA Java metódus hívásokkal kommunikál, melyeket a Java virtuális gép hajt végre.

4. ábra: A TOE határai



A TOE közvetlen környezetét a JAVA virtuális gép alkotja. A Java virtuális gép kapcsolódik az operációs rendszerhez, amely biztosítja az egyéb infrastruktúrális elemek és funkciók (Internet, kulcstárolók) közvetett (az ábrán fehér körben határolt területek) elérhetőségét a TOE számára.

A TOE bármely operációs rendszeren használható, amely az 5.2 fejezetben leírt biztonsági követelményeknek eleget tesz és amelyen megfelelő verziószámú Java futtató környezet (JRE 1.5.0 vagy magasabb verzió szám) telepítve van. A TOE a Java futtató környezetben telepített Java könyvtárakat használja. A TOE feltételezi, hogy legalább FIPS 140-1 szint 1. megfelelőségű (compliant) kriptográfiai szolgáltató és/vagy PKCS#11 interfész telepítve van és azok megfelelően működnek. A TOE a kriptográfiai műveletek végrehajtásához a FIPS 140-1 kriptográfiai szolgáltatót és/vagy a PKCS#11 interfészen keresztül a biztonságos aláírás létrehozó eszközt használja.

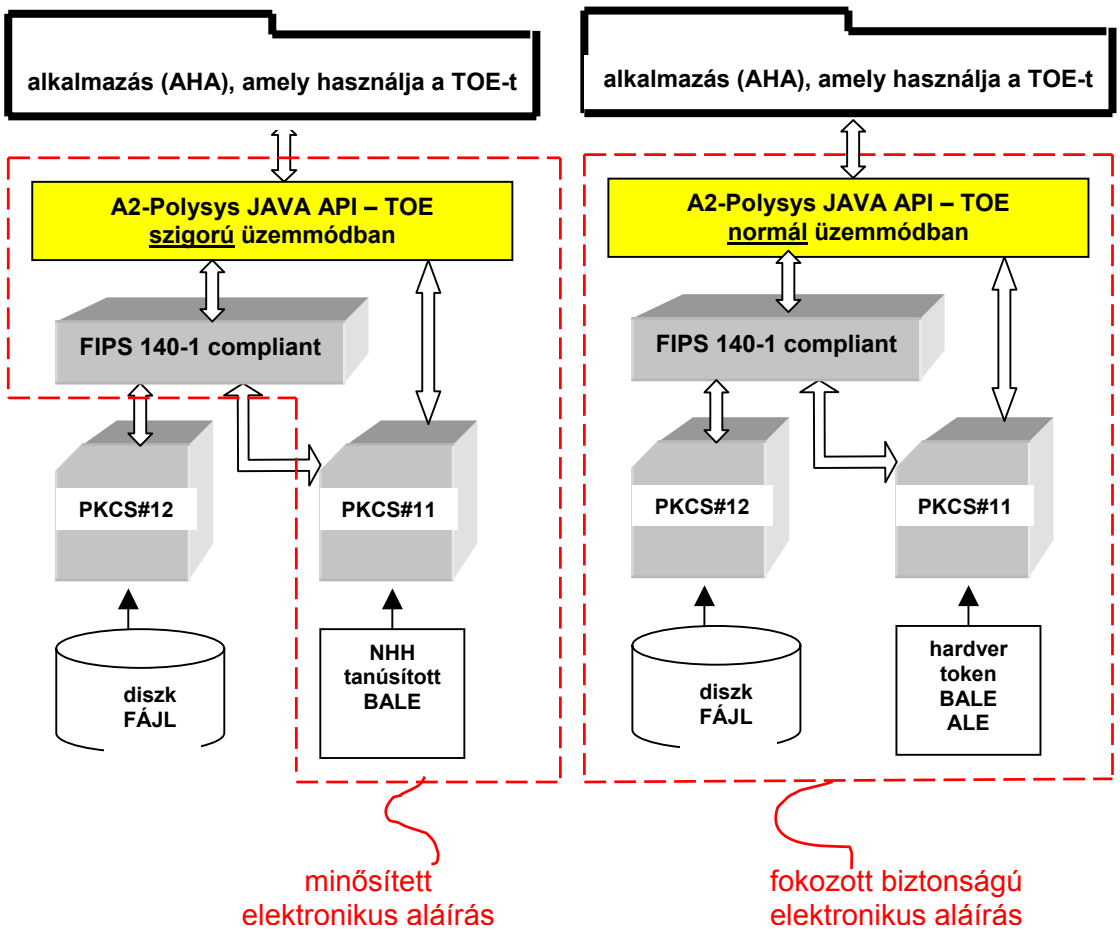
A TOE az AHA-n keresztül további, opcionális Java könytárakat is használ(hat), mint pl. SNTP kliens (pontos idő), JAAS szerviz (SSO), GUI komponens könyvtár, XML támogatás (Xalan, Xerces).

Az AHA az informatikai környezetből, a kulcstárolóból szerzi be a magánkulcsot az elektronikus aláírás létrehozásánál, illetve visszafejtésnél. A TOE két üzemmódban használható. Szigorú üzemmódban tanúsított eletronikus aláíráshoz, és a normál üzemmódban, fokozott biztonságú elektronikus aláíráshoz. Az alábbi ábrán piros szaggatott vonal határolja körül az elektronikus aláíráshoz kapcsolható logikai elemeket.

A szigorú üzemmód megköveteli az NHH által nyilvántartásba vett tanúsított aláírás létrehozó eszközt (BALE) használatát, amely a PKCS#11 interfészen keresztül tartja a kapcsolatot a TOE-val. A TOE lehetőséget biztosít arra, hogy az elektronikus aláírás alkalmazása során egyes kriptográfiai funkciókat az informatikai környezetbe telepített FIPS 140-1 megfelelő (compliant) kriptográfiai modul átvállaljon, pl. hash képzés , valós-véletlenszám generálás. Ennek a lehetőségnek a fenntartása a gyakorlati alkalmazások során bír jelentőséggel, mivel a BALE eszközök jelenleg limitált erőforrással rendelkeznek. Másrészt az azonosítás és hitelesítés eljárások határozottan elkülöníthetőek az elektronikus aláírás létrehozás vagy titkosítás visszafejtése tevékenységtől.

A normál üzemmódban PKCS#12 szoftveres kulcstároló vagy nem tanúsított aláírás létrehozó eszköz (ALE) is alkalmazható. Az üzemmód lehetővé teszi a TOE olyan AHA alkalmazásokban való használatát, amelyek fókusza nem tanúsított, hanem fokozott biztonságú elektronikus aláírás, vagy egyéb szolgáltatások (pl. titkosításon alapuló információ védelem, nagytömegű adat hitelesítés).

5. ábra: A TOE üzemmódjai



2.5 A környezettel szemben támasztott előfeltételek

Ez a fejezet leírja a TOE működési környezetét, a környezettel szemben támasztott előfeltételeket.

Szoftver konfiguráció:

- Operációs rendszer: Linux, Solaris, Unix, Java Desktop System, Windows, stb.
- JRE 1.5 vagy magasabb verziószámú Java futtató környezet (lásd 1. megjegyzés)
- PKCS#11 driver
- FIPS 140-1 kriptográfiai szolgáltató

1. megjegyzés:

A JRE 1.5 verzió tartalmazza a PKCS#11 kriptográfiai szolgáltató modult. Ha az adott platformon nem áll rendelkezésre az 1.5 vagy magasabb verzió, akkor az helyettesíthető JRE 1.4.2 + PKCS#11 kriptográfiai szolgáltató modul együttesével. A PKCS#11 kriptográfiai szolgáltató modul különböző gyártóktól szerezhető be.

Hardver konfiguráció:

- CPU: 400 MHz vagy magasabb
- RAM: 256 Mbyte vagy több
- Diszk hely: 20 Mbyte vagy több
- PKCS#11 token

Az alábbi táblázat részletezi a TOE-nak az informatikai környezettel szemben támasztott előfeltételeit, üzemmódok szerinti bontásban.

2. táblázat: A TOE informatikai környezettel szemben támasztott előfeltételei

üzemmód	elvárás
szigorú	• SUN JAVA JRE 1.5 vagy magasabb futtató környezet (lásd 1. megjegyzés) • FIPS 140-1 sorozat level 1 vagy magasabb szintnek megfelelő (compliant) kriptográfiai szolgáltató modul • PKCS#11 kompatibilis NHH által nyilvántartásba vett tanúsított biztonságos aláírás létrehozó eszköz (BALE) mint kulcstároló
normál	• SUN JAVA JRE 1.5 vagy magasabb futtató környezet (lásd 1. megjegyzés) • FIPS 140-1 sorozat level 1 vagy magasabb szintnek megfelelő (compliant) kriptográfiai szolgáltató modul • PKCS#12 vagy PKCS#11 kompatibilis kulcstároló

2.6 Informatikai környezet meghatározó biztonsági tulajdonságai

Java futtató környezet

A TOE közvetlen informatikai környezetét a Java virtuális gép alkotja. A Java nyelvet és a Java virtuális gépet kifejezetten a biztonság szem előtt tartásával tervezték. A Java minden részletre kiterjedő biztonsági szabályzata a Java virtuális gépben van implementálva.

A Java virtuális gép, mint közvetlen környezet egy védelmi szigetelő burkot képez a TOE és AHA együttese, valamint az operációs rendszer és azon esetleg futó „rosszindulatú” programok között.

A Java virtuális gép gondoskodik a memória elérésének a védelméről. A Java virtuális gép garantálja azt, hogy a Java által használt memória területek kinullázásra kerülnek, mielőtt

elengedné azt, és az adott memória terület használhatóvá válna a Java virtuális gépnek egy másik folyamata, vagy az operációs rendszer számára. A Java futtató környezet garantálja a Java programot futtató gép memóriájának integritását.

Az AHA és a TOE ugyanazon Java virtuális gépen belül futnak. Az AHA és a TOE metódus hívásokkal kommunikál, amelyet a Java virtuális gép hajt végre. A Java virtuális gép az entitások számára a private, protected, default, public elérési védelmeket biztosítja, lásd Java Language Specification, 2.0.
A TOE minden belső összetevője (class, method, member) privát, így a TOE meg van védve az AHA ellen is. A TOE által kezelt minden adat privát, így ezekhez az AHA-nak nincs hozzáférése. A TOE-nak csak azon összetevői nyilvánosak (public interface vagy public abstract class), amelyek az AHA számára a nyilvános interfészt reprezentálják.

PKCS#11 kulcstároló
A TOE számára bemenő paraméterek a hardver eszközben tárolt magánkulcsot azonosító címke (alias) és a felhasználói adatok (objektumok). A magánkulcsot használó műveletek esetében a PKCS#11 hardver eszköz interfésze, egy úgynevezett „proxy” objektumot biztosít a Java virtuális gép számára, amely kulcs anyagot (key material) nem tartalmaz. A proxy objektum egy csatlakozó, amely lehetővé teszi, hogy a Java program az objektumot „virtuális magánkulcsként” érzékelje és használja, miközben a magánkulcs soha nem hagyja el a tárolót. A PKCS#11 interfészen keresztül a proxy objektum kezdeményezi, hogy a kulcstároló eszköz a magánkulccsal a műveletet végezze el és annak eredményét adja vissza. Összefoglalva, a PKCS#11 eszköz használata esetén a művelet során használt magánkulcs anyagához a TOE sem férhet hozzá.

PKCS#12 kulcstároló
A TOE számára bemenő paraméterek a szoftveres kulcstárolóban (PFX fájl) tárolt magánkulcsot azonosító címke (alias) és a felhasználói adatok (objektumok). A TOE a magánkulcsot a fájl-ból beolvassa és a memóriában példányosítja. A kulcs példány a Java virtuális gép által felügyelt memóriában jelen van, a TOE számára látható. A TOE magánkulcsokat minden esetben privát adatként kezeli, így nem teszi lehetővé a kulcs anyagának (key material) vagy a kulcs példányának (instance) elérését, a Java virtuális gépben futó egyéb programok (pl. AHA) számára. A környezet, a Java virtuális gép gondoskodik a memória elérésének a védelméről, ahol ezek a kulcs anyagok vagy kulcs példányok jelen vannak, a használat befejezésekor azok kinullázásra kerülnek.

3 A TOE biztonsági környezete (ASE_ENV)

Ez a fejezet magában foglalja a következőket:

- biztonságos használat feltételezései
- fenyegetéseket
- a szervezetbiztonsági szabályzatokat

Ezek az információk alapul szolgálnak a 4. fejezetben kifejtésre kerülő „Biztonsági célkitűzéseknek”, az 5.1.1 fejezet, „TOE funkcionális biztonsági követelményeihez”, az 5.1.2 fejezet, „TOE csomagok biztonsági funkcionális követelményeihez”, 5.1.3 fejezet „A TOE garanciális követelményeihez”, továbbá a 5.2. fejezet, „Az informatikai környezet biztonsági követelményeihez”.

3.1 Feltételezések

Az alábbi táblázatban felsorolásra kerülnek a informatikai környezet biztonságos használatának feltételezései.

3. táblázat: Az informatikai környezet biztonságos használatának feltételezései

#	Feltételezés megnevezése	Leírás
1	AE.Authorized_Users	A jogosult felhasználók megbízhatóak a számukra kijelölt funkciók végrehajtására.
2	AE.Configuration	A TOE helyesen van installálva és konfigurálva.
3	AE.Crypto_Module_Normal	A TOE környezetéről fel van tételezve, hogy tartalmaz egy vagy több kriptográfiai szolgáltatót (modult), amelyek megfelelnek a FIPS 140-1, 1.szintnek vagy magasabb szintnek. Ez a modul, vagy ezek a modulok alkalmazásra kerülnek a következő műveletek során: kulcs pár generálás, elektronikus aláírás és ellenőrzés, titkosítás, visszafejtés, biztonságos lenyomat képzés, véletlenszám generálás, lenyomat képzéses Message Authentication Code (HMAC) eljárás, és/vagy egyéb szükséges kriptográfiai funkciók. Összegezve: a TOE minden kriptográfiai modulja FIPS 140-1 sorozat,1. szint vagy magasabb szintnek megfelelő (compliant) kell legyen.
4	AE.Crypto_Module_Rigid	A TOE környezetéről fel van tételezve, hogy tartalmaz legalább kettő kriptográfiai szolgáltatót, amelyek közül az egyiket NHH minősítéssel rendelkező BALE biztosít. a) A BALE kriptográfiai szolgáltatója alkalmazásra kerül a következő műveletek során: elektronikus aláírás, visszafejtés, biztonságos lenyomat képzés, véletlenszám generálás. b) A FIPS 140-1 sorozat,1. szint vagy magasabb szintnek megfelelő (compliant) kriptográfiai szolgáltató alkalmazásra kerül a következő műveletek során: elektronikus aláírás ellenőrzése, titkosítás, lenyomat képzés, véletlenszám generálás (FIPS-140-2 compliant), lenyomat képzéses Message Authentication Code (HMAC) eljárás, és/vagy egyéb szükséges kriptográfiai funkciók.

5	AE.Low	A TOE támadási lehetősége alacsonynak van feltételezve.
6	AE.Physical_Protection	A fizikai védelemről a környezet gondoskodik. A TOE hardver és szoftver elemei jogosulatlan fizikai hozzáférés ellen védettnek vannak feltételezve.
7	AE.PKI_Info	A TOE-nak tanúsítvány és tanúsítvány visszavonási lista információk a rendelkezésére állnak.
8	AE.Time	A környezet gondoskodik a megfelelő pontosságú rendszeridőről, GMT formátumban.

3.2 Fenyegetések

3.2.1 Alap fenyegetések

Ez a fejezet meghatározza a TOE alap fenyegetéseit az alábbi táblázatban. A támadás tárgya a TOE-hoz továbbított információ. Általában a fenyegetések (nem kizárólagos módon) származhatnak 1.) olyan személytől, aki hozzáfér a TOE-hoz, és akiről feltételezhető, hogy átlagos szakértelemmel, kevés erőforrással és közepes motivációval rendelkezik. vagy 2.) a TOE hibájából.

4. táblázat: Alap fenyegetések

#	Fenyegetés megnevezése	Fenyegetés leírása
1	T.Attack	A TOE egy észre nem vett kompromittálódása azt eredményezheti, hogy egy (akár belső, akár külső) támadó megkísérelheti egy olyan tevékenység végrehajtását, amelyre nem jogosult.
2	T.Bypass	Egy jogosulatlan magánszemély vagy felhasználó meghamisíthatja a biztonsági attributumokat vagy egyéb adatokat, a TOE biztonsági funkcióinak kikerülésére, és ezáltal a TOE erőforrásaihoz való jogosulatlan hozzáférésre.
3	T.Imperson	Egy jogosulatlan személy megszemélyesítheti a TOE-nak egy jogosult felhasználóját, és ezáltal hozzáférhet a TOE adataihoz, kulcsaihoz és műveleteihez.
4	T.Modify	Egy támadó módosíthatja a TSF vagy felhasználói adatokat, pl. a biztonsági attributumokat, kulcsokat, azzal a céllal, hogy hozzáférjen TOE-hoz és annak erőforrásaihoz.
5	T.Object_Init	Egy támadó jogosulatlan hozzáférést szerezhet egy objektumhoz annak létrejötte során, ha annak biztonsági attributumainak értékadása nem történt meg, vagy azt bárki ki el tudja végezni.
6	T.Private_key	Egy támadó színlelheti a felhasználó személyazonosságát, olyan módon, hogy generálja vagy felhasználja a felhasználó magánkulcsát.
7	T.Role	Egy felhasználó a számára engedélyezettnél több kiváltsággal rendelkező szerepet színlelhet, és kiterjesztett kiváltságokkal

		jogosulatlan tevékenységet végezhet.
8	T.Secure_Attributes	Egy felhasználó megváltoztathatja a biztonsági attributumait egy objektumnak, és ezáltal jogosulatlanul fér hozzá az objektumhoz.
9	T.Shoulder_Surf	Egy jogosulatlan felhasználó a jogosult felhasználó válla felett megfigyelheti a hitelesítési eljárást és elolvashatja a hitelesítési információkat.
10	T.Tries	Egy jogosulatlan személy próbálgatást és hibát kihasználva, találgatással meghatározhatja a hitelesítési információkat.

3.2.2 Csomagokhoz kapcsolható fenyegetések

A következő alfejezetek csomagokra bontva határozzák meg a biztonság fenyegetettségeit. A támadás tárgya a TOE-hoz továbbított információ. Általában a fenyegetések (nem kizárólagos módon) származhatnak 1.) olyan személytől, aki hozzáfér a TOE-hoz, és akiről feltételezhető, hogy átlagos szakértelemmel, kevés erőforrással és közepes motivációval rendelkezik. vagy 2.) a TOE hibájából.

Megjegyzés: A fenti táblázatban meghatározott alapfenyegetéseken túl, a további fejezetek tartalmazzák az egyes csomagokhoz kapcsolódó fenyegetéseket.

3.2.2.1 Tanúsítási útvonal érvényesítése (CPV- alap)

Az alábbi fenyegetések a Tanúsítási útvonal érvényesítése (CPV) – Alap csomaghoz kapcsolódnak és hozzáadódnak az alap fenyegetésekhez.

5. táblázat: Fenyegetések a Tanúsítási útvonal érvenyesítése csomagban

#	Fenyegetés megnevezése	Fenyegetés leírása
1	T.Certificate_Modi	Egy nem megbízható felhasználó módosíthatja a tanúsítványt, ami azt eredményezi, hogy rossz nyilvános kulcs lesz használva.
2	T.DOS_CPV_Basic	A visszavonási információ vagy a visszavonási információ elérése lehetetlenné válik, ami azt eredményezi, hogy a rendszer elveszíti a használhatóságát.
3	T.Expired_Certificate	Egy lejárt (és esetleg visszavont) tanúsítvány felhasználható aláírás ellenőrzésre.
4	T.Masquarade	Egy nem megbízható entitás (CA) kiadhat tanúsítványokat ál (hamis) entitásoknak, megengedve azoknak, hogy színleljék más legitim felhasználók személyazonosságát.
5	T.No_Crypto	A felhasználó nyilvános kulcsa és a kapcsolódó információk lehet, hogy nem állnak rendelkezésre a kriptográfiai funkció végrehajtására.
6	T.Path_Not_Found	A valós érvényesítési útvonal nem található meg, a rendszer működőképességének hiányában.

7	T.Revoked_Certificate	Egy visszavont tanúsítvány érvényesként felhasználható, és ez a biztonság veszélyeztetését eredményezi.
8	T.User_CA	Egy felhasználó CA-ként léphet fel és jogosulatlan tanúsítványt adhat ki.

3.2.2.2 PKI aláírás készítés

Az alábbi fenyegetések a PKI aláírás készítés csomaghoz kapcsolódnak és hozzáadódnak az alap fenyegetésekhez.

6. táblázat: Fenyegetések a PKI aláírás készítés csomagban

#	Fenyegetés megnevezése	Fenyegetés leírása
1	T.Clueless_PKI_Sig	A felhasználó útmutatás hiányában csak nem megfelelő tanúsítványokkal próbálkozik az aláírásnál.

3.2.2.3 PKI aláírás ellenőrzés

Az alábbi fenyegetések a PKI aláírás ellenőrzés csomaghoz kapcsolódnak és hozzáadódnak az alap fenyegetésekhez.

7. táblázat: Fenyegetések a PKI aláírás ellenőrzés csomagban

#	Fenyegetés megnevezése	Fenyegetés leírása
1	T.Assumed_Identity_PKI_Ver	Egy felhasználó az aláíró személyére mást feltételezhet egy PKI aláírás ellenőrzése során.
2	T.Clueless_PKI_Ver	A felhasználó útmutatás hiányában csak nem megfelelő tanúsítványokkal próbálkozik az aláírás ellenőrzésénél.

3.2.2.4 PKI titkosítás kulcs átviteli algoritmusokkal

Az alábbi fenyegetések a PKI titkosítás kulcsátviteli algoritmusokkal csomaghoz kapcsolódnak és hozzáadódnak az alap fenyegetésekhez.

8. táblázat: Fenyegetések a PKI titkosítás kulcs átviteli algoritmusokkal csomagban

#	Fenyegetés megnevezése	Fenyegetés leírása
1	T.Assumed_Identity_WO_En	Egy felhasználó a címzett személyére mást feltételezhet, egy kulcs átviteli algoritmussal végrehajtott titkosítás során.
2	T.Clueless_WO_En	A felhasználó útmutatás hiányában csak nem megfelelő tanúsítványokkal próbálkozik a titkosítás végzésénél.

3.2.2.5 PKI visszafejtés kulcs átviteli algoritmusokkal

Az alábbi fenyegetések a PKI visszafejtés kulcs átviteli csomaghoz kapcsolódnak és hozzáadódnak az alap fenyegetésekhez. Ezek a fenyegetések egyaránt szerepelnek EAL3 kiterjesztett és EAL4 kiterjesztett garancia szintek esetén.

9. táblázat: Fenyegetések a PKI visszafejtés kulcs átviteli algoritmusokkal csomagban

#	Fenyegetés megnevezése	Fenyegetés leírása
1	T.Garble_WO_De	A felhasználó nem a megfelelő kulcs átviteli algoritmust vagy nem a megfelelő magánkulcsot alkalmazhatja, ami az adatok összezagyválását eredményezi..

3.2.2.6 Tanúsítvány visszavonási lista (CRL) érvényesítés

Az alábbi fenyegetések a Tanúsítvány visszavonási lista (CRL) csomaghoz kapcsolódnak és hozzáadódnak az alap fenyegetésekhez.

10. táblázat: Fenyegetések a tanúsítvány visszavonási lista (CRL) érvényesítés csomagban

#	Fenyegetés megnevezése	Fenyegetés leírása
1	T.DOS_CRL	A CRL vagy a CRL hozzáférés elérhetetlenné válik és emiatt a rendszer elveszíti a rendelkezésre állását.
2	T.Replay_Revoc_Info_CRL	A felhasználó elfogadhat egy régi CRL-t, ami egy már visszavont tanúsítvány elfogadását eredményezheti.
3	T.Wrong_Revoc_Info_CRL	A felhasználó elfogadhat egy visszavont tanúsítványt vagy visszautasíthat egy érvényes tanúsítványt, egy rossz CRL miatt.

3.2.2.7 Időbélyeg kliens

Az alábbi fenyegetések az Időbélyeg kliens csomaghoz kapcsolódnak és hozzáadódnak az alap fenyegetésekhez.

11. táblázat: Fenyegetések az Időbélyeg kliens csomagban

#	Fenyegetés megnevezése	Fenyegetés leírása
1	T.DOS_TSP	Az időbélyeg válasz vagy az időbélyeg szolgáltatáshoz való hozzáférés elérhetetlenné válik és emiatt a rendszer elveszíti a rendelkezésre állását.
2	T.Replay_TSP_Info	A felhasználó elfogadhat egy régi időbélyeg választ, ami egy már visszavont tanúsítvány elfogadását eredményezheti.
3	T.Wrong_TSP_Info	A felhasználó elfogadhat egy visszavont tanúsítványt vagy visszautasíthat egy érvényes tanúsítványt, egy rossz időbélyeg válasz miatt.

3.2.2.8 Valós idejű tanúsítvány állapot protokoll (OCSP) kliens

Az alábbi fenyegetések a valós idejű tanúsítvány állapot protokoll (OCSP) kliens csomaghoz kapcsolódnak és hozzáadódnak az alap fenyegetésekhez.

12. táblázat: Fenyegetések az OCSP kliens csomagban

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

3.3 Szervezet biztonsági szabályzatok

A TOE nem követel meg szervezet biztonsági szabályzatot.

4 Biztonsági célkitűzések (ASE_OBJ)

Ez a fejezet két részre bontja a biztonsági célkitűzéseket, leírja a TOE biztonsági céljait, és az informatikai környezet biztonsági céljait.

A biztonsági előirányzat alapjaként szolgáló védelmi profil család meghatározza azokat az alap biztonsági célkitűzéseket, amelyet a családból származó minden védelmi profilnak ki kell elégítenie, így a védelmi profilból származó biztonsági előirányzatnak is.
Ezeket a továbbiakban 1.) A TOE biztonsági célkitűzéseinek, és 2.) Az informatikai környezet alap biztonsági célkitűzéseinek nevezzük.

Megjegyezzük azt, hogy az informatikai környezet biztonsági célkitűzéseit „OE" előtag jelzi, míg ellenkező esetben az „O" előtag jelzést alkalmazzuk.

Az alap biztonsági célkitűzések meghatározását követik a csomagokhoz tartozó egyedi célkitűzések. Az egyedi célkitűzések minden esetben feltételezik az alap célkitűzéseket is.

Az alábbi táblázat egymáshoz rendeli a jelen ST és a PP megfelelő fejezeteit.

13. táblázat: A PP és ST fejezetek egymáshoz rendelése

PP		ST	
Fejezet #	**Fejezet cím**	**Fejezet #**	**Fejezet cím**
4.1	A TOE alap biztonsági célkitűzései	4.1	A TOE biztonsági célkitűzései
		4.1.1	A TOE alap biztonsági célkitűzései
4.2	A környezet biztonsági célkitűzései	4.2	Az informatikai környezet biztonsági célkitűzései
4.3	A csomagok biztonsági célkitűzései	4.1.2	A TOE biztonsági célkitűzései csomagok szerint

4.1 A TOE biztonsági célkitűzései

Ez a fejezet a TOE biztonsági célkitűzéseit írja le. A 4.1.1 alfejezet leírja a TOE alap biztonsági célkitűzéseit, a 4.1.2 alfejezet leírja a TOE biztonsági célkitűzéseit a csomagok szerint.

4.1.1 A TOE alap biztonsági célkitűzései

14. táblázat: A TOE alap biztonsági célkitűzései

#	Célkitűzés megnevezése	Célkitűzés leírása
1	O.DAC	A TSF ellenőrzi és korlátozza a felhasználó hozzáférését a TOE erőforrásaihoz, összhangban a meghatározott hozzáférés ellenőrzés szabályzattal.
2	O.I&A	A TSF egyedileg azonosít minden felhasználót, és hitelesíti az igényelt személyazonosságot, mielőtt engedélyezné a felhasználó hozzáférését a TOE lehetőségeihez.
3	O.Init_Secure_Attr	A TSF-nek a biztonsági attributumokra érvényes alapértékeket kell

		biztosítani az objektum inicializálódásakor.
4	O.Invoke	A TSF minden művelet során meghívásra kerül.
5	O.Limit_Actions_Auth	A TSF korlátozza a felhasználó által végezhető tevékenységeket, mielőtt a TSF ellenőrizné a felhasználó személyazonosságát.
6	O.Limit_Tries	A TSF korlátozza az egymást követő sikertelen hitelesítési kísérleteket.
7	O.No_Echo	A TSF nem jelez vissza hitelesítési információkat.
8	O.Protect_I&A_Data	A TSF csak jogosult felhasználó számára engedélyezi az I&A (a felhasználót azonosító) adatok megváltoztatását.
9	O.Secure_Attributes	A TSF csak jogosult felhasználó számára engedélyezi a biztonsági attributumok megváltoztatását.
10	O.Security_Roles	A TSF karbantartja a biztonsággal összefüggő szerepeket, és a felhasználók kapcsolatát ezekhez a szerepekhez.
11	O.Self_Protect	A TSF karbantartja a saját végrehajtási környezetét, amely védi önmagát és erőforrásait a külső beavatkozásoktól, megmásítástól, jogosulatlan közzétételtől.
12	O.Trust_Anchor	A TSF csak jogosult felhasználó számára engedélyezi a megbízható legfelső szintű hitelesítő tanúsítványok kezelését.
13	O.TSF_Data	A TSF csak jogosult felhasználó számára engedélyezi a TSF adatok módosítását.

4.1.2 A TOE biztonsági célkitűzései csomagok szerint

A biztonsági célkitűzések csomagok szerinti meghatározása minden esetben hozzáadódik a TOE alap biztonsági célkitűzéseihez, valamint az informatikai környezet biztonsági célkitűzéseihez.

4.1.2.1 Tanúsítási útvonal érvényesítése (CPV) - Alap

Ezek a biztonsági célkitűzések a Tanúsítási útvonal érvényesítése (CPV) - Alap csomaghoz lettek meghatározva.

15. táblázat: Biztonsági célkitűzések a Tanúsítási útvonal érvényesítése (CPV) - Alap csomaghoz

#	Célkitűzés megnevezése	Célkitűzés leírása
1	O.Availability	A TSF biztosítja a biztonsági szolgáltatásokat, akkor is, ha a visszavonási információ nem áll rendelkezésre.
2	O.Correct_Time	A TSF gondoskodik precíz átmeneti érvényesítési eredményekről.
3	O.Current_Certificate	A TSF csak akkor fogadja el a tanúsítványokat, ha azok nem jártak

		le.
4	O.Get_KeyInfo	A TSF-nek a kriptográfiai funkciók végrehajtása céljából biztosítania kell a felhasználó nyilvános kulcsát és a kapcsolódó információkat.
5	O.Path_Find	A TSF képes lesz megtalálni a tanúsítási útvonalat a megbízható legfelső szintű hitelesítő tanúsítványtól a végtanúsítványig.
6	O.Trusted_Keys	A TSF megbízható nyilvános kulcsokat használ a tanúsítási útvonal érvényesítésénél.
7	O.User	A TSF csak CA által kiadott tanúsítványokat fogad el.
8	O.Verified_Certificate	A TSF csak ellenőrizhető aláírással ellátott tanúsítványokat fogad el.
9	O.Valid_Certificate	A TSF csak érvényes, azaz nem visszavont tanúsítványokat használ.

4.1.2.2 PKI aláírás készítés

Ezek a biztonsági célkitűzések a PKI aláírás készítés csomaghoz lettek meghatározva.

16. táblázat: Biztonsági célkitűzések a PKI aláírás készítés csomaghoz

#	Célkitűzés megnevezése	Célkitűzés leírása
1	O.Give_Sig_Hints	A TSF útmutatást ad a helyes tanúsítány kiválasztására az aláírás ellenőrzésénél.

4.1.2.3 PKI aláírás ellenőrzés

Ezek a biztonsági célkitűzések a PKI aláírás ellenőrzés csomaghoz lettek meghatározva.

17. táblázat: Biztonsági célkitűzések a PKI aláírás ellenőrzés csomaghoz

#	Célkitűzés megnevezése	Célkitűzés leírása
1	O.Use_Sig_Hints	A TSF az útmutatást használja a helyes tanúsítvány kiválasztására az aláírás ellenőrzésénél.
2	O.Linkage_Sig_Ver	A TSF a helyes felhasználói nyilvános kulcsot használja az aláírás ellenőrzésénél.

4.1.2.4 PKI titkosítás kulcs átviteli algoritmusokkal

Ezek a biztonsági célkitűzések a PKI titkosítás kulcs átviteli algoritmusokkal csomaghoz lettek meghatározva.

18. táblázat: Biztonsági célkitűzések a PKI titkosítás kulcs átviteli algoritmusokkal csomaghoz

#	Célkitűzés megnevezése	Célkitűzés leírása
1	O.Hints_Enc_WO	A TSF útmutatást ad a helyes tanúsítványok vagy kulcsok kiválasztására a PKI kulcs átviteli algoritmusokkal történő titkosításhoz.
2	O.Linkage_Enc_WO	A TSF a helyes felhasználói nyilvános kulcsot használja a kulcsátvitel során.

4.1.2.5 PKI visszafejtés kulcs átviteli algoritmusokkal

Ezek a biztonsági célkitűzések a PKI visszafejtés kulcs átviteli algoritmusokkal csomaghoz lettek meghatározva.

19. táblázat: Biztonsági célkitűzések a PKI visszafejtés kulcs átviteli algoritmusokkal csomaghoz

#	Célkitűzés megnevezése	Célkitűzés leírása
1	O.Correct_KT	A TSF a megfelelő magánkulcsot és kulcsátviteli algoritmust használja.

4.1.2.6 Tanúsítvány visszavonási lista (CRL) érvényesítés

Ezek a biztonsági célkitűzések a Tanúsítvány visszavonási lista (CRL) érvényesítés csomaghoz lettek meghatározva.

20. táblázat: Biztonsági célkitűzések a Tanúsítvány visszavonási lista (CRL) érvényesítés csomaghoz

#	Célkitűzés megnevezése	Célkitűzés leírása
1	O.Accurate_Rev_Info	A TSF csak pontos visszavonási információkat fogad el.
2	O.Auth_Rev_Info	A TSF a visszavonási információkat jogosult CRL forrásból fogadja el.
3	O.Fresh_Rev_Info	A TSF csak megfelelően időszerű CRL-t fogad el.
4	O.User_Override_Fresh_CRL	A TSF engedélyezi a felhasználónak, hogy hatástalanítsa a CRL frissességének követelményét.

4.1.2.7 Időbélyeg kliens

Ezek a biztonsági célkitűzések az Időbélyeg kliens csomaghoz lettek meghatározva.

21. táblázat: Biztonsági célkitűzések az Időbélyeg kliens csomaghoz

#	Célkitűzés megnevezése	Célkitűzés leírása
1	O.Accurate_TSP_Info	A TSF csak pontos időbélyeg választ fogad el.
2	O.Auth_TSP_Info	A TSF az időbélyeg válaszokat csak jogosult TSA forrásból fogadja el.
3	O.Fresh_TSP_Info	A TSF mindig új időbélyeg kérést küld és csak az arra adott időbélyeg választ fogadja el.
4	O.User_Decide_TSP	A TSF engedélyezi a felhasználónak, annak meghatározását, hogy mikor történjen az időbélyeg kérés.

4.1.2.8 Valós idejű tanúsítvány állapot protokoll (OCSP) kliens

Ezek a biztonsági célkitűzések a valós idejű tanúsítvány állapot protokoll (OCSP) kliens csomaghoz lettek meghatározva.

22. táblázat: Biztonsági célkitűzések az OCSP kliens csomaghoz

#	Célkitűzés megnevezése	Célkitűzés leírása
1	O.Accurate_OCSP_Info	A TSF csak pontos OCSP választ fogad el.
2	O.Auth_OCSP_Info	A TSF a visszavonási információkat csak jogosult OCSP forrásból fogadja el.
3	O.Fresh_OCSP_Info	A TSF csak megfelelően aktuális visszavonási információkat fogad el az OCSP tranzakciók esetén.
4	O.User_Override_Fresh_OCSP	A TSF engedélyezi a felhasználónak, hogy felülbírálja az OCSP válasz frisseségének ellenőrzését.

4.2 Az informatikai környezet biztonsági célkitűzései

Az alábbi táblázat felsorolja az informatikai környezet biztonsági célkítűzéseit.

23. táblázat: Az informatikai környezet biztonsági célkitűzései

#	Célkitűzés megnevezése	Célkitűzés leírása
1	OE.Authorized_Users	A jogosult felhasználók megbízhatóak, hogy végrehajtsák jogosult feladataikat.
2	OE.Configuration	A TOE helyesen van installálva és konfigurálva, ahhoz, hogy a TOE biztonságos állapotban induljon.
3	OE.Crypto_Normal	A TOE környezetének tartalmaznia kell egy vagy több kriptográfiai szolgáltatót (modult), amelyek megfelelnek a FIPS 140-1 sorozat 1.szintnek vagy magasabb szintnek. Ez a modul, vagy ezek a modulok alkalmazásra kerülnek a következő műveletek során: kulcs pár generálás, elektronikus aláírás és ellenőrzés, titkosítás, visszafejtés, biztonságos lenyomat képzés, véletlenszám generálás, lenyomat képzéses Message Authentication Code (HMAC) eljárás, és/vagy egyéb szükséges kriptográfiai funkciók. Összegezve: a TOE minden kriptográfiai modulja FIPS 140 sorozat,1. szint vagy magasabb szintnek megfelelő (compliant) kell legyen.
4	OE.Crypto_Rigid	A TOE környezetének tartalmaznia kell legalább kettő kriptográfiai szolgáltatót, amelyek közül az egyiket NHH minősítéssel rendelkező BALE biztosít. a) A BALE kriptográfiai szolgáltatója alkalmazásra kerül a következő műveletek során: elektronikus aláírás, visszafejtés, biztonságos lenyomat képzés, véletlenszám generálás. b) A FIPS 140-1 sorozat,1. szint vagy magasabb szintnek megfelelő (compliant) kriptográfiai szolgáltató alkalmazásra kerül a következő műveletek során: elektronikus aláírás ellenőrzése, titkosítás, lenyomat képzés, véletlenszám generálás (FIPS-140-2 compliant), lenyomat képzéses Message Authentication Code (HMAC) eljárás, és/vagy egyéb szükséges kriptográfiai funkciók.
5	OE.Low	A TOE azonosítási és hitelesítési funkciói legalább alacsony támadási lehetőségre vannak tervezve és megvalósítva, ahogy azt a sebezhetőségi értékelés és a funkció erősség vizsgálat analízis (Strength of Function analyses) jóváhagyta.
6	OE.Physical_Security	A környezetnek gondoskodnia kell a fizikai biztonság egy elfogadható szintjéről azon célból, hogy a környezet a TOE-t ne befolyásolhassa vagy ne lehessen tárgya megkerülő csatorna támadásoknak, mint az erő analízis és idő analízis különböző formái.
7	OE.PKI_Info	Az informatikai környezetnek szolgáltatnia kell a TOE számára tanúsítványokat és a tanúsítvány visszavonási információkat.
8	OE.Time	A környezetnek gondoskodnia kell az aktuális idő eléréséről, a megkövetelt pontosság szerinti, GMT formában.

5 Az informatikai biztonság követelményei (ASE_REQ)

Ez a fejezet az 5.1 alfejezetben a TOE biztonsági funkcionális követelményeit és a garanciális követelményeit, az 5.2 alfejezetben az informatikai környezet biztonsági követelményeit írja le.

A követelmények a CC 2. és 3. kötetéből származnak. A CC 2.kötete nem tartalmazza az összes lehetséges biztonsági funkcionális követelményt, ezért a jelen ST alapját képező PKE PP, a CC 2. kötet kiterjesztéseként nem szabványos biztonsági követelményeket is bevezetett. Az 5.1 táblázat minden egyes ST funkcionális követelményre meghatározza, hogy az a CC 2. kötetéből, vagy annak kiterjesztéséből származik.

24. táblázat: Biztonsági követelmények származása

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

A PKE PP szögletes zárójelek között, *[dőlt]* szedéssel jelzi az ST-ben végzendő kiválasztásokat (selection) és az értékadásokat (assignment). Ezek a kiválasztások és értékadások jelen ST-ben a szögletes zárójelek elhagyásával *aláhúzásra kerülnek, dőlt betűvel szedve*.
Félkövér dőlt szedés jelzi azt a szövegrészt, ahol jelen ST alapját képező PKE PP, a CC 2. kötet követelményeit finomította.
Dőlt szedés jelzi azt a szövegrészt, ahol jelen ST alapját képező PKE PP, a CC 2. kötet követelményeiben kiválasztást (selection) vagy értékadást (assignment) műveletet végzett.

5.1 A TOE biztonsági követelményei

Az 5.1.1 fejezet leírja a TOE alap biztonsági funkcionális követelményeket.
Az 5.1.2 fejezet leírja a TOE csomagok biztonsági funkcionális követelményeit.
Az 5.1.3 fejezet leírja a TOE EAL 3+ kibővített biztonsági garanciális követelményeit.

5.1.1 A TOE alap biztonsági funkcionális követelményei

Az alapkövetelmények meghatározzák azt a képességet, hogy több magánkulcs, az ezekhez tartozó tanúsítványok, valamint azonosító adatok és ezek közötti hivatkozások menedzselhetők. A menedzselés kifejezés azt jelenti, hogy megtehető egy vagy több dolog a következők közül: generálás, megsemmisítés törlés, használat, import, export, módosítás, stb. Az azonosító adat és a társítás a magánkulcs és a nyilvános kulcs között, a megfelelő kriptográfiai kulcsok kiválasztására használatos, amelyekkel a TOE által végzett kriptográfiai művelet elvégzésre kerül. Az alapkövetelmények biztosítják a megbízható legfelső szintű hitelesítő tanúsítványok biztonságos tárolását.

25. táblázat: A TOE alap biztonsági funkcionális követelményei

#	Funkcionális követelmény	Cím
1	FDP_ACC.1	Hozzáférés ellenőrzés részhalmaza – PKI megbízólevél menedzsment
2	FDP_ACF.1	Biztonsági attributum alapú hozzáférés ellenőrzés - PKI megbízólevél menedzsment
3	FIA_AFL.1	Hitelesítési sikertelenség kezelése
4	FIA_ATD.1	Felhasználói attributum meghatározása
5	FIA_UAU.1	Hitelesítés időzítése
6	FIA_UID.1	Azonosítás időzítése
7	FIA_UAU.7	Védett hitelesítési visszajelzés
8	FMT_MSA.1	Biztonsági attributumok menedzsmentje
9	FMT_MSA.3	Statikus attributum inicializáció
10	FMT_MTD.1	A TSF adatok menedzsmentje
11	FMT_SMF.1	Menedzsment funkciók specifikációja
12	FMT_SMR.2	Biztonsági szerepkörök szigorításai
13	FPT_RVM.1	A TSP kikerülhetetlensége
14	FPT_SEP.1	TSF körzetszétválasztás

5.1.1.1 Felhasználói adat védelem (FDP)

FDP_ACC.1 Hozzáférés ellenőrzés részhalmaza – PKI megbízólevél menedzsment

Hierarchikus kapcsolat: nincs más komponenshez.

FDP_ACC.1.1 A TSF-nek érvényesítenie kell a *PKI megbízólevél menedzsment SFP-t* a
- *a) Szubjektum: felhasználó nevében végrehajtott folyamat*
- *b) Objektum: adat, amely a TOE számára átadásra kerül a kriptográfiai művelet végzéséhez, vagy amelyet a TOE ad át tárolásra, vagy egyéb használatra*
- c) *Művelet: a TOE által biztosított kriptográfiai művelet, a TOE működését vezérlő paraméterek beállítása/lekérdezése*

között.

Függőség: FDP_ACF.1 Biztonsági attributum alapú hozzáférés ellenőrzés

FDP_ACF.1 Biztonsági attributum alapú hozzáférés ellenőrzés – PKI megbízólevél menedzsment

Hierarchikus kapcsolat: nincs más komponenshez.

FDP_ACF.1.1 A TSF-nek érvényesítenie kell a *PKI megbízólevél menedzsment SFP-t* olyan objektumokon, amelyek *a szubjektum azonosságán és egy olyan szerep halmazon alapul, amelyet a szubjektum jogosult felvenni.*

FDP_ACF.1.2 A TSF-nek érvényesítenie kell az alábbi szabályokat, hogy megállapíthassa, engedélyezett-e a művelet az ellenőrzött szubjektumok és objektumok között:
- ***a) Magánkulcs importálható, használható, a felhasználó nevében végrehajtott folyamatok által.***
- ***b) Nyilvános kulcsú tanúsítványok importálhatók, exportálhatók, törölhetők a felhasználó nevében végrehajtott folyamatok által.***
- ***c) Nyilvános kulcsú tanúsítványok használhatók a felhasználó nevében végrehajtott folyamatok által.***
- ***d) Titkos kulcs generálható, megsemmisíthető, használható a felhasználó nevében végrehajtott folyamatok által.***
- ***e) Titkos kulcs kizárólag aszimmetrikus titkosítással csomagolva importálható és exportálható.***

FDP_ACF.1.3 A TSF-nek félreérthetetlenül hitelesítenie kell a szubjektumoknak az objektumokhoz való hozzáférését, amely az alábbi kiegészítő szabályokon alapul: *nincs további szabály.*

FDP_ACF.1.4 A TSF-nek félreérthetetlenül meg kell tagadnia a szubjektumoknak az objektumokhoz való azon hozzáférést, *ha az I&A (a felhasználót azonosító) adatokat tároló eszköz (kulcstároló) az adott pillanatban nem elérhető.*

Függőség: FDP_ACC.1 Hozzáférés ellenőrzés részhalmaza
FMT_MSA.3 Statikus attributum inicializáció

5.1.1.2 Azonosítás és hitelesítés (FIA)

FIA_AFL.1 Hitelesítési sikertelenség kezelése

Hierarchikus kapcsolat: nincs más komponenshez.

FIA_AFL.1.1 A TSF-nek észlelnie kell, amikor *a használó alkalmazás által konfigurálható számú* sikertelen hitelesítési próbálkozás fordul elő *a kijelölt felhasználó azonosság hitelesítésére irányuló utolsó sikeres próbálkozás óta végbement sikertelen hitelesítési próbálkozásokat* illetően.

FIA_AFL.1.2 Amikor a sikertelen hitelesítési próbálkozások száma elér vagy meghalad egy meghatározott számot, a TSF-nek *a TOE képességeinek igénybevételét a használó alkalmazás számára meg kell tagadnia.*

Függőség: FIA_UAU.1 Hitelesítés időzítése

FIA_ATD.1 Felhasználói attributum meghatározása

Hierarchikus kapcsolat: nincs más komponenshez.

FIA_ATD.1.1 A TSF-nek karban kell tartania az alábbi biztonsági attributum-listát, amely különálló felhasználókhoz tartozik: *az I&A (a felhasználót azonosító) adatokat tároló eszköz (kulcstároló) jellemzői.*

Függőség: Nincs

FIA_UAU.1 Hitelesítés időzítése

Hierarchikus kapcsolat: nincs más komponenshez.

FIA_UAU.1.1 A TSF-nek lehetővé kell tenni *a használó alkalmazás által konfigurálható paraméterek átadását* a felhasználó nevében, mielőtt a felhasználó hitelesítésre kerül.

FIA_UAU.1.2 A TSF-nek meg kell követelnie, hogy minden egyes felhasználó sikeresen hitelesítve legyen, mielőtt bármelyik másik TSF által közvetített tevékenységet engedélyezne annak a felhasználónak a nevében.

Függőség: FIA_UID.1 Azonosítás időzítése

FIA_UAU.7 Védett hitelesítési visszajelzés

Hierarchikus kapcsolat: nincs más komponenshez.

FIA_UAU.7.1 A TSF-nek csak *a begépelt karaktereknek csak a * (csillag) mintával történő visszajelzését* kell biztosítania a felhasználó számára, mialatt a hitelesítés folyamatban van.

Függőség: FIA_UID.1 Azonosítás időzítése

FIA_UID.1 Azonosítás időzítése

Hierarchikus kapcsolat: nincs más komponenshez.

FIA_UID.1.1 A TSF-nek lehetővé kell tennie ***a használó alkalmazás által konfigurálható paraméterek átadását*** a felhasználó nevében, mielőtt a felhasználó azonosítása megtörténik.

FIA_UID.1.2 A TSF-nek meg kell követelnie minden egyes felhasználó sikeres azonosítását, mielőtt bármelyik másik, TSF által közvetített tevékenységet engedélyez annak a felhasználónak a nevében.

Függőség: Nincs.

5.1.1.3 Biztonság menedzsment (FMT)

FMT_MSA.1 Biztonsági attributumok menedzsmentje

Hierarchikus kapcsolat: nincs más komponenshez.

FMT_MSA.1.1 A TSF-nek érvényre kell juttatnia a *PKI megbízólevél menedzsment SFP-t*, hogy korlátozza: a ***lekérdezését, megváltoztatását, törlését, kiválasztását*** a következő vezérlő biztonsági attributumoknak: ***az I&A (a felhasználót azonosító) adatok, TOE működését vezérlő paraméterek, kriptográfiai műveleteket befolyásoló paraméterek***, az ***azonosított és hitelesített felhasználó nevében végrehajtott folyamatokra***.

Függőség: FMT_SMF.1 Menedzsment funkciók specifikációja
FMT_SMR.1 Biztonsági szerepkörök
FDP_ACC.1 Hozzáférés ellenőrzés részhalmaza

FMT_MSA.3 Statikus attributum inicializáció

Hierarchikus kapcsolat: nincs más komponenshez.

FMT_MSA.3.1 A TSF-nek érvényesítenie kell a *PKI megbízólevél menedzsment SFP-t,* hogy biztosítsa a *megfelelő* alapértelmezett értékeket a biztonsági attributumok számára, amelyek az SFP végrehajtásakor használatosak.

FMT_MSA.3.2 A TSF-nek lehetővé kell tennie ***a felhasználó nevében végrehajtott folyamat*** számára a lehetséges kezdeti értékek meghatározását abból a célból, hogy felülírja az alapértékeket, amikor egy objektum vagy információ készül.

Függőség: FMT_SMR.1 Biztonsági szerepkörök
FMT_MSA.1 Biztonsági attributumok menedzsmentje

FMT_MTD.1 A TSF adatok menedzsmentje

Hierarchikus kapcsolat: nincs más komponenshez.

FMT_MTD.1.1 A TSF-nek korlátoznia kell a: *megváltoztatását, törlését, üresítését,* ***importálását, hozzáadását****,* a ***megbízható legfelső szintű hitelesítő tanúsítványok****,* ***közbenső szintű hitelesítő tanúsítványok, saját tanúsítványok, más személyek tanúsítványai, tanúsítvány visszavonási listák, a CRL a kibocsátást követően hány napig aktuális, a CRL a következő kibocsátást követő hány napig aktuális, CRL frissesség ellenőrzés engedélyezése, visszavonás ellenőrzés kihagyhatóság engedélyezése, megbízható időszerverek, szolgáltatás igénybevétele utáni kényszerített kijelentkeztetés engedélyezése, OCSP válasz az előállítást követő hány percig aktuális, OCSP válasz a kibocsátást követő hány percig aktuális, OCSP válasz a következő kibocsátást követő hány percig aktuális, OCSP válasz frissesség ellenőrzés engedélyezése, időbélyeg szolgáltatás elérhetősége, OCSP szolgáltatás elérhetősége, szervezeti aláírási szabályzat*** a ***felhasználó nevében végrehajtott folyamatokra****.*

Függőség: FMT_SMF.1 Menedzsment funkciók specifikációja
FMT_SMR.1 Biztonsági szerepkörök

FMT_SMF.1 Menedzsment funkciók specifikációja

Hierarchikus kapcsolat: nincs más komponenshez.

FMT_SMF.1.1 A TSF-nek alkalmasnak kell lennie arra, hogy végrehajtsa következő biztonsági menedzsment funkciókat:

a) a használó alkalmazás által konfigurálható paraméterek importálását
b) önellenőrzés
c) azonosítás, hitelesítés és jogosultság ellenőrzés, a felhasználó bejelentkeztetése a kulcstárolóhoz
d) a következő biztonsági attributumok menedzsmentje:
- *megbízható legfelső szintű hitelesítő tanúsítványok,*
- *közbenső szintű hitelesítő tanúsítványok*
- *saját tanúsítványok*
- *más személyek tanúsítványai*
- *tanúsítvány visszavonási listák*
- *a CRL a kibocsátást követően hány napig aktuális*
- *a CRL a következő kibocsátást követő hány napig aktuális*
- *CRL frissesség ellenőrzés engedélyezése*
- *visszavonás ellenőrzés kihagyhatóság engedélyezése*
- *megbízható időszerverek*
- *szolgáltatás igénybevétele utáni kényszerített kijelentkeztetés engedélyezése*
- *OCSP válasz az előállítást követő hány percig aktuális*
- *OCSP válasz a kibocsátást követő hány percig aktuális*
- *OCSP válasz a következő kibocsátást követő hány percig aktuális*
- *OCSP válasz frissesség ellenőrzés engedélyezése*
- *időbélyeg szolgáltatás elérhetősége*

- *OCSP szolgáltatás elérhetősége*
- *szervezeti aláírási szabályzat*

e) tanúsítási útvonal érvényesítés
f) CRL érvényesítés
g) elektronikus aláírás létrehozása és ellenőrzése
h) *titkosítás és visszafejtés*
i) *időbélyeg kérés és ellenőrzés*
j) *OCSP kérés és ellenőrzés*

Függőség: Nincs

FMT_SMR.2 Biztonsági szerepkörök szigorításai

Hierarchikus kapcsolat: FMT_SMR.1 Biztonsági szerepkörök.

FMT_SMR.2.1 A TSF-nek karban kell tartania a következő szerepeket***: felhasználó nevében végrehajtott folyamat.***

FMT_SMR.2.2 A TSF-nek képesnek kell lennie felhasználók és szerepek összerendelésére.

FMT_SMR.2.3 A TSF-nek biztosítania kell, hogy *a felhasználó nevében végrehajtott folyamatok feltételei* ki legyenek elégítve.

Függőség: FIA_UID.1 Azonosítás időzítése

5.1.1.4 A TOE biztonsági funkcióinak védelme (FPT)

FPT_RVM.1 A TSP kikerülhetetlensége

Hierarchikus kapcsolat: nincs más komponenshez.

FPT_RVM.1.1 TSF-nek biztosítania kell, hogy a TSP-t érvényre juttató funkciói meghívásra kerülnek és sikeresen végrehajtódnak, mielőtt minden egyes **TSF irányítási tárgykör (TSC)** funkció továbbhaladása engedélyeződne.

Függőség: Nincs

FPT_SEP.1 TSF körzetszétválasztás

Hierarchikus kapcsolat: nincs más komponenshez.

FPT_SEP.1.1 A TSF-nek fenn kell tartania a saját végrehajtása számára egy biztonsági körzetet, amely védelmet nyújt a nem megbízható szubjektumok általi beavatkozás és meghamisítás ellen.

FPT_SEP.1.2 A TSF-nek érvényesítenie kell a TSC szubjektumainak biztonsági körzeteinek egymástól való elkülönítését.

Függőség: Nincs

5.1.1.5 Funkció szilárdsági követelmény

A TOE hitelesítési funkció szilárdsága SOF-alap ként van feltételezve. Ez a SOF szint alacsony támadási képességet jelent. A kriptográfiai algoritmusok erőssége a CC tárgykörén kívül esik. A funkció szilárdságok csak a nem kriptográfiai, valószínűségi és felcserélési mechanizmusokra vonatkoznak. A SOF követelmény a TOE-én belül az azonosítási és hitelesítési funkciókra vonatkoznak.

5.1.2 A TOE csomagok biztonsági funkcionális követelményei

A következő alfejezetek a TOE biztonsági alapkövetelményeket kiegészítően, az egyes csomagok biztonsági funkcionális követelményeit írja le. Az alábbi táblázat csomagonként összegzi a funkcionális követelményeket és a csomag függéseket.

26. táblázat: A csomagok funkcionális követelményeinek összegzése

Csomagnév	Funkcionális követelmények	Függések
Tanúsítási útvonal érvényesítése (CPV) - Alap	FDP_CPD.1	Tanúsítvány visszavonási lista (CRL) érvényesítés
	FDP_DAU_CPV_INI.1	
	FDP_DAU_CPV_CER.1	
	FDP_DAU_CPV_CER.2	
	FDP_DAU_CPV_OUT.1	
PKI aláírás készítés	FDP_ETC_SIG.1	Nincs
PKI aláírás ellenőrzés	FDP_ITC_SIG.1	Tanúsítási útvonal érvényesítése (CPV) - Alap
	FDP_DAU_SIG.1	
PKI titkosítás kulcs átviteli algoritmusokkal	FDP_ETC_ENC.1	Tanúsítási útvonal érvényesítése (CPV) - Alap
	FDP_DAU_ENC.1	
PKI visszafejtés kulcs átviteli algoritmusokkal	FDP_ITC_ENC.1	Nincs
Tanúsítvány visszavonási lista (CRL) érvényesítés	FDP_DAU_CRL.1	Nincs
Időbélyeg kliens	FDP_DAU_TSP.1	Tanúsítási útvonal érvényesítése (CPV) - Alap
Valós idejű tanúsítvány állapot protokoll (OCSP) kliens	FDP_DAU_OCS.1	Tanúsítási útvonal érvényesítése (CPV) - Alap

5.1.2.1 Tanúsítási útvonal érvényesítése (CPV) - Alap csomag

Ennek a csomagnak a funkciója a tanúsítás útvonal érvényesítése. A tanúsítási útvonal felépítése szintén része a csomagnak. Az érvényesítés lépései: a tanúsítási útvonal felépítése, majd a tanúsítási útvonal ellenőrzése. Az ellenőrzés a megbízható legfelső szintű hitelesítő tanúsítvány vizsgálatával kezdődik, a közbenső tanúsítványok vizsgálatával folytatódik és végül az aláírói tanúsítvány (végtanúsítvány) vizsgálatával fejeződik be. Minden folyamat az X.509 és PKIX szabványoknak megfelelő.

A nyilvános kulcsú tanúsítványok három típusa:

- Megbízható legfelső szintű hitelesítő tanúsítvány: önaláírt tanúsítvány, amely nem igényel semmilyen érvényesítést. A megbízható legfelső szintű tanúsítvány elsődleges célja, hogy rendelkezésre álljon a Distinguished Name (DN), nyilvános kulcs, algoritmus azonosító és a nyilvános kulcs paraméterei. A csomag megengedi a megbízható legfelső szintű tanúsítvány érvényesítését, vagyis az aláírás ellenőrzését és az érvényességi időszak lejáratának ellenőrzését.
- Közbenső tanúsítványok: ezek a CA számára kiadott tanúsítványok. Minden tanúsítvány a tanúsítási útvonalban közbenső tanúsítvány, az utolsó kivételével.
- Végtanúsítvány: ez a tanúsítási útvonalban az utolsó tanúsítvány. Ez tipikusan vég entitás (nem CA) tanúsítvány, azonban a csomag megengedi azt is, hogy a végtanúsítvány CA tanúsítvány legyen.

A csomag a következő biztonsággal összefüggő tanúsítvány kiterjesztés ellenőrzéseket végzi: nocheck, keyUsage, extendedKeyUsage, és basicConstraints.

A csomag feltételezi, hogy az érvényesítési útvonal ellenőrzése az aktuális időpontban történik. Mivel visszavonás ellenőrzése elő van írva, ez a csomag függ a Tanúsítvány visszavonási lista (CRL) érvényesítés csomagtól.

5.1.2.1.1 Felhasználói adat védelem (FDP osztály)

FDP_CPD.1 Tanúsítási útvonal felépítése

Hierarchikus kapcsolat: nincs más komponenshez.

FDP_CPD.1.1 A TSF-nek az érvényesítési útvonalat a *felhasználó nevében végrehajtott folyamat* által szolgáltatott megbízható legfelső szintű hitelesítő tanúsítvánnyal kezdve a végtanúsítványig kell felépítenie, a következő tanúsítvány mezők vagy kiterjesztések egyezőségi szabályait alkalmazva: *distinguished name*.

FDP_CPD.1.2 A TSF-nek a tanúsítási útvonalat a következő kiegészítő egyezőségi szabályok alkalmazásával kell felépítenie:

a) aláírás ellenőrzése esetén:
aa) ha aláírási szabályzat nincs érvényben, akkor a keyUsage kiterjesztésben a nonRepudiation bit be van állítva
ab) ha aláírási szabályzat érvényben van, akkor annak rendelkezéseitől függően: a keyUsage kiterjesztésben a nonRepudiation vagy digitalSignature bit be van állítva
b) a keyUsage kiterjesztésben a digitalSignature bit be van állítva, entitás hitelesítése esetén
c) *a keyUsage kiterjesztésben a keyEncipherment bit be van állítva, titkosítás, visszafejtés esetén*

FDP_CPD.1.3 A TSF-nek a tanúsítási útvonalat a következő kiegészítő egyezőségi szabályok alkalmazásával kell felépítenie:

a) *nincs további szabály az extendedKeyUsage kiterjesztés tartalmára*

FDP_CPD.1.4 A TSF kikerülhet bármely egyezőségi szabályt, kivéve:

a) distinguished name
b) *a tanúsítvány formátuma X.509*

amennyiben további tanúsítási útvonalak szükségesek.

Függőség: Nincs

FDP_DAU_CPV_INI.1 Tanúsítási útvonal inicializálása -- alap

Hierarchikus kapcsolat: nincs más komponenshez.

FDP_DAU_CPV_INI.1.1 A TSF-nek a *felhasználó nevében végrehajtott folyamat* által szolgáltatott megbízható legfelső szintű hitelesítő tanúsítványt kell használnia.

FDP_DAU_CPV_INI.1.2 A TSF-nek a *felhasználó nevében végrehajtott folyamat által meghatározott időszerverektől vagy ha az nem áll rendelkezésre, akkor a lokális környezetből,* mint megbízható forrásból kell megszereznie az aktuális időt, amelyet 'current-time'-nak nevezünk.

FDP_DAU_CPV_INI.1.3 A TSF-nek a megbízható legfelső szintű tanúsítványok esetében a következő ellenőrzéseket kell elvégeznie:

a) *Subject DN és az Issuer DN egyezik*
b) *A tanúsítványon az aláírás érvényes, a megbízható legfelső szintű hitelesítő tanúsítvány alanyának nyilvános kulcsával és annak paraméterével (ha az rendelkezésre áll) ellenőrizve*
c) *a megbízható legfelső szintű tanúsítvány notBefore mezője <= current-time*
d) *a megbízható legfelső szintű tanúsítvány notAfter mezője => current-time*

FDP_DAU_CPV_INI.1.4 A TSF-nek a megbízható legfelső szintű hitelesítő tanúsítványból származtatnia kell a következő információkat: *subject DN, subject public key, subject public key algorithm object identifier, subject public key paraméterek.*

Függőség: FCS_COP.1 Kriptográfiai működés
FPT_STM.1 Megbízható időpont

FDP_DAU_CPV_CER.1 Tanúsítvány feldolgozás -- alap

Hierarchikus kapcsolat: nincs más komponenshez.

FDP_DAU_CPV_CER.1.1 A TSF-nek a tanúsítványt csak akkor szabad elfogadnia, ha a következő ellenőrzések sikeresen megtörténtek:

a) A tanúsítványon az aláírás ellenőrzése a következőekkel: parent-public-key, parent-public-key-algorithm-identifier, és parent-public-key-parameters
b) A tanúsítvány notBefore mezője < = current-time
c) A tanúsítvány notAfter mezője > = current-time
d) A tanúsítvány issuer mezője = parent-DN
e) A TSF képes a tanúsítvány minden kritikus kiterjesztését feldolgozni.

FDP_DAU_CPV_CER.1.2 A TSF kikerülheti a visszavonási állapot ellenőrzését, ha a tanúsítvány tartalmazza a no-check kiterjesztést.

FDP_DAU_CPV_CER.1.3 A TSF ki kell hagynia a visszavonás ellenőrzését, ha a visszavonási információ nem áll rendelkezésre és *a felhasználó nevében végrehajtott folyamat* felülbírálja a visszavonás ellenőrzést.

FDP_DAU_CPV_CER.1.4 A TSF-nek el kell fogadnia a tanúsítványt, ha a visszavonási állapot *CRL ellenőrzés vagy OCSP ellenőrzés* alapján, meggyőződött arról, hogy a tanúsítvány nincs visszavonva.

FDP_DAU_CPV_CER.1.5 A TSF-nek nyilvános kulcs paraméterei állapotgépet a következő szabályok szerint kell vezérelnie:

a) a paraméter megállapítása a tanúsítvány subjectPublickeyInfo mezőjéből, ha abban szerepel a paraméter, különben
b) az eredeti paraméter állapot megtartása, ha az aktuális tanúsítvány nyilvános kulcsának algoritmusa és a kibocsátó nyilvános kulcsának algoritmusa azonos algoritmus családba

tartozik, különben
c) a paramétert be kell állítani „null” értékre

Függőség: FCS_COP.1 Kriptográfiai működés
FPT_STM.1 Megbízható időpont

FDP_DAU_CPV_CER.2 Közbenső tanúsítvány feldolgozás -- alap

Hierarchikus kapcsolat: nincs más komponenshez.

FDP_DAU_CPV_CER.2.1 A TSF-nek a közbenső tanúsítványt csak akkor kell elfogadnia, ha a következő ellenőrzések sikeresen megtörténtek:
a) basicConstraints kiterjesztés jelen van, és abban a cA = TRUE
b) pathLenConstraint kényszer teljesül
c) ha kritikus keyUsage kiterjesztés jelen van, akkor abban a keyCertSign bit be van állítva

Függőség: FDP_DAU_CPV_CER.1 Tanúsítvány feldolgozás -- alap

FDP_DAU_CPV_OUT.1 Tanúsítási útvonal kimenete -- alap

Hierarchikus kapcsolat: nincs más komponenshez.

FDP_DAU_CPV_OUT.1.1 A TSF-nek tanúsítási útvonal érvényesítési hibát kell visszaadnia, ha a tanúsítási útvonalban bármely tanúsítvány visszautasításra került.

FDP_DAU_CPV_OUT.1.2 A végtanúsítványból a TSF-nek a következő változókat kell visszaadnia: subject DN, subject public key algorithm identifier, subject public key, kritikus keyUsage kiterjesztés.

FDP_DAU_CPV_OUT.1.3 A végtanúsítványból a TSF-nek a következő további változókat kell visszaadnia: *tanúsítvány*, *subject alternative names, tanúsítvány lánc, extendedKeyUsage*.

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

Függőség: Nincs.

5.1.2.2 PKI aláírás készítés csomag

A PKI aláírás készítés csomag magánkulcsot használ az aláírás létrehozására és az aláírási információ előállításának képességéről gondoskodik.

5.1.2.2.1 Felhasználói adat védelem (FDP osztály)

FDP_ETC_SIG.1 PKI aláírás exportálás

Hierarchikus kapcsolat: nincs más komponenshez.

FDP_ETC_SIG.1.1 A TSF-nek a magánkulcs felhasználásával elektronikus aláírást kell létrehozni.

FDP_ETC_SIG.1.2 *A TSF-nek az elektronikus aláírásba a következő aláírást kísérő információkat kell befoglalnia:*

1)A1-kombatibilis elektronikus aláírás készítése esetén:

a)kötelezően: hash algoritmus, aláírási algoritmus, aláíró nyilvános kulcs, aláíró DN, aláíró tanúsítványt kibocsátó DN, aláíró tanúsítványának sorozatszáma, aláíró tanúsítványa, aláíró tanúsítványának az érvényesített tanúsítási útvonala, aláírás időpontja

b)opcionálisan: aláírás helye(város), aláírás helye(irányítószám), aláírás helye(megye), aláírás helye(ország), aláíró szerepkör

2)A2 elektronikus aláírás készítése esetén:

a)„Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára (2005. november 22.)” választása esetén:

aa)kötelezően:

- *kanonizálási módszer (CanonicalizationMethod), a http://www.w3.org/TR/2001/REC-xml-c14n-20010315 értékkel*
- *aláírási algoritmus (SignatureMethod) az RSAwithSHA1 értékkel*
- *aláírt dokumentumok külső vagy belső hivatkozásai (Reference)*
- *transzformációk (Transforms) az http://www.w3.org/TR/2001/REC-xml-c14n-20010315 vagy http://www.w3.org/2000/09/xmldsig#BASE64 értékkel*
- *lenyomatképző algoritmus (DigestMethod) az SHA1 értékkel*
- *az aláíró tanúsítványa (KeyInfo)*
- *aláírás időpontja (SigningTime)*
- *hivatkozás az aláíró tanúsítványára (SigningCertificate)*
- *aláírási szabályzat (SignaturePolicyIdentifier)*
- *aláírt dokumentumok adatformátum leírásai (DataObjectFormat)*

ab)opcionálisan:

- *az aláíró nyilvános kulcsa (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)*
- *aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)*
- *aláíró szerepkörei (SignerRole)*
- *kötelezettségvállalás jelzése (CommitmentTypeIndication)*

- *aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)*
- *ellenjegyző aláírás (CounterSignature)*
- *aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)*
- *aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)*
- *referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)*
- *archív időbélyeg(ek) (ArchiveTimeStamp)*

b)v1.2.2 vagy v1.3.2 szabványos formátum választása esetén:
ba)kötelezően:

- *kanonizálási módszer (CanonicalizationMethod)*
  http://www.w3.org/TR/2001/REC-xml-c14n-20010315,
  http://www.w3.org/TR/2001/REC-xml-c14n-0010315#WithComments,
  http://www.w3.org/TR/2001/REC-xml-c14n-20010315,
  http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments,
  http://www.w3.org/2006/12/xml-c14n11,
  http://www.w3.org/2006/12/xml-c14n11#WithComments
- *aláírási algoritmus (SignatureMethod) RSAwithSHA1, RSAwithSHA256, RSAwithSHA384, RSAwithSHA512 vagy DSAwithSHA1*
- *aláírt dokumentumok külső vagy belső hivatkozásai (Reference)*
- *transzformációk (Transforms)*
- *lenyomatképző algoritmus (DigestMethod)*
- *az aláíró tanúsítványa (KeyInfo)*
- *aláírás időpontja (SigningTime)*
- *hivatkozás az aláíró tanúsítványára (SigningCertificate)*

bb)opcionálisan:

- *az aláíró nyilvános kulcsa (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)*
- *aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)*
- *aláíró szerepkörei (SignerRole)*
- *aláírási szabályzat (SignaturePolicyIdentifier)*
- *aláírt dokumentumok adatformátum leírásai (DataObjectFormat*
- *kötelezettségvállalás jelzése (CommitmentTypeIndication)*
- *aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy*

IndividualDataObjectsTimeStamp)
- *ellenjegyző aláírás (CounterSignature)*
- *aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)*
- *aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)*
- *referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)*
- *archív időbélyeg(ek) (ArchiveTimeStamp)*

c)„Egységes MELASZ formátum elektronikus aláírásokra” v2.0 választása esetén:
ca)kötelezően:
- *kanonizálási módszer (CanonicalizationMethod), a http://www.w3.org/TR/2001/REC-xml-c14n-20010315 értékkel*
- *aláírási algoritmus (SignatureMethod) az RSAwithSHA1 vagy RSAwithSHA256 értékkel*
- *aláírt dokumentumok külső vagy belső hivatkozásai (Reference)*
- *transzformációk (Transforms) az http://www.w3.org/TR/2001/REC-xml-c14n-20010315 vagy http://www.w3.org/2000/09/xmldsig#BASE64 értékkel*
- *lenyomatképző algoritmus (DigestMethod) az SHA1 vagy SHA256 értékkel*
- *az aláíró tanúsítványa (KeyInfo)*
- *aláírás időpontja (SigningTime)*
- *hivatkozás az aláíró tanúsítványára (SigningCertificate)*
- *aláírási szabályzat (SignaturePolicyIdentifier)*
- *aláírt dokumentumok adatformátum leírásai (DataObjectFormat)*

cb)opcionálisan:
- *az aláíró nyilvános kulcsa (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)*
- *aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)*
- *aláíró szerepkörei (SignerRole)*
- *kötelezettségvállalás jelzése (CommitmentTypeIndication)*
- *aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)*
- *ellenjegyző aláírás (CounterSignature)*

- *aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)*
- *aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)*
- *referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)*
- *archív időbélyeg(ek) (ArchiveTimeStamp)*

Függőség: FCS_COP.1 Kriptográfiai működés

5.1.2.3 PKI aláírás ellenőrzés csomag

A PKI aláírás ellenőrzési csomag feldolgozza az aláírási információkat és a nyilvános kulcsot használja az aláírás ellenőrzéséhez. Ez a csomag a Tanúsítási útvonal érvényesítése (CPV) - Alap csomagtól függ. A aláírás ellenőrzési csomag a Tanúsítási útvonal érvényesítése (CPV) - Alap csomag adatait használja inputként.

5.1.2.3.1 Felhasználói adat védelem (FDP osztály)

FDP_ITC_SIG.1 PKI aláírás importálása

Hierarchikus kapcsolat: nincs más komponenshez.

FDP_ITC_SIG.1.1 *A TSF-nek az alábbi aláírást kísérő információkat kell használnia az aláírás ellenőrzése során:*

1)A1-kombatibilis elektronikus aláírás ellenőrzése esetén:

a)kötelezően: hash algoritmus, aláírási algoritmus, aláíró nyilvános kulcs, aláíró DN, aláíró tanúsítványt kibocsátó DN, aláíró tanúsítványának sorozatszáma, aláíró tanúsítványa, aláíró tanúsítványának az érvényesített tanúsítási útvonala, aláírás időpontja

b)opcionálisan: aláírás helye(város), aláírás helye(irányítószám), aláírás helye(megye), aláírás helye(ország), aláíró szerepkör

2)A2 elektronikus aláírás ellenőrzés esetén:

a)„Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára (2005. november 22.)” formátumnak vagy az „Egységes MELASZ formátum elektronikus aláírásokra” v2.0 dokumentumnak megfelelő aláírás ellenőrzése esetén:

aa) kötelezően:

- *kanonizálási módszer (CanonicalizationMethod)*
- *aláírási algoritmus (SignatureMethod)*
- *aláírt dokumentumok külső vagy belső hivatkozásai (Reference)*
- *transzformációk (Transforms)*
- *lenyomatképző algoritmus (DigestMethod)*
- *az aláíró tanúsítványa (KeyInfo)*
- *aláírás időpontja (SigningTime)*
- *hivatkozás az aláíró tanúsítványára (SigningCertificate)*
- *aláírási szabályzat (SignaturePolicyIdentifier)*
- *aláírt dokumentumok adatformátum leírásai (DataObjectFormat)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)*

ab) opcionálisan:

- *az aláíró nyilvános kulcsa (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)*
- *aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)*
- *aláíró szerepkörei (SignerRole)*
- *kötelezettségvállalás jelzése (CommitmentTypeIndication)*
- *aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)*
- *ellenjegyző aláírás (CounterSignature)*
- *aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)*
- *aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)*
- *referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)*
- *archív időbélyeg(ek) (ArchiveTimeStamp)*

b) v1.2.2 vagy v1.3.2 szabványos formátumnak megfelelő aláírás ellenőrzése esetén:

ba) kötelezően:

- *kanonizálási módszer (CanonicalizationMethod)*
- *aláírási algoritmus (SignatureMethod)*
- *aláírt dokumentumok külső vagy belső hivatkozásai (Reference)*
- *transzformációk (Transforms)*
- *lenyomatképző algoritmus (DigestMethod)*
- *az aláíró tanúsítványa (KeyInfo)*

- *aláírás időpontja (SigningTime)*
- *hivatkozás az aláíró tanúsítványára (SigningCertificate)*

bb) opcionálisan:

- *az aláíró nyilvános kulcsa (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)*
- *aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)*
- *aláíró szerepkörei (SignerRole)*
- *aláírási szabályzat (SignaturePolicyIdentifier)*
- *aláírt dokumentumok adatformátum leírásai (DataObjectFormat*
- *kötelezettségvállalás jelzése (CommitmentTypeIndication)*
- *aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)*
- *ellenjegyző aláírás (CounterSignature)*
- *aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)*
- *aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)*
- *referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)*
- *archív időbélyeg(ek) (ArchiveTimeStamp)*

Függőség: Nincs

FDP_DAU_SIG.1 Aláírás bináris ellenőrzése

Hierarchikus kapcsolat: nincs más komponenshez.

FDP_DAU_SIG.1.1 A TSF-nek a Tanúsítási útvonal érvényesítése (CPV) - Alap csomagból a következő információkat kell használnia: subject public key algorithm, subject public key, subject public key parameters, amikor az aláírt adaton az elektronikus aláírást ellenőrzi.

FDP_DAU_SIG.1.2 A TSF-nek ellenőriznie kell, hogy a Tanúsítási útvonal érvényesítése (CPV) - Alap csomag által visszaadott keyUsage kiterjesztésben a nonRepudiation bit **vagy a digitalSignature bit** be van állítva.

FDP_DAU_SIG.1.3 A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie:

a) *Tanúsítási útvonal érvényesítése (CPV) - Alap csomag által visszaadott subject DN egyezik az aláírási információkkal.*

b) a tanúsítvány keyUsage kiterjesztésében:
ba) ha aláírási szabályzat nincs érvényben, akkor kizárólag csak a nonRepudiation bit van beállítva
bb) ha aláírási szabályzat van érvényben, akkor annak rendelkezésétől függően az alábbiak valamelyike:
- kizárólag csak a nonRepudiation bit van beállítva
- kizárólag csak a digitalSignature bit van beállítva
- a nonRepudiation bit van beállítva, a többi bit nem számít
- a digitalSignature bit van beállítva, a többi bit nem számít

c) *szigorú üzemmódban a minősített elektronikus aláírás esetén az aláíró tanúsítványában a kötelező qcStatements kiterjesztésben az id-etsi-qcs-QcCompliance OID meglétének ellenőrzése*

Függőség: FCS_COP.1 Kriptográfiai működés
FDP_DAU_CPV_OUT.1 Tanúsítási útvonal kimenete -- alap

5.1.2.4 PKI titkosítás kulcs átviteli algoritmusokkal csomag

Ez a csomag támogatja a nyilvános kulcsú titkosítást kulcsátviteli algoritmusokkal (pl. RSA). Tanúsítási útvonal érvényesítést használ arra, hogy a visszafejtő félnek a megfelelő nyilvános kulcsa legyen használva. Ez a csomag függ a Tanúsítási útvonal érvényesítési (CPV) - Alap csomagtól.

5.1.2.4.1 Felhasználói adat védelem (FDP osztály)

FDP_ETC_ENC.1 PKI titkosítás exportja – Kulcs átvitel algoritmusok

Hierarchikus kapcsolat: nincs más komponenshez.

FDP_ETC_ENC.1.1 A TSF-nek a következő információkat kell a titkosított adattal együtt biztosítania:

a) visszafejtő (címzett) nyilvános kulcsú tanúsítványa
b) titkosítás időpontja
c) fájl név vagy annak megfelelője
d) titkosítatlan tartalomra képzett lenyomat
e) a címzett részére aszimmetrikus titkosítással csomagolt titkos kulcs

FDP_ETC_ENC.1.2 A TSF-nek a Tanúsítási útvonal érvényesítése (CPV) - Alap csomagból a következő információkat kell használnia a titkosított adat létrehozásakor: subject public key algorithm, subject public key, subject public key paraméterek.

Függőség: FCS_COP.1 Kriptográfiai működés
FDP_DAU_CPV_OUT.1 Érvényesítési útvonal kimenete -- alap

FDP_DAU_ENC.1 PKI titkosítás ellenőrzése – Kulcs átvitel algoritmusok

Hierarchikus kapcsolat: nincs más komponenshez.

FDP_DAU_ENC.1.1 A TSF-nel ellenőriznie kell, hogy a Tanúsítási útvonal érvényesítése (CPV) - Alap csomagból visszaadott keyUsage kiterjesztésben a keyEncipherment bit be van állítva.

FDP_DAU_ENC.1.2 A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie:
a) a visszafejtett tartalomra képzett lenyomat megegyezik-e az eredeti lenyomattal

Függőség: FDP_DAU_CPV_OUT.1 Érvényesítési útvonal kimenete -- alap

5.1.2.5 PKI visszafejtés kulcs átviteli algoritmusokkal csomag

Ez a csomag támogatja a nyilvános kulcsú titkosítás kulcsátviteli algoritmusokkal (pl. RSA) visszafejtését. Mivel a visszafejtéshez csak a a visszafejtő fél magánkulcsát használja, tanúsítási útvonal ellenőrzést nem használ. Ez a csomag nem függ a Tanúsítási útvonal érvényesítése útvonal (CPV- alap) csomagtól.

5.1.2.5.1 Felhasználói adat védelem (FDP osztály)

FDP_ITC_ENC.1 PKI titkosítás importja – Kulcs átviteli algoritmusok

Hierarchikus kapcsolat: nincs más komponenshez.

FDP_ITC_ENC.1.1 A TSF-nek a titkosított adatról a következő információkat kell használnia:
a) visszafejtő (címzett) nyilvános kulcsú tanúsítványa
b) titkosítás időpontja
c) fájl név vagy annak megfelelője
d) titkosítatlan tartalomra képzett lenyomat
e) a címzett részére aszimmetrikus titkosítással csomagolt titkos kulcs

FDP_ITC_ENC.1.2 A TSF-nek el kell végeznie a visszafejtést.

Függőség: FCS_COP.1 Kriptográfiai működés

5.1.2.6 Tanúsítvány visszavonási lista (CRL) érvényesítés csomag

Ez a csomag a CRL érvényesítésére van használva. A csomag nem írja elő a CRL issuingDistributionPoint (IDP) CRL kiterjesztés kezelését, valamint delta CRL-ek feldolgozását. A csomag lehetővé teszi olyan CRL feldolgozását, amelyre valamely tanúsítvány crlDistributionPoint (CRLDP) kiterjesztése mutat, abban az esetben, ha a hivatkozott CRL egy teljes CRL, amelyet az IDP és a deltaCRLIndicator CRL kiterjesztések hiánya jelez.

A csomag megengedi, de nem teszi kötelezővé, hogy a CRL aláírásának ellenőrzése és a tanúsítvány aláírásának ellenőrzéséhez ugyanazon nyilvános kulcs legyen használva. Más szóval az alkalmazás egyaránt használhatja az említett nyilvános kulcsot, vagy felépíthet tanúsítási útvonalat.

5.1.2.6.1 Felhasználói adat védelem (FDP osztály)

FDP_DAU_CRL.1 Alap CRL ellenőrzés

Hierarchikus kapcsolat: nincs más komponenshez.

FDP_DAU_CRL.1.1 A TSF-nek a CRL-t a következő forrásokból kell beszereznie:a *felhasználó nevében végrehajtott folyamat által szolgáltatott tároló, a kérdéses tanúsítvány CRLDistributionPoints kiterjesztése által mutatott cím.*

FDP_DAU_CRL.1.2 A TSF-nek meg kell szereznie a CRL kibocsátójáról a következő adatokat: megbízható nyilvános kulcs, algoritmus, és a nyilvános kulcs paraméterei.

FDP_DAU_CRL.1.3 A TSF-nek a CRL aláírását a következőekkel kell ellenőriznie: a CRL kibocsátójának a megbízható nyilvános kulcsa, algoritmusa, és nyilvános kulcsának paraméterei.

FDP_DAU_CRL.1.4 A TSF-nek ellenőriznie kell, hogy a CRL-t kibocsátó tanúsítványában a kritikus keyUsage kiterjesztés jelen legyen és abban a cRLSign bit be legyen állítva.

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

FDP_DAU_CRL.1.6 A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha *thisUpdate mező értékére nézve* a következő szabályzat érvényesül: *current-time <= thisUpdate + x, ahol az x a felhasználó nevében végrehajtott folyamat által megadott érték.*

FDP_DAU_CRL.1.7 A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha *nextUpdate mező értékére nézve* a következő szabályzat érvényesül: *current-time <= nextUpdate + x, ahol az x a felhasználó nevében végrehajtott folyamat által megadott érték.*

FDP_DAU_CRL.1.8 A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha a *felhasználó nevében végrehajtott folyamat* felülbírálja a frissesség ellenőrzését.

FDP_DAU_CRL.1.9 A TSF-nek vissza kell utasítania a CRL-t, ha az olyan kritikus kiterjesztést tartalmaz, amelyet a TSF nem dolgoz fel.

FDP_DAU_CRL.1.10 A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie:
a) a CRL formátuma X.509

Függőség: FCS_COP.1 Kriptográfiai működés
FPT_STM.1 Megbízható időpont

5.1.2.7 Időbélyeg kliens csomag

Ez a csomag az Időbélyeg kliens kéréseket és az időbélyeg válaszok ellenőrzését teszi lehetővé. Az időbélyeg válaszadó, mint megbízható legfelső szintű hitelesítés szolgáltató, egy TSA, mint időbélyeg válasz aláírására jogosult végentitás. Az Időbélyeg kliens csomag a tanúsítási útvonal érvényességének ellenőrzésével bírálja el az időbélyeg aláírására szóló jogosultságot. Ez a csomag így függ a Tanúsítási útvonal érvényesítése (CPV) - Alap csomagtól.

5.1.2.7.1 Felhasználói adat védelem (FDP osztály)

FDP_DAU_TSP.1 Alap időbélyeg ellenőrzés

Hierarchikus kapcsolat: nincs más komponenshez.

FDP_DAU_TSP.1.1 A TSF-nek a PKIX RFC 3161-nek megfelelő formában kell összeállítania az időbélyeg kérést.

FDP_DAU_TSP.1.2 Az időbélyeg kérésnek a következő adatokat kell tartalmaznia
a) kötelezően: verzió, messageImprint, nonce, certReq true értékkel,
b) opcionálisan: reqPolicy, extensions.

FDP_DAU_TSP.1.3 A TSF-nek ellenőriznie kell, hogy a kapott időbélyeg válasz formátuma az PKIX RFC 3161-nek megfelelő.

FDP_DAU_TSP.1.4 A TSF-nek az időbélyeg válaszban a következő alap ellenőrzéseket kell elvégeznie:
a) ha a státusz nem granted vagy grantedWithMods, akkor nem szerepelhet a válaszban TimeStampToken
b) ha a státusz nem granted vagy grantedWithMods, akkor a válaszban szerepelnie kell PKIFailureInfo hiba információnak
c) ha a státusz granted vagy grantedWithMods, akkor a válaszban szerepelnie kell TimeStampToken objektumnak
d) ha a státusz granted vagy grantedWithMods, akkor a válaszban kapott TimeStampToken tartalom típusa pkcs7-signedData kell, hogy legyen
e) ha a státusz granted vagy grantedWithMods, akkor a válaszban kapott SignedData tartalom típusa id-ct-TSPInfo kell, hogy legyen

FDP_DAU_TSP.1.5 A TSF-nek az időbélyeget aláíró tanúsítványt az időbélyeg válaszból kell megismernie.

FDP_DAU_TSP.1.6 A TSF-nek a TSA megbízhatóságának megállapítására tanúsítási útvonal érvényesség ellenőrzést kell végrehajtania a Tanúsítási útvonal érvényesítése (CPV) - Alap csomag felhasználásával.

FDP_DAU_TSP.1.7 A TSF-nek ellenőriznie kell az időbélyeg válasz aláírását a Tanúsítási útvonal érvényesítése (CPV) - Alap csomag kimenetéből származó nyilvános kulccsal.

FDP_DAU_TSP.1.8 A TSF-nek ellenőriznie kell, hogy ha az időbélyeget aláíró tanúsítvány tartalmazza az extendedKeyUsage kiterjesztést, akkor a kiterjesztés tartalmazza-e a PKIX OID-t időbélyeg aláírásra (id-kp-timeStamping).

FDP_DAU_TSP.1.9 A TSF-nek az időbélyeg válaszban a további ellenőrzéseket kell elvégeznie:
a) messageImprint azonosságát az időbélyeg kérés messageImprint értékkel
b) nonce azonosságát az időbélyeg kérés nonce értékkel
c) ha a kérés tartalmazott TSAPolicyId-t, akkor az azonos-e a válaszban kapott TSAPolicyId értékkel

FDP_DAU_TSP.1.10 A TSF-nek el kell utasítania az időbélyeg választ, ha a válasz olyan kritikus kiterjesztést tartalmaz, amelyet a TSF nem képes feldolgozni.

FDP_DAU_TSP.1.11 A TSF-nek az időbélyeg kérést abban az időpontban kell intéznie, amelyet a felhasználó nevében végrehajtott folyamat beállított.

FDP_DAU_TSP.1.12 A TSF-nek, amennyiben az aláírás formátuma XAdES v1.3.2 vagy „Egységes MELASZ formátum elektronikus aláírásokra” v2.0, az aláírásban az időbélyeg válaszból (TimeStampResp) kiemelt időbélyeg tokot (TimeStampToken) kell elhelyeznie. A TSF-nek, az ellenőrzés alatt álló aláírásban, amennyiben annak formátuma XAdES v1.3.2-nek vagy „Egységes MELASZ formátum elektronikus aláírásokra” v2.0-nak megfelelő, időbélyeg válasz helyett időbélyeg tokot kell elvárnia. Amennyiben az időbélyeg tok formátuma az RFC 3161-nek megfelelő, a TSF-nek fel kell tételeznie, hogy az időbélyeg tok egy olyan időbélyeg válaszból származik, amelyben a státusz granted.

Függőség: FCS_COP.1

5.1.2.8 Valós idejű tanúsítvány állapot protokoll (OCSP) kliens

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

5.1.2.8.1 Felhasználói adat védelem (FDP osztály)

FDP_DAU_OCS.1 Alap OCSP ellenőrzés

Hierarchikus kapcsolat: nincs más komponenshez.

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

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

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

FDP_DAU_OCS.1.4 A TSF-nek a következő további funkciókat kell végrehajtania: *az OCSP válaszadó megbízhatóságának megállapítása a Tanúsítási*

útvonal érvényesítése (CPV) - Alap csomag felhasználásával.

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

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

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

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

FDP_DAU_OCS.1.9 A TSF-nek aktuálisnak kell elfogadnia az OCSP választ minden bejegyzés tekintetében, ha az alábbi szabályzat érvényesül:
current-time <= producedAt + x, ahol x a felhasználó nevében végrehajtott folyamat által megadott érték

FDP_DAU_OCS.1.10 A TSF-nek aktuálisnak kell elfogadnia az OCSP választ egy bejegyzés tekintetében, ha az alábbi szabályzat érvényesül:
current-time <= thisUpdate a bejegyzésből + x, ahol a x a felhasználó nevében végrehajtott folyamat által megadott érték.

FDP_DAU_OCS.1.11 A TSF-nek aktuálisnak kell elfogadnia az OCSP választ egy bejegyzés tekintetében, ha az alábbi szabályzat érvényesül:
current-time <= nextUpdate a bejegyzésből + x, ahol a x a felhasználó nevében végrehajtott folyamat által megadott érték.

FDP_DAU_OCS.1.12 A TSF-nek az OCSP választ aktuálisnak kell elfogadni, ha a *felhasználó nevében végrehajtott folyamat* felülbírálja a frissesség ellenőrzését.

FDP_DAU_OCS.1.13 A TSF-nek vissza kell utasítania az OCSP választ, ha az olyan kritikus kiterjesztést tartalmaz, amelyet a TSF nem dolgoz fel.

FDP_DAU_OCS.1.14 A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie:
nonce a kérésből = nonce a válaszból

Függőség: FCS_COP.1, FTP_STM.1

5.1.3 A TOE biztonsági garanciális követelményei

Jelen ST az EAL 3+kibővített garancia szintet valósít meg, kiegészítve az ALC_FLR.1 osztállyal.

27. táblázat: EAL 3+ kibővítés garanciális követelményei

Garancia osztály azonosítója	Garancia osztály megnevezése
ACM_CAP.3	Jogosultság ellenőrzések
ACM_SCP.1	Minimális konfigurációkezelés lefedés
ADO_DEL.1	Kiszállítási eljárás
ADO_IGS.1	Installálás, generálás, rendszer indítás
ADV_FSP.1	Informális funkcionális előírás
ADV_HLD.2	Biztonság érvényesítő magas-szintű tervezés
ADV_RCR.1	A megfelelés informális bemutatása
AGD_ADM.1	Adminisztrátori útmutató
AGD_USR.1	Felhasználói útmutató
ALC_DVS.1	A biztonsági intézkedések meghatározása
ALC_FLR.1	Alapszintű hibajavítás
ATE_COV.2	A lefedettség elemzése
ATE_DPT.1	A magas-szintű tervek vizsgálata
ATE_FUN.1	A működés tesztelése
ATE_IND.2	Független tesztelés - mintán
AVA_MSU.1	Az útmutatás vizsgálata
AVA_SOF.1	A TOE biztonsági funkciók erejének értékelése
AVA_VLA.1	A fejlesztői sebezhetőség elemzése

5.1.3.1 Konfiguráció kezelés (ACM osztály)

ACM_CAP.3 Jogosultság ellenőrzések

Függőség: ALC_DVS.1 A biztonsági intézkedések azonosítása

Fejlesztői tevékenység elemek:

ACM_CAP.3.1D A fejlesztőnek kell gondoskodnia hivatkozásról a TOE számára.

ACM_CAP.3.2D A fejlesztőnek egy konfigurációkezelés rendszert kell használnia.

ACM_CAP.3.3D A fejlesztőnek konfigurációkezelés dokumentációt kell szolgáltatnia.

Bizonyíték elemek tartalma és megjelenésmódja:

ACM_CAP.3.1C A TOE-ra vonatkozó hivatkozásoknak egyedinek kell lennie a TOE minden verziójára vonatkozóan.

ACM_CAP.3.2C A TOE-t fel kell címkézni hivatkozással.

ACM_CAP.3.3C A konfigurációkezelés dokumentációnak tartalmaznia kell egy konfiguráció listát és egy konfigurációkezelési tervet.

ACM_CAP.3.NEWC A konfiguráció listának egyedileg azonosítania kell az összes konfigurációs tételt, amelyek a TOE-t alkotják.

ACM_CAP.3.4C A konfiguráció listának mindazokat a konfigurációs tételeket le kell írnia, amelyek a TOE-t alkotják.

ACM_CAP.3.5C A konfigurációkezelés dokumentációnak ismertetnie kell azokat a módszereket, amelyeket a konfigurációs tételek egyedi azonosításához alkalmaznak.

ACM_CAP.3.6C A konfigurációkezelés rendszernek minden konfigurációs tételt egyedileg azonosítania kell.

ACM_CAP.3.7C A konfigurációkezelési tervnek ismertetnie kell, hogy a konfigurációkezelés rendszer hogyan van használva.

ACM_CAP.3.8C Bizonyítéknak kell szemléltetni, hogy a konfiguráció kezelés rendszer a konfigurációkezelés tervnek megfelelően működik.

ACM_CAP.3.9C A konfigurációkezelés dokumentumnak bizonyítékot kell nyújtani arra vonatkozóan, hogy a konfigurációkezelés rendszer alatt minden konfigurációs tételt hatékonyan kezeltek és kezelnek.

ACM_CAP.3.10C A konfigurációkezelés rendszernek intézkedéseket kell foganatosítania, hogy csak jogosult változtatásokat lehessen végrehajtani a konfigurációs tételeken.

Értékelői tevékenység elemek:

ACM_CAP.3.1E Az értékelőnek kell alátámasztania, hogy az információ megfelel a bizonyíték tartalmára és prezentációjára vonatkozó összes követelménynek.

ACM_SCP.1 A TOE CM lefedettsége

Függőség: ACM_CAP.3 Jogosultság ellenőrzések

Fejlesztői tevékenység elemek:

ACM_SCP.1.1D A fejlesztőnek konfigurációkezelés dokumentációt kell szolgáltatnia.

Bizonyíték elemek tartalma és megjelenésmódja:

ACM_SCP.1.1C A konfigurációkezelés dokumentációnak bizonyítania kell, hogy a konfigurációkezelés rendszer minimumként nyomon követi a következőket: értékelés tárgya implementációs forma, terv dokumentáció, teszt dokumentáció, felhasználói dokumentáció, adminisztrátori dokumentáció és konfigurációkezelés dokumentáció.

Értékelői tevékenység elemek:

ACM_SCP.1.1E Az értékelőnek kell alátámasztania, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó követelményeknek.

5.1.3.2 Szállítás és működtetés (ADO osztály)

ADO_DEL.1 Kiszállítási eljárás

Függések: Nincs.

Fejlesztői tevékenység elemek:

ADO_DEL.1.1D A fejlesztőnek dokumentálnia kell a TOE vagy annak részeinek a címzett számára történő kiszállítási eljárásait.

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

Bizonyíték elemek tartalma és megjelenésmódja:

ADO_DEL.1.1C A kiszállítási dokumentációnak le kell írnia minden eljárást, amely szükséges ahhoz, hogy a TOE-nak a felhasználó telephelyére történő kiszállítása során a biztonság fenntartható legyen.

Értékelői tevékenység elemek:

ADO_DEL.1.1E Az értékelőnek kell alátámasztania, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó követelményeknek.

ADO_IGS.1 Installálás, generálás, rendszer indítás

Függőség: AGD_ADM.1 Adminisztrátori útmutató

Fejlesztői tevékenység elemek:

ADO_IGS.1.1D A fejlesztőnek dokumentálnia kell a TOE biztonságos installálásához, generálásához és rendszer indításához szükséges eljárásokat.

Bizonyíték elemek tartalma és megjelenésmódja:

ADO_IGS.1.1C A dokumentációnak ismertetnie kell a TOE biztonságos installációhoz, generáláshoz és rendszer indításához szükséges lépéseket.

Értékelői tevékenység elemek:

ADO_IGS.1.1E Az értékelőnek kell alátámasztania, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó követelményeknek.

ADO_IGS.1.2E Az értékelőnek meg kell határoznia azokat a telepítéssel, generálással és rendszer indítással kapcsolatos eljárásokat, amelyek biztonságos konfigurációt eredményeznek.

5.1.3.3 Fejlesztés (ADV osztály)

ADV_FSP.1 Informális funkcionális előírás

Függőség: ADV_RCR.1 A kölcsönös megfelelés informális szemléltetése

Fejlesztői tevékenység elemek:

ADV_FSP.1.1D A fejlesztőnek funkcionális specifikációt kell szolgáltatnia.

Bizonyíték elemek tartalma és megjelenésmódja:

ADV_FSP.1.1C A funkcionális specifikációnak ismertetnie kell a biztonsági funkciókat és azok külső felületét informális stílus alkalmazásával.

ADV_FSP.1.2C A funkcionális specifikációnak belsőleg konzisztensnek kell lennie.

ADV_FSP.1.3C A funkcionális specifikációnak minden külső biztonsági funkció felület használatának célját és módszerét ismertetnie kell, és részleteket kell szolgáltatnia a hatások, a kivételek és a hibajelzések tekintetében, ahol ez lehetséges.

ADV_FSP.1.4C A funkcionális specifikációnak teljes egészében be kell mutatnia a biztonsági funkciókat.

Értékelői tevékenység elemek:

ADV_FSP.1.1E Az értékelőnek igazolnia kell, hogy a rendelkezésre álló információ eleget tesz a Bizonyítékelemek tartalma és megjelenésmódja összes követelményének.

ADV_FSP.1.2E Az értékelő meghatározza, hogy a funkcionális előírás a TOE biztonsága funkcionális követelmények pontos és teljes megjelenítése.

ADV_HLD.2 Biztonság érvényesítő átfogó tervezés

Függőség: ADV_FSP.1 Informális funkcionális előírás
ADV_RCR.1 A megfelelés informális bemutatása

Fejlesztői tevékenység elemek:

ADV_HLD.2.1D A fejlesztőnek szolgáltatnia kell a TSF átfogó (magas-szintű) tervét.

Bizonyíték elemek tartalma és megjelenésmódja:

ADV_HLD.2.1C Az átfogó terv bemutatásának informálisnak kell lennie.

ADV_HLD.2.2C Az átfogó tervnek belsőleg konzisztensnek kell lennie.

ADV_HLD.2.3C Az átfogó tervnek ismertetnie kell a biztonsági funkciók struktúráját az alrendszerek szintjén.

ADV_HLD.2.4C A magas-szintű tervnek a TSF minden egyes alrendszere által szolgáltatott biztonsági funkcionalitást ismertetnie kell.

ADV_HLD.2.5C Az átfogó tervnek azonosítania kell meg kell határoznia az alapját képező minden hardvert, förmvert és/vagy szoftvert, amely a biztonsági funkciók szükségessé tesznek, a támogatást nyújtó védelmi mechanizmusok által biztosított mindazon funkciók bemutatásával, amely a szóban forgó hardverben, förmverben vagy szoftverben vannak implementálva.

ADV_HLD.2.6C Az átfogó tervnek meg kell határoznia minden, a biztonsági funkciók alrendszerhez csatlakozó interfészt.

ADV_HLD.2.7C Az átfogó tervnek meg kell határoznia, hogy a biztonsági funkciók alrendszerhez csatlakozó felületek közül melyek azok, amelyek kívülről láthatóak.

ADV_HLD.2.8C Az átfogó tervnek ismertetnie kell minden, a biztonsági funkciók alrendszereihez csatlakozó interfész használatának célját és módszerét, részleteket szolgáltatva a hatásokról, kivételekről, illetve hibajelzésekről, ahol ez lehetséges.

ADV_HLD.2.9C Az átfogó tervnek ismertetnie kell a TOE felosztását a biztonság politikát érvényre juttató és egyéb alrendszerekre.

Értékelői tevékenység elemek:

ADV_HLD.2.1E Az értékelőnek igazolnia kell, hogy a rendelkezésre álló információ eleget tesz a Bizonyítékelemek tartalma és megjelenésmódja összes követelményének.

ADV_HLD.2.2E Az értékelő meghatározza, hogy a felső-szintű tervezés a TOE biztonsága funkcionális követelmények pontos és teljes megjelenítése.

ADV_RCR.1 A megfelelés informális bemutatása

Függőség: Nincs.

Fejlesztői tevékenység elemek:

ADV_RCR.1.1D A fejlesztőnek analízist kell szolgáltatnia a rendelkezésre bocsátott egymást követő biztonsági funkció megjelenési forma párok között megfelelésekre vonatkozóan.

Bizonyíték elemek tartalma és megjelenésmódja:

ADV_RCR.1.1C A rendelkezésre bocsátott egymást követő biztonsági funkció megjelenési forma pár közötti megfelelésekre vonatkozó analíziseknek demonstrálnia kell, hogy az absztraktabb biztonsági funkció megjelenési forma megfelelő biztonsági funkcionalitása helyesen és teljesen kerül finomításra a kevésbé absztrakt biztonsági funkció megjelenési formában.

Értékelői tevékenység elemek:

ADV_RCR.1.1E Az értékelőnek igazolnia kell, hogy a rendelkezésre álló információ eleget tesz a Bizonyítékelemek tartalma és megjelenésmódja összes követelményének

5.1.3.4 Útmutató dokumentumok AGD

AGD_ADM.1Adminisztrátori útmutató

Függőség: ADV_FSP.1 Informális funkcionális előírás

Fejlesztői tevékenység elemek:

AGD_ADM.1.1D A fejlesztőnek adminisztrátori útmutatót kell szolgáltatnia a rendszer adminisztrációs személyzetnek címezve.

Bizonyíték elemek tartalma és megjelenésmódja:

AGD_ADM.1.1C Az adminisztrátori útmutatónak ismertetnie kell a TOE adminisztrátor rendelkezésre álló adminisztrációs funkciókat és interfészeket.

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

AGD_ADM.1.3C Az adminisztrátori útmutatónak figyelmeztetéseket kell tartalmaznia azon funkciókra és privilégiumokra vonatkozóan, amelyek kontrollálhatók egy biztonságos feldolgozási környezetben.

AGD_ADM.1.4C Az adminisztrátori útmutatónak ismertetnie kell a felhasználói viselkedésre vonatkozó minden olyan feltételezést, amely a TOE biztonsági működés szempontjából fontos.

AGD_ADM.1.5C Az adminisztrátori útmutatónak ismertetnie kell minden, az adminisztrátor felügyelete alá tartozó biztonsági paramétert, megjelölve a biztonságos értékeket, ahogyan az alkalmas.

AGD_ADM.1.6C Az adminisztrátori útmutatónak ismertetnie kell a biztonsággal kapcsolatos események valamennyi típusát, amelyek a végrehajtandó

adminisztratív funkciókkal kapcsolatosak, beleértve a biztonsági funkciók felügyelete alá tartozó entitások biztonsági jellemzőit is.

AGD_ADM.1.7C Az adminisztrátori útmutatónak konzisztensnek kell lennie minden más értékelésre rendelkezésre bocsátott dokumentációval.

AGD_ADM.1.8C Az adminisztrátori útmutatónak ismertetnie kell az informatikai környezetre vonatkozó mindazon biztonsági követelményt, amely az adminisztrátor számára fontos.

Értékelői tevékenység elemek:

AGD_ADM.1.1E Az értékelőnek kell alátámasztania, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó követelményeknek.

AGD_USR.1 Felhasználói útmutató

Függőség: ADV_FSP.1 Informális funkcionális előírás

Fejlesztői tevékenység elemek:

AGD_USR.1.1D A fejlesztőnek felhasználói útmutatót kell szolgáltatnia.

Bizonyíték elemek tartalma és megjelenésmódja:

AGD_USR.1.1C A felhasználói útmutatónak ismertetnie kell a TOE nem adminisztrációs felhasználói számára a rendelkezésre álló funkciókat és interfészeket.

AGD_USR.1.2C A felhasználói útmutatónak ismertetnie kell a TOE által biztosított, a felhasználók által hozzáférhető biztonsági funkciók használatát.

AGD_USR.1.3C A felhasználói útmutatónak figyelmeztetéseket kell tartalmaznia a felhasználók által hozzáférhető azon funkciókra és privilégiumokra vonatkozóan, amelyek kontrollálhatóak egy biztonságos feldolgozási környezetben.

AGD_USR.1.4C A felhasználói útmutatónak világosan be kell mutatnia minden felhasználói felelőséget, amely a TOE biztonságos működéséhez szükséges, beleértve azokat, amelyek a felhasználói viselkedésre vonatkozó azon feltételezésekkel kapcsolatosak, amelyek a TOE biztonsági környezetének ismertetésében találhatók.

AGD_USR.1.5C A felhasználói útmutatónak konzisztensnek kell lennie minden más értékelésre rendelkezésre bocsátott dokumentummal.

AGD_USR.1.6C A felhasználói útmutatónak ismertetnie kell az informatikai környezetre vonatkozó mindazon biztonsági követelményt, amely a felhasználó számára fontos.

Értékelői tevékenység elemek:

AGD_USR.1.1E Az értékelőnek kell alátámasztania, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó követelményeknek.

5.1.3.5 Életciklus-támogatás (ALC osztály)

ALC_DVS.1 A biztonsági intézkedések meghatározása

Függőség: Nincs.

Fejlesztői tevékenység elemek:

ALC_DVS.1.1D A fejlesztőnek fejlesztési biztonsági dokumentációt kell szolgáltatnia.

Bizonyíték elemek tartalma és megjelenésmódja:

ALC_DVS.1.1C A fejlesztési biztonsági dokumentációnak ismertetnie kell minden fizikai, ügyrendi, személyi és más biztonsági intézkedést, amely a TOE terv és implementáció fejlesztői környezetben való bizalmasságának és sértetlenségének védelmére szükséges.

ALC_DVS.1.2C A fejlesztés biztonsági dokumentációjának bizonyítékot kell nyújtania arra vonatkozóan, hogy ezen biztonsági intézkedések a TOE fejlesztése és kezelése során be lettek tartva.

Értékelői tevékenység elemek:

ALC_DVS.1.1E Az értékelőnek kell alátámasztania, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó követelményeknek.

ALC_DVS.1.2E Az értékelőnek kell alátámasztania, hogy a biztonsági intézkedéseket betartják.

ALC_FLR.1 Alapszintű hibajavítás

Függőség: Nincs.

Fejlesztői tevékenység elemek:

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

Bizonyíték elemek tartalma és megjelenésmódja:

ALC_FLR.1.1C A hibajavítási dokumentációnak le kell írnia az teendőket az azonosított biztonsági rések nyomon követéséhez a TOE minden egyes verziójában.

ALC_FLR.1.2C A hibajavítási eljárásoknak elő kell írniuk a biztonsági rések tulajdonságait és hatásait, valamint a rés kijavításának státuszát tartalmazó leírás meglétét.

ALC_FLR.1.3C A hibajavítási eljárásoknak elő kell írniuk, hogy minden egyes biztonsági rés számára javítási lépéseket kell tenni.

ALC_FLR.1.4C A hibajavítási eljárásoknak le kell írniuk azokat a módszereket, amelyek a résekkel kapcsolatos információ, hibajavítások és a TOE felhasználói számára szükséges hibajavítási és útmutató jellegű lépések biztosítására használatos.

Értékelői tevékenység elemek:

ALC_FLR.1.1E Az értékelőnek kell alátámasztania, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó követelményeknek.

5.1.3.6 Tesztelés (ATE osztály)

ATE_COV.2 A lefedettség elemzése

Függőség: ADV_FSP.1 Informális funkcionális előírás
ATE_FUN.1 Funkcionális tesztelés

Fejlesztői tevékenység elemek:

ATE_COV.2.1D A fejlesztőnek egy vizsgálatot kell szolgáltatnia a teszt lefedettségére.

Bizonyíték elemek tartalma és megjelenésmódja:

ATE_COV.2.1C A teszt lefedettség vizsgálatnak demonstrálnia kell a teszt dokumentációban meghatározott tesztek és a biztonsági funkciók közötti megfelelést, ahogyan a biztonsági funkciók a funkcionális specifikációban ismertetve van.

ATE_COV.2.2C A teszt lefedettség vizsgálatnak demonstrálnia kell, hogy a biztonsági funkciók, ahogyan azok a funkcionális specifikációban ismertetve vannak, illetve a teszt dokumentációban meghatározott tesztek közötti megfelelés teljes.

Értékelői tevékenység elemek:

ATE_COV.2.1E Az értékelőnek kell alátámasztania, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó követelményeknek.

ATE_DPT.1 A magas-szintű tervek vizsgálata

Függőség: ADV_HLD.1 Magas-szintű tervezés
ATE_FUN.1 Funkcionális tesztelés

Fejlesztői tevékenység elemek:

ATE_DPT.1.1D A fejlesztőnek szolgáltatnia kell a teszt mélységének a vizsgálatát.

Bizonyíték elemek tartalma és megjelenésmódja:

ATE_DPT.1.1C A teszt mélysége vizsgálatának bizonyítania kell, hogy a teszt dokumentációban meghatározott tesztek elegendőek annak bizonyítására, hogy a biztonsági funkciók az átfogó tervnek megfelelően működik.

Értékelői tevékenység elemek:

ATE_DPT.1.2E Az értékelőnek kell alátámasztania, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó követelményeknek.

ATE_FUN.1 Funkcionális tesztelés

Függőség: Nincs

Fejlesztői tevékenység elemek:

ATE_FUN.1.1D A fejlesztőnek a biztonsági funkciókat tesztelnie kell és az eredményeket dokumentálnia kell.

ATE_FUN.1.2D A fejlesztőnek teszt dokumentációt kell szolgáltatnia.

Bizonyíték elemek tartalma és megjelenésmódja:

ATE_FUN.1.1C A teszt dokumentációnak a teszt tervekből, a teszt eljárások leírásából, a várt teszt eredmények és tényleges teszt eredmények ismertetéséből kell állnia.

ATE_FUN.1.2C A teszt terveknek meg kell határozniuk azokat a biztonsági funkciókat, amelyeket tesztelni kell, és ismertetni kell a végrehajtandó tesztek célját.

ATE_FUN.1.3C A teszt eljárások leírásának meg kell határozniuk a végrehajtandó teszteket, és ismertetniük kell az egyes biztonsági funkciók tesztelésére vonatkozó forgatókönyvet. Ezen forgatókönyveknek tartalmazniuk kell minden, a többi teszt eredményétől való sorrendi függőséget.

ATE_FUN.1.4C A várt teszt eredményeknek be kell mutatniuk azokat az eredményeket, amelyekre a teszt sikeres végrehajtása esetén számítani lehet.

ATE_FUN.1.5C A fejlesztő által végrehajtott tesztek eredményeinek bizonyítaniuk kell, hogy minden tesztelt biztonsági funkció az előírásoknak megfelelően viselkedett.

Értékelői tevékenység elemek:

ATE_FUN.1.1E Az értékelőnek kell alátámasztania, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó követelményeknek.

ATE_IND.2 Független tesztelés - mintán

Függőség: ADV_FSP.1 Informális funkcionális előírás
AGD_ADM.1 Adminisztrátori útmutató
AGD_USR.1 Felhasználói útmutató
ATE_FUN.1 Funkcionális tesztelés

Fejlesztői tevékenység elemek:

ATE_IND.2.1D A fejlesztőnek rendelkezésre kell bocsátania a TOE-t tesztelés céljából.

Bizonyíték elemek tartalma és megjelenésmódja:

ATE_IND.2.1C A TOE-nak alkalmasnak kell lennie a tesztelésre.

ATE_IND.2.2C A fejlesztőnek gondoskodnia kell az erőforrásoknak egy ugyanolyan halmazáról, mint amelyet a fejlesztők a biztonsági funkciók funkcionális tesztelésekor használtak.

Értékelői tevékenység elemek:

ATE_IND.2.1E Az értékelőnek kell alátámasztania, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó követelményeknek.

ATE_IND.2.2E Az értékelőnek meg kell vizsgálnia a TSF egy részhalmazát annak igazolására, hogy a TOE a előírás szerint működik.

ATE_IND.2.3E Az értékelőnek végre kell hajtania egy mintavizsgálatot a vizsgálati dokumentáción azért, hogy ellenőrizze a fejlesztői vizsgálati eredményeket.

5.1.3.7 Sebezhetőség értékelés (AVA osztály)

AVA_MSU.1 Az útmutatás vizsgálata

Függőség: ADO_IGS.1 Installálás, generálás, rendszer indítás
ADV_FSP.1 Informális funkcionális előírás
AGD_ADM.1 Adminisztrátori útmutató
AGD_USR.1 Felhasználói útmutató

Fejlesztői tevékenység elemek:

AVA_MSU.1.1D A fejlesztőnek használati útmutatót kell biztosítani.

Bizonyíték elemek tartalma és megjelenésmódja:

AVA_MSU.1.1C A használati útmutatónak meg kell határoznia a TOE minden lehetséges működési módját (beleértve a meghibásodást vagy működési hibát követő működést is), annak következményeit és jelentőségét a biztonságos működés kezelésére.

AVA_MSU.1.2C A használati útmutatónak teljesnek, világosnak, ellentmondásmentesnek és indokoltnak kell lennie.

AVA_MSU.1.3C A használati útmutatónak fel kell sorolnia minden, a tervezett környezetre vonatkozó feltételezést.

AVA_MSU.1.4C A használati útmutatónak fel kell sorolnia minden, külső biztonsági intézkedésre vonatkozó követelményt (beleértve az eljárási, a fizikai és a személy(zet)i óvintézkedéseket.

Értékelői tevékenység elemek:

AVA_MSU.1.1E Az értékelőnek kell alátámasztania, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó követelményeknek
.

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 útmutatási dokumentáció használatával.

AVA_MSU.1.3E Az értékelőnek meg kell határoznia, hogy az útmutatási dokumentáció lehetővé teszi az összes nem biztonságos állapot érzékelését.

AVA_SOF.1 A TOE biztonsági funkciók erejének értékelése

Függőség: ADV_FSP.1 Informális funkcionális előírás
ADV_HLD.1 Magas-szintű tervezés leírása

Fejlesztői tevékenység elemek:

AVA_SOF.1.1D A fejlesztőnek kell elvégeznie a TOE biztonsági funkciója erősségének elemzését minden olyan mechanizmusra, amelyet az ST-ben azzal azonosítottak, hogy a TOE biztonsági funkciójának erősségére vonatkozó kijelentést tartalmaz.

Bizonyíték elemek tartalma és megjelenésmódja:

AVA_SOF.1.1C Minden egyes mechanizmusra, amely TOE biztonsági funkciójának erősségére vonatkozó kijelentést tartalmaz, a TOE biztonsági funkcióerőssége elemzésének kell kimutatnia, hogy a mechanizmus kielégíti vagy túllépi a PP/ST-ben meghatározott legkisebb erősségi szintet.

AVA_SOF.1.2C Minden egyes mechanizmusra, amely TOE biztonsági funkciójának külöleges erősségére vonatkozó kijelentést tartalmaz, a TOE biztonsági funkcióerőssége elemzésének kell kimutatnia, hogy a mechanizmus kielégíti vagy túllépi a PP/ST-ben meghatározott külöleges funkcióerősségi mértéket.

Értékelői tevékenység elemek:

AVA_SOF.1.1E Az értékelőnek kell alátámasztania, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó követelményeknek.

AVA_SOF.1.2E Az értékelőnek kell alátámasztania, hogy az erősségi igények megfelelőek.

AVA_VLA.1 A sebezhetőség fejlesztői elemzése

Függőség: ADV_FSP.1 Informális funkcionális előírás
ADV_HLD.1 Magas-szintű tervezés leírása
AGD_ADM.1 Adminisztrátori útmutató
AGD_USR.1 Felhasználói útmutató

Fejlesztői tevékenység elemek:

AVA_VLA.1.1D A fejlesztőnek el kell végeznie a sebezhetőségi vizsgálatot.

AVA_VLA.1.2D A fejlesztőnek el kell készítenie a sebezhetőség elemzési dokumentációt.

Bizonyíték elemek tartalma és megjelenésmódja:

AVA_VLA.1.1C A dokumentációnak le kell írni annak a tevékenységnek az analízisét, amelyet elvégeztek, azért, hogy megkeressék a nyilvánvaló módokat, ahogy egy felhasználó megszegheti a TSP szabályokat.

AVA_VLA.1.2C A dokumentációnak le kell írnia a nyilvánvaló sebezhetőségek természetét.

AVA_VLA.1.3C A dokumentációnak valamennyi azonosított sebezhetőségi pontra ki kell mutatnia, hogy a TOE tervezett környezetében egyik sebezhetőségi pont sem használható ki.

Értékelői tevékenység elemek:

AVA_VLA.1.1E Az értékelőnek kell alátámasztania, hogy a szolgáltatott információ megfelel a bizonyítékok tartalmára és megjelenésmódjára vonatkozó követelményeknek.

AVA_VLA.1.2E Az értékelőnek a fejlesztő sebezhetőségi elemzésén alapuló behatolási vizsgálatot kell végrehajtania annak biztosítására, hogy az azonosított nyilvánvaló sebezhetőségi pontok tárgyalásra kerültek.

5.2 Az informatikai környezet biztonsági követelményei

5.2.1 Cryptographic Support (FCS)

FCS_CRM_FPS.1 Kriptográfiai modulok FIPS szerinti megfelelősége

Hierarchikus kapcsolat: nincs más komponenshez.

FCS_CRM_FPS.1.1 Az informatikai környezetnek biztosítania kell az összes, TSF számára szükséges kriptográfiai modult.

FCS_CRM_FPS.1.2 Minden kriptográfiai modulnak FIPS 140 sorozat 1. szint vagy magasabb szintnek megfelelő (compliant) kriptográfiai szolgáltatónak kell lennie vagy NHH minősítéssel rendelkező BALE-nak kell lennie.

Függőség: Nincs

5.2.2 Felhasználói adat védelem(FDP osztály)

FDP_ITC_PKI_INF.1 PKI információk importálása a TSF ellenőrzésén kívülről

Hierarchikus kapcsolat: nincs más komponenshez.

FDP_ITC_PKI_INF.1.1 Az informatikai környezetnek a TOE számára *folyamatosan* biztosítania kell: *tanúsítványokat, CRL-ket,* a következő feltételek teljesülése esetén: *információ rendelkezésre állása az informatikai környezet számára*.

Függőség: Nincs

5.2.3 A TSF védelme (FTP osztály)

FPT_STM.1 Megbízható időpont

Hierarchikus kapcsolat: nincs más komponenshez.

FPT_STM.1.1	Az informatikai környezetnek képesnek kell lennie megbízható időpontok szolgáltatására a TSF számára.
Függőség:	Nincs

6 A TOE összefoglaló specifikációja (ASE_TSS)

6.1 A TOE biztonsági funkciói

Az összefoglaló specifikáció a TOE alábbi tíz biztonsági funkcióját azonosítja:

SF.BASE: Alap

Ez a biztonsági funkció a TOE-t használó alkalmazás (AHA) számára biztosítja a modell létrehozásának, valamint a vezérlő megszerzésének a lehetőségét, valamint a TOE többi biztonsági funkciója számára belső támogatást, alapozást biztosít.

SF.INIT: Inicializálás

Ez a biztonsági funkció biztosítja a TOE hitelességét, annak sértetlenségének és megváltozatlanságának fenntartását.

SF.IAA: Azonosítás, hitelesítés és jogosultság ellenőrzés

Ez a biztonsági funkció kikényszeríti, hogy az AHA felhasználója, azaz a TOE szolgáltatásaihoz hozzáférést kérő személy sikeresen azonosítva, majd közvetlenül ezután (hitelesítő adatának megadásával) sikeresen hitelesítve legyen, valamint jogosultsága ellenőrzésre kerüljön, mielőtt engedélyezné a TOE valamely szolgáltatásának igénybe vételét.

SF.MAN: Menedzsment

Ez a biztonsági funkció a biztonságot érintő jellemzők menedzsmentjét valósítja meg, az AHA számára lehetővé teszi:

- a PKI biztonsági jellemzők menedzsmentjét
- a TOE működését befolyásoló biztonsági jellemzők menedzsmentjét
- biztonságot érintő jellemzők alapállapotának előidézését

SF.CPV: Tanúsítási útvonal érvényesítés

Ez a biztonsági funkció végzi:

- a tanúsítványok ellenőrzését
- a tanúsítási útvonalak felépítését,majd annak érvényességének az ellenőrzését

SF.CRL Visszavonási információ érvényesítés

Ez a biztonsági funkció a visszavonási információk (CRL) érvényességének az ellenőrzését végzi.

SF.SIGSIV: Elektronikus aláírás létrehozása és ellenőrzése

Ez a biztonsági funkció az alábbi két feladatkör végrehajtására képes:

- a felhasználó aláíró magánkulcsának felhasználásával elekronikus aláírást valamint, azt kiegészítő aláírási információkat hoz létre
- az elektronikus aláírást, valamint az azt kiegészítő aláírási információk érvényességét ellenőrzi az aláíró nyilvános kulcsát tartalmazó tanúsítványának felhasználásával

SF.ENCDEC: Titkosítás és visszafejtés

Ez a biztonsági funkció az alábbi három feladatkör végrehajtására képes:

- a címzett(ek) nyilvános kulcsát tartalmazó tanúsítvány(ok) felhasználásával titkosítja a címzett(ek)nek továbbítandó információkat
- a titkosított információkat az AHA felhasználó visszafejtő magánkulcsának felhasználásával visszafejti
- a titkosított információkat az AHA felhasználó visszafejtő magánkulcsának felhasználásával visszafejti, majd egy megadott címzett számára újratitkosítja

SF.TSP: Időbélyeg kérés és ellenőrzés

Ez a biztonsági funkció az alábbi két feladatkör végrehajtására képes:

- aláírás létrehozása vagy ellenőrzése során időbélyeget kér a hitelesítés szolgáltatótól
- a hitelesítés szolgáltatótól kapott vagy az XML aláírásban fellelt időbélyeget ellenőrzi

SF.OCSP: OCSP kérés és ellenőrzés

Ez a biztonsági funkció az alábbi két feladatkör végrehajtására képes:

- aláírás létrehozása vagy ellenőrzése során OCSP kérést állít elő és küld az OCSP válaszadó felé
- az OCSP válaszadótól kapott vagy az XML aláírásban fellelt OCSP választ ellenőrzi

A TOE biztonsági funkciói összefüggésben állnak a PP csomagokkal, amelyet egyrészt az elnevezés hasonlósága, másrészt az alábbi táblázat szemléltet.

28. táblázat: Biztonsági funkciók és a PP csomagok összefüggései

Biztonsági funkció		**PP csomag**	
SF.BASE	Alap	BASE	Alap
SF.INIT	Inicializálás		
SF.IAA	Azonosítás, hitelesítés és jogosultság ellenőrzés		
SF.MAN	Menedzsment		
SF.CPV	Tanúsítási útvonal érvényesítés	CPV	Tanúsítási útvonal érvényesítése (CPV) - Alap
SF.CRL	Visszavonási információ érvényesítés	CRL	Tanúsítvány visszavonási lista (CRL) érvényesítés
SF.SIGSIV	Elektronikus aláírás létrehozása és ellenőrzése	SIG	PKI aláírás készítés
		SIV	PKI aláírás ellenőrzés
SF.ENCDEC	Titkosítás és visszafejtés	ENC	PKI titkosítás kulcs átviteli algoritmusokkal
		DEC	PKI visszafejtés kulcs átviteli algoritmusokkal
SF.TSP	Időbélyeg kérés és ellenőrzés	TSP	Időbélyeg kliens
SF.OCSP	OCSP kérés és ellenőrzés	OCSP	Valós idejű tanúsítvány állapot protokoll (OCSP) kliens

6.1.1 Alap (SF.BASE)

A biztonsági funkció fő célja, hogy a model-view-controller paradigma szerint, az AHA számára lehetővé tegye a modell (model) létrehozását. A modell birtokában az AHA megszerezheti a TOE biztonsági politikáját érvényesítő vezérlőt (controller). A vezérlő működik közre a TOE szolgáltatásainak az AHA számára történő kiközvetítésében. Így ez a biztonsági funkció a TOE összes biztonsági funkciójában közreműködik.

A biztonsági funkció az alábbi szolgáltatásokat nyújtja az AHA számára:

- modell létrehozása
  - hitelesítő kulcs elérési információk és általános adatok megadása
  - aláíró kulcs elérési információk megadása
  - visszafejtő kulcs elérési információk megadása
- vezérlő megszerzése

A biztonsági funkció részletei, a biztonsági igények szempontjából:

- Felhasználói attributum meghatározása során a kulcstároló jellemzők karbantartása felhasználónként elkülönítésre kerül
- Hitelesítése időzítése során az AHA által konfigurálható paraméterek átadhatóak a hitelesítést megelőzően
- Azonosítás időzítése során az AHA által konfigurálható paraméterek átadhatóak az azonosítást megelőzően
- Menedzsment funkciók specifikációja során a biztonsági funkciók végrehajtásának a képessége biztosításra kerül
- TSF körzetszétválasztás során a TSC szubjektumok biztonsági körzetei egymástól elkülönítésre kerülnek

Az SF.BASE biztonsági funkció a következő biztonsági funkcionális követelményekkel találkozik:

29. táblázat: Az SF.BASE biztonsági funkció által lefedett biztonsági követelmények

FIA_ATD.1.1 A TSF-nek karban kell tartania az alábbi biztonsági attributum-listát, amely különálló felhasználókhoz tartozik: *az I&A (a felhasználót azonosító) adatokat tároló eszköz (kulcstároló) jellemzői.*

FIA_UAU.1.1 A TSF-nek lehetővé kell tenni *a használó alkalmazás által konfigurálható paraméterek átadását* a felhasználó nevében, mielőtt a felhasználó hitelesítésre kerül.

FIA_UID.1.1 A TSF-nek lehetővé kell tennie *a használó alkalmazás által konfigurálható paraméterek átadását* a felhasználó nevében, mielőtt a felhasználó azonosítása megtörténik.

FMT_SMF.1.1 A TSF-nek alkalmasnak kell lennie arra, hogy végrehajtsa következő biztonsági menedzsment funkciókat:

k) a használó alkalmazás által konfigurálható paraméterek importálását
l) önellenőrzés
m) azonosítás, hitelesítés és jogosultság ellenőrzés, a felhasználó bejelentkeztetése a kulcstárolóhoz
n) a következő biztonsági attributumok menedzsmentje:

- *megbízható legfelső szintű hitelesítő tanúsítványok,*
- *közbenső szintű hitelesítő tanúsítványok*
- *saját tanúsítványok*
- *más személyek tanúsítványai*
- *tanúsítvány visszavonási listák*
- *a CRL a kibocsátást követően hány napig aktuális*
- *a CRL a következő kibocsátást követő hány napig aktuális*
- *CRL frissesség ellenőrzés engedélyezése*
- *visszavonás ellenőrzés kihagyhatóság engedélyezése*
- *megbízható időszerverek*
- *szolgáltatás igénybevétele utáni kényszerített kijelentkeztetés engedélyezése*
- *OCSP válasz az előállítást követő hány percig aktuális*
- *OCSP válasz a kibocsátást követő hány percig aktuális*
- *OCSP válasz a következő kibocsátást követő hány percig aktuális*
- *OCSP válasz frissesség ellenőrzés engedélyezése*

- *időbélyeg szolgáltatás elérhetősége*
- *OCSP szolgáltatás elérhetősége*
- *szervezeti aláírási szabályzat*

o) tanúsítási útvonal érvényesítés
p) CRL érvényesítés
q) elektronikus aláírás létrehozása és ellenőrzése
r) *titkosítás és visszafejtés*
s) *időbélyeg kérés és ellenőrzés*
t) OCSP kérés és ellenőrzés

FPT_SEP.1.2 A TSF-nek érvényesítenie kell a TSC szubjektumainak biztonsági körzeteinek egymástól való elkülönítését.

6.1.2 Inicializálás (SF.INIT)

A biztonsági funkció öntesztet hajt végre, amelynek fő feladata a TOE hitelességének ellenőrzése, annak sértetlenségének és megváltozatlanságának fenntartása.

A biztonsági funkció részletei, a biztonsági igények szempontjából:

- TSF körzetszétválasztás során védelmet nyújt a nem megbízható szubjektumok általi beavatkozás és megmásítás ellen

Az SF.INIT biztonsági funkció a következő biztonsági funkcionális követelményekkel találkozik:

30. táblázat: Az SF.INIT biztonsági funkció által lefedett biztonsági követelmények

FPT_SEP.1.1 A TSF-nek fenn kell tartania a saját végrehajtása számára egy biztonsági körzetet, amely védelmet nyújt a nem megbízható szubjektumok általi beavatkozás és meghamisítás ellen.

6.1.3 Azonosítás, hitelesítés és jogosultság ellenőrzés (SF.IAA)

A biztonsági funkció fő feladata, hogy biztosítsa, hogy a TOE szolgáltatásait csak az AHA azonosított, hitelesített és jogosult felhasználója, illetve annak nevében eljáró folyamat vehesse igénybe. A biztonsági funkció a TOE szolgáltatásának igénybe vétele előtt és után működésbe lép. A biztonsági funkció a szolgáltatás kérésekor a folyamatot (annak felhasználóját) azonosítja, hitelesíti és jogosultságát ellenőrzi. A biztonsági funkció a sikeres IAA hatására a szolgáltatás igénybe vételét engedélyezi. A biztonsági funkció az IAA-t a szolgáltatás igénybe vétele után alapesetben lebontja.

Használatának fő célja, hogy a hozzáférést kérő személy, az AHA felhasználó bizonyítsa, hogy birtokol egy olyan kulcstárolót, amelyben a személyes tanúsítványa és az ahhoz tartozó magánkulcsa rendelkezésre áll, és azokat használni tudja.

Szintén ez a biztonsági funkció végzi az AHA felhasználójának az aláíró kulcsot vagy visszafejtő kulcsot tartalmazó kulcstárolóhoz történő bejelentkeztetését.

A biztonsági funkció részletei, a biztonsági igények szempontjából:

- Hozzáférés ellenőrzés részhalmaza – PKI megbízólevél menedzsment során a PKI megbízólevél menedzsment SFP érvényesítésre kerül a szubjektumok, az objektumok és a műveletek között
- Biztonsági attributum alapú hozzáférés ellenőrzés – PKI megbízólevél menedzsment során a PKI megbízólevél menedzsment SFP érvényesítésre kerül az objektumokon
- Biztonsági attributum alapú hozzáférés ellenőrzés – PKI megbízólevél menedzsment során a PKI megbízólevél SFP érvényesítésre kerül a művelet engedélyezésének elbírálására
- Biztonsági attributum alapú hozzáférés ellenőrzés – PKI megbízólevél menedzsment során a hozzáférés félreérthetetlenül hitelesítésre kerül minden esetben
- Biztonsági attributum alapú hozzáférés ellenőrzés – PKI megbízólevél menedzsment során a hozzáférés megtagadásra kerül, ha a kulcstároló nem elérhető
- Hitelesítési sikertelenség kezelése során a sikertelen hitelesítési próbálkozások száma észlelésre kerül
- Hitelesítési sikertelenség kezelése során a sikertelen hitelesítési próbálkozások számára vonatkozó korlát elérésekor a TOE képességei igénybe vétele megtagadásra kerül
- Hitelesítési időzítés során a felhasználó hitelesítésre kerül a tevékenység engedélyezése előtt
- Védett hitelesítési visszajelzés során a begépelt karakterek visszajelzése csak a * (csillag) mintával történik
- Azonosítás időzítése során a felhasználó azonosításra kerül a tevékenység engedélyezése előtt
- Biztonsági attributumok menedzsmentje során a biztonsági jellemzők menedzsment korlátozásra kerül az AHA azonosított és hitelesített folyamataira a PKI megbízólevél SFP alapján
- TSF adatok menedzsmentje során a biztonsági jellemzők menedzsment korlátozásra kerül az AHA folyamatokra
- Biztonsági szerepkörök szigorításai során a felhasználó nevében végrehajtott folyamat szerep karbantartásra kerül
- Biztonsági szerepkörök szigorításai során a felhasználók és szerepek összerendelésre kerülnek
- Biztonsági szerepkörök szigorításai során a felhasználó nevében végrehajtott folyamatok feltételei kielégítésre kerülnek
- A TSP kikerülhetetlensége során a TSP kényszerítő funkciói sikeresen végrehajtásra kerülnek a TSC továbbhaladás engedélyezése előtt

Az SF.IAA biztonsági funkció a következő biztonsági funkcionális követelményekkel találkozik:

31. táblázat Az SF.IAA biztonsági funkció által lefedett biztonsági követelmények

FDP_ACC.1.1	A TSF-nek érvényesítenie kell a *PKI megbízólevél menedzsment SFP-t* a *a) Szubjektum: felhasználó nevében végrehajtott folyamat* *b) Objektum: adat, amely a TOE számára átadásra kerül a kriptográfiai művelet végzéséhez, vagy amelyet a TOE ad át tárolásra, vagy egyéb használatra* c) *Művelet: a TOE által biztosított kriptográfiai művelet, a TOE működését vezérlő paraméterek beállítása/lekérdezése* között.
FDP_ACF.1.1	A TSF-nek érvényesítenie kell a *PKI megbízólevél menedzsment SFP-t* olyan objektumokon, amelyek *a szubjektum azonosságán és egy olyan szerep halmazon alapul, amelyet a szubjektum jogosult felvenni.*

FDP_ACF.1.2 A TSF-nek érvényesítenie kell az alábbi szabályokat, hogy megállapíthassa, engedélyezett-e a művelet az ellenőrzött szubjektumok és objektumok között:

a) Magánkulcs importálható, használható, a felhasználó nevében végrehajtott folyamatok által.

b) Nyilvános kulcsú tanúsítványok importálhatók, exportálhatók, törölhetők a felhasználó nevében végrehajtott folyamatok által.

c) Nyilvános kulcsú tanúsítványok használhatók a felhasználó nevében végrehajtott folyamatok által.

d) Titkos kulcs generálható, megsemmisíthető, használható a felhasználó nevében végrehajtott folyamatok által.

e) Titkos kulcs kizárólag aszimmetrikus titkosítással csomagolva importálható és exportálható.

FDP_ACF.1.3 A TSF-nek félreérthetetlenül hitelesítenie kell a szubjektumoknak az objektumokhoz való hozzáférését, amely az alábbi kiegészítő szabályokon alapul: *nincs további szabály.*

FDP_ACF.1.4 A TSF-nek félreérthetetlenül meg kell tagadnia a szubjektumoknak az objektumokhoz való azon hozzáférést, *ha az I&A (a felhasználót azonosító) adatokat tároló eszköz (kulcstároló) az adott pillanatban nem elérhető.*

FIA_AFL.1.1 A TSF-nek észlelnie kell, amikor *a használó alkalmazás által konfigurálható számú* sikertelen hitelesítési próbálkozás fordul elő *a kijelölt felhasználó azonosság hitelesítésére irányuló utolsó sikeres próbálkozás óta végbement sikertelen hitelesítési próbálkozásokat* illetően.

FIA_AFL.1.2 Amikor a sikertelen hitelesítési próbálkozások száma elér vagy meghalad egy meghatározott számot, a TSF-nek *a TOE képességeinek igénybevételét a használó alkalmazás számára meg kell tagadnia.*

FIA_UAU.1.2 A TSF-nek meg kell követelnie, hogy minden egyes felhasználó sikeresen hitelesítve legyen, mielőtt bármelyik másik TSF által közvetített tevékenységet engedélyezne annak a felhasználónak a nevében.

FIA_UAU.7.1 A TSF-nek csak *a begépelt karaktereknek csak a * (csillag) mintával történő visszajelzését* kell biztosítania a felhasználó számára, mialatt a hitelesítés folyamatban van.

FIA_UID.1.2 A TSF-nek meg kell követelnie minden egyes felhasználó sikeres azonosítását, mielőtt bármelyik másik, TSF által közvetített tevékenységet engedélyez annak a felhasználónak a nevében.

FMT_MSA.1.1 A TSF-nek érvényre kell juttatnia a *PKI megbízólevél menedzsment SFP-t*, hogy korlátozza: a *lekérdezését, megváltoztatását, törlését, kiválasztását* a következő vezérlő biztonsági attributumoknak: ***az I&A (a felhasználót azonosító) adatok, TOE működését vezérlő paraméterek, kriptográfiai műveleteket befolyásoló paraméterek***, az ***azonosított és hitelesített felhasználó nevében végrehajtott folyamatokra.***

FMT_MTD.1.1 A TSF-nek korlátoznia kell a: *megváltoztatását, törlését, üresítését,* ***importálását, hozzáadását***, a ***megbízható legfelső szintű hitelesítő tanúsítványok, közbenső szintű hitelesítő tanúsítványok, saját tanúsítványok, más személyek tanúsítványai, tanúsítvány visszavonási listák, a CRL a kibocsátást követően hány napig aktuális,***

a CRL a következő kibocsátást követő hány napig aktuális, CRL frissesség ellenőrzés engedélyezése, visszavonás ellenőrzés kihagyhatóság engedélyezése, megbízható időszerverek, szolgáltatás igénybevétele utáni kényszerített kijelentkeztetés engedélyezése, OCSP válasz az előállítást követő hány percig aktuális, OCSP válasz a kibocsátást követő hány percig aktuális, OCSP válasz a következő kibocsátást követő hány percig aktuális, OCSP válasz frissesség ellenőrzés engedélyezése, időbélyeg szolgáltatás elérhetősége, OCSP szolgáltatás elérhetősége, szervezeti aláírási szabályzat a ***felhasználó nevében végrehajtott folyamatokra***.

FMT_SMR.2.1 A TSF-nek karban kell tartania a következő szerepeket***: felhasználó nevében végrehajtott folyamat.***

FMT_SMR.2.2 A TSF-nek képesnek kell lennie felhasználók és szerepek összerendelésére.

FMT_SMR.2.3 A TSF-nek biztosítania kell, hogy *a felhasználó nevében végrehajtott folyamatok feltételei* ki legyenek elégítve.

FPT_RVM.1.1 TSF-nek biztosítania kell, hogy a TSP-t érvényre juttató funkciói meghívásra kerülnek és sikeresen végrehajtódnak, mielőtt minden egyes **TSF irányítási tárgykör (TSC)** funkció továbbhaladása engedélyeződne.

6.1.4 Menedzsment (SF.MAN)

A biztonsági funkció célja, hogy az AHA számára lehetővé tegye:

- a PKI biztonsági jellemzők menedzsmentjét:
  - tanúsítvány jellegű:
    - megbízható legfelső szintű hitelesítő tanúsítványok (trust anchor)
    - közbenső tanúsítványok (intermediate certificate)
    - saját tanúsítványok (personal end entity certificate)
    - más személyek tanúsítványai (other end entity certificate)
  - CRL jellegű:
    - visszavonási információk
- aTOE működését befolyásoló biztonsági jellemzők menedzsmentjét:
  - a CRL a kibocsátást követő hány napig tekinthető aktuálisnak
  - a CRL a következő kibocsátási dátumot követő hány napig tekinthető
  - a CRL frissesség ellenőrzés engedélyezése
  - visszavonás ellenőrzés kihagyásának engedélyezése
  - megbízható időszerverek
  - szolgáltatás igénybevétele utáni kényszerített kijelentkeztetés engedélyezése
  - OCSP válasz az előállítást követő hány percig tekinthető aktuálisnak
  - OCSP válasz a kibocsátás követő hány percig tekinthető aktuálisnak
  - OCSP válasz a következő kibocsátást követő hány percig tekinthető aktuálisnak
  - OCSP válasz frissesség ellenőrzés engedélyezése
  - időbélyeg szolgáltatás elérhetősége
  - OCSP szolgáltatás elérhetősége
  - szervezeti aláírási szabályzat
- biztonságot érintő jellemzők alapállapotba állítását

A biztonsági funkció részletei, a biztonsági igények szempontjából:

- Statikus attributum inicializáció során a biztonsági jellemzők alapértékei biztosításra kerülnek
- Statikus attributum inicializáció során az alapértéket az AHA folyamatok megváltoztathatják

Az SF.MAN biztonsági funkció a következő biztonsági funkcionális követelményekkel találkozik:

32. táblázat: Az SF.MAN biztonsági funkció által lefedett biztonsági követelmények

FMT_MSA.3.1	A TSF-nek érvényesítenie kell a *PKI megbízólevél menedzsment SFP-t,* hogy biztosítsa a *megfelelő* alapértelmezett értékeket a biztonsági attributumok számára, amelyek az SFP végrehajtásakor használatosak.
FMT_MSA.3.2	A TSF-nek lehetővé kell tennie ***a felhasználó nevében végrehajtott folyamat*** számára a lehetséges kezdeti értékek meghatározását abból a célból, hogy felülírja az alapértékeket, amikor egy objektum vagy információ készül.

6.1.5 Tanúsítási útvonal érvényesítés (SF.CPV)

A biztonsági funkció célja kettős:

- az AHA számára tanúsítvány ellenőrzés, PKIX szabvány szerinti tanúsítási útvonal felépítés és érvényesítés szolgáltatásokat nyújt
- a TOE biztonsági funkciókat támogatja a tanúsítvány ellenőrzés, PKIX szabvány szerinti tanúsítási útvonal felépítés és érvényesítés ellenőrzésekkel

A biztonsági funkció az AHA, valamint a többi biztonsági funkció számára a következő szolgáltatásokat nyújtja:

tanúsítvány ellenőrzés jellegű:

- megbízható legfelső szintű tanúsítvány ellenőrzése
- közbenső tanúsítvány ellenőrzése
- végtanúsítvány (saját vagy más személy tanúsítványa) ellenőrzése
- kulcshasználat ellenőrzése

tanúsítási útvonal felépítés és érvényesítés jellegű:

- tanúsítási útvonal felépítése
- tanúsítási útvonal érvényesítése
- tanúsítási útvonal együttes felépítése és érvényesítése

A biztonsági funkció részletei, a biztonsági igények szempontjából:

- Tanúsítási útvonal felépítése az AHA folyamat által megadott megbízható tanúsítvánnyal kezdve kezdődik és a végtanúsítványig tart, a distinguished name egyezősége alapján
- Tanúsítási útvonal felépítése során a kulcshasználat ellenőrzésre kerül
- Tanúsítási útvonal felépítése során az extendedKeyUsage tartalmára nincs szabály
- Tanúsítási útvonal felépítése során a distinguished name és X.509 formátum szabály kivételével a további szabályok kikerülhetők
- Tanúsítási útvonal inicializálása során az AHA folyamat által megadott megbízható legfelső szintű hitelesítő tanúsítványok lesznek használva
- Tanúsítási útvonal inicializálása során az aktuális idő megszerzésre kerül az AHA folyamat által megadott időszerverektől, vagy az aktuális környezetből
- Tanúsítási útvonal inicializálása során a megbízható legfelső szintű tanúsítvány ellenőrzésre kerül
- Tanúsítási útvonal inicializálása során az információk származtatása a megbízható legfelső szintű tanúsítványból történik
- Tanúsítvány feldolgozás során a tanúsítvány ellenőrzésre kerül
- Tanúsítvány feldolgozás során a visszavonási állapot ellenőrzése kihagyásra kerül a no-check kiterjesztés esetén
- Tanúsítvány feldolgozás során a visszavonási állapot ellenőrzés kihagyásra kerül, ha az AHA folyamat felülbírálta azt
- Tanúsítvány feldolgozás során a tanúsítvány elfogadásra kerül, ha az a CRL vagy OCSP ellenőrzése alapján nincs visszavonva
- Tanúsítvány feldolgozás során a nyilvános kulcs paraméterei állapotgép szabályai alkalmazásra kerülnek
- Közbenső tanúsítvány feldolgozás során a közbenső tanúsítvány elfogadásának feltételei ellenőrzésre kerülnek
- Tanúsítási útvonal kimenetében hiba kerül visszaadásra, ha a tanúsítási útvonalban bármely tanúsítvány visszavonásra került
- Tanúsítási útvonal kimenetében az alany, nyilvános kulcs és további adatok visszaadása a végtanúsítványból
- Tanúsítási útvonal kimenetében a végtanúsítvány, az alternatív nevek, tanúsítvány lánc és extendedKeyUsage visszaadása a végtanúsítványból

- Tanúsítási útvonal kimenetében a nyilvános kulcs visszaadása a tanúsítási útvonal állapotgép alapján történik

Az SF.CPV biztonsági funkció a következő biztonsági funkcionális követelményekkel találkozik:

33. táblázat: Az SF.CPV biztonsági funkció által lefedett biztonsági követelmények

FDP_CPD.1	***Tanúsítási útvonal felépítése***
FDP_CPD.1.1	A TSF-nek az érvényesítési útvonalat a *felhasználó nevében végrehajtott folyamat* által szolgáltatott megbízható legfelső szintű hitelesítő tanúsítvánnyal kezdve a végtanúsítványig kell felépítenie, a következő tanúsítvány mezők vagy kiterjesztések egyezőségi szabályait alkalmazva: *distinguished name*.
FDP_CPD.1.2	A TSF-nek a tanúsítási útvonalat a következő kiegészítő egyezőségi szabályok alkalmazásával kell felépítenie: *d) aláírás ellenőrzése esetén:* *aa) ha aláírási szabályzat nincs érvényben, akkor a keyUsage kiterjesztésben a nonRepudiation bit be van állítva* *ab) ha aláírási szabályzat érvényben van, akkor annak rendelkezéseitől függően: a keyUsage kiterjesztésben a nonRepudiation vagy digitalSignature bit be van állítva* *e) a keyUsage kiterjesztésben a digitalSignature bit be van állítva, entitás hitelesítése esetén* a) *a keyUsage kiterjesztésben a keyEncipherment bit be van állítva, titkosítás, visszafejtés esetén*
FDP_CPD.1.3	A TSF-nek a tanúsítási útvonalat a következő kiegészítő egyezőségi szabályok alkalmazásával kell felépítenie: a) *nincs további szabály az extendedKeyUsage kiterjesztés tartalmára*
FDP_CPD.1.4	A TSF kikerülhet bármely egyezőségi szabályt, kivéve: *a) distinguished name* *b) a tanúsítvány formátuma X.509* amennyiben további tanúsítási útvonalak szükségesek.
FDP_DAU_CPV_INI.1	***Tanúsítási útvonal inicializálása -- alap***
FDP_DAU_CPV_INI.1.1	A TSF-nek a *felhasználó nevében végrehajtott folyamat* által szolgáltatott megbízható legfelső szintű hitelesítő tanúsítványt kell használnia.
FDP_DAU_CPV_INI.1.2	A TSF-nek a *felhasználó nevében végrehajtott folyamat által meghatározott időszerverektől vagy ha az nem áll rendelkezésre, akkor a lokális környezetből,* mint megbízható forrásból kell megszereznie az aktuális időt, amelyet 'current-time'-nak nevezünk.
FDP_DAU_CPV_INI.1.3	A TSF-nek a megbízható legfelső szintű tanúsítványok esetében a következő ellenőrzéseket kell elvégeznie: *a) Subject DN és az Issuer DN egyezik* *b) A tanúsítványon az aláírás érvényes, a megbízható legfelső szintű hitelesítő tanúsítvány alanyának nyilvános kulcsával és annak paraméterével (ha az rendelkezésre áll) ellenőrizve* *c) a megbízható legfelső szintű tanúsítvány notBefore mezője <= current-time*

d) *a megbízható legfelső szintű tanúsítvány notAfter mezője => current-time*

kell A TSF-nek a megbízható legfelső szintű hitelesítő tanúsítványból származtatnia kell a következő információkat: *subject DN, subject public key, subject public key algorithm object identifier, subject public key paraméterek.*

FDP_DAU_CPV_CER.1 Tanúsítvány feldolgozás -- alap

FDP_DAU_CPV_CER.1.1 A TSF-nek a tanúsítványt csak akkor szabad elfogadnia, ha a következő ellenőrzések sikeresen megtörténtek:

a) A tanúsítványon az aláírás ellenőrzése a következőekkel: parent-public-key, parent-public-key-algorithm-identifier, és parent-public-key-parameters
b) A tanúsítvány notBefore mezője < = current-time
c) A tanúsítvány notAfter mezője > = current-time
d) A tanúsítvány issuer mezője = parent-DN
e) A TSF képes a tanúsítvány minden kritikus kiterjesztését feldolgozni.

FDP_DAU_CPV_CER.1.2 A TSF kikerülheti a visszavonási állapot ellenőrzését, ha a tanúsítvány tartalmazza a no-check kiterjesztést.

FDP_DAU_CPV_CER.1.3 A TSF ki kell hagynia a visszavonás ellenőrzését, ha a visszavonási információ nem áll rendelkezésre és *a felhasználó nevében végrehajtott folyamat* felülbírálja a visszavonás ellenőrzést.

FDP_DAU_CPV_CER.1.4 A TSF-nek el kell fogadnia a tanúsítványt, ha a visszavonási állapot *CRL ellenőrzés vagy OCSP ellenőrzés* alapján, meggyőződött arról, hogy a tanúsítvány nincs visszavonva.

FDP_DAU_CPV_CER.1.5 A TSF-nek nyilvános kulcs paraméterei állapotgépet a következő szabályok szerint kell vezérelnie:

a) a paraméter megállapítása a tanúsítvány subjectPublickeyInfo mezőjéből, ha abban szerepel a paraméter, különben
b) az eredeti paraméter állapot megtartása, ha az aktuális tanúsítvány nyilvános kulcsának algoritmusa és a kibocsátó nyilvános kulcsának algoritmusa azonos algoritmus családba tartozik, különben
c) a paramétert be kell állítani „null” értékre.

FDP_DAU_CPV_CER.2 Közbenső tanúsítvány feldolgozás -- alap

FDP_DAU_CPV_CER.2.1 A TSF-nek a közbenső tanúsítványt csak akkor kell elfogadnia, ha a következő ellenőrzések sikeresen megtörténtek:

a) basicConstraints kiterjesztés jelen van, és abban a cA = TRUE
b) pathLenConstraint kényszer teljesül
c) ha kritikus keyUsage kiterjesztés jelen van, akkor abban a keyCertSign bit be van állítva

FDP_DAU_CPV_OUT.1 Tanúsítási útvonal kimenete -- alap

FDP_DAU_CPV_OUT.1.1 A TSF-nek tanúsítási útvonal érvényesítési hibát kell visszaadnia, ha az tanúsítási útvonalban bármely tanúsítvány visszautasításra került.

FDP_DAU_CPV_OUT.1.2 A végtanúsítványból a TSF-nek a következő változókat kell

visszaadnia: subject DN, subject public key algorithm identifier, subject public key, kritikus keyUsage kiterjesztés.

FDP_DAU_CPV_OUT.1.3 A végtanúsítványból a TSF-nek a következő további változókat kell visszaadnia: *tanúsítvány, subject alternative names, tanúsítvány lánc, extendedKeyUsage.*

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

6.1.6 Visszavonási információ érvényesítés (SF.CRL)

A biztonsági funkció célja kettős:

- az AHA számára visszavonási információ ellenőrzés szolgáltatást nyújt
- az A2-API biztonsági funkciókat támogatja a visszavonási információk ellenőrzésével

A biztonsági funkció részletei, a biztonsági igények szempontjából:

- Alap CRL ellenőrzés során a CRL beszerzése az AHA folyamat által szolgáltatott tárolóból vagy a szóban forgó tanúsítvány CRLDistributionPoints kiterjesztése által mutatott címről történik
- Alap CRL ellenőrzés során a CRL kibocsátó nyilvános kulcsának adatai megszerzésre kerülnek
- Alap CRL ellenőrzés során a CRL aláírása a megbízható nyilvános kulccsal ellenőrzésre kerül
- Alap CRL ellenőrzés során a CRL-t kibocsátó tanúsítványában a kulcshasználat (cRLSign) ellenőrzésre kerül
- Alap CRL ellenőrzés során CRL kibocsátó mezője egyeztetésre kerül a feltételezett kibocsátóval
- Alap CRL ellenőrzés során a CRL aktuálisnak kerül elfogadásra, a CRLAfterThisUpdateLimit ellenőrzés teljesülésekor
- Alap CRL ellenőrzés során a CRL aktuálisnak kerül elfogadásra, a CRLAfterNextUpdateLimit ellenőrzés teljesülésekor
- Alap CRL ellenőrzés során a CRL aktuálisnak kerül elfogadásra, ha az AHA folyamat felülbírálja a frissesség ellenőrzését
- Alap CRL ellenőrzés során a fel nem dolgozott kritikus kiterjesztést tartalmazó CRL visszautasításra kerül
- Alap CRL ellenőrzés során az X.509 formátum ellenőrzésre kerül

Az SF.CRL biztonsági funkció a következő biztonsági funkcionális követelményekkel találkozik:

34. táblázat: Az SF.CRL biztonsági funkció által lefedett biztonsági követelmények

FDP_DAU_CRL.1.1 A TSF-nek a CRL-t a következő forrásokból kell beszereznie:a *felhasználó nevében végrehajtott folyamat által szolgáltatott tároló, a kérdéses tanúsítvány CRLDistributionPoints kiterjesztése által mutatott cím.*

FDP_DAU_CRL.1.2 A TSF-nek meg kell szereznie a CRL kibocsátójáról a következő adatokat: megbízható nyilvános kulcs, algoritmus, és a nyilvános kulcs paraméterei.

FDP_DAU_CRL.1.3 A TSF-nek a CRL aláírását a következőekkel kell ellenőriznie: a CRL kibocsátójának a megbízható nyilvános kulcsa, algoritmusa, és nyilvános

kulcsának paraméterei.

FDP_DAU_CRL.1.4 A TSF-nek ellenőriznie kell, hogy a CRL-t kibocsátó tanúsítványában a kritikus keyUsage kiterjesztés jelen legyen és abban a cRLSign bit be legyen állítva.

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

FDP_DAU_CRL.1.6 A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha a *thisUpdate mező értékére nézve* a következő szabályzat érvényesül: *current-time <= thisUpdate + x, ahol az x a felhasználó nevében végrehajtott folyamat által megadott érték.*

FDP_DAU_CRL.1.7 A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha a *nextUpdate mező értékére nézve* a következő szabályzat érvényesül: *current-time <= nextUpdate + x, ahol az x a felhasználó nevében végrehajtott folyamat által megadott érték*.

FDP_DAU_CRL.1.8 A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha a *felhasználó nevében végrehajtott folyamat* felülbírálja a frissesség ellenőrzését.

FDP_DAU_CRL.1.9 A TSF-nek vissza kell utasítania a CRL-t, ha az olyan kritikus kiterjesztést tartalmaz, amelyet a TSF nem dolgoz fel.

FDP_DAU_CRL.1.10 A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie:
a) a CRL formátuma X.509

6.1.7 Elektronikus aláírás létrehozása és ellenőrzése (SF.SIGSIV)

A biztonsági funkció két fő feladatköre:

- az AHA felhasználó aláíró magánkulcsával elektronikus aláírás és kiegészítő aláírási információk létrehozása
- elektronikus aláírás és az azt kiegészítő aláírási információk ellenőrzése az aláíró tanúsítványának felhasználásával

A biztonsági funkció az elektronikus aláírás létrehozását és ellenőrzését az XMLDSIG szabvány és az XAdES v1.2.2 vagy v1.3.2 szabvány XAdES-BES, EPES, T, C, X, X-L és A formátumának és **„**Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára (2005. november 22.)**”** megfelelően vagy a „Egységes MELASZ formátum elektronikus aláírásokra” v2.0 dokumentumnak megfelelően végzi.

A biztonsági funkció részletei, a biztonsági igények szempontjából:

- PKI aláírás exportálása során a magánkulcs használatával az aláírás létrehozása
- PKI aláírás exportálása során az aláírást kísérő információk az aláíráshoz csatolásra kerülnek.
- PKI aláírás importálása során az aláírást kísérő információk használva lesznek
- Aláírás bináris ellenőrzése során az aláírás ellenőrzéséhez az SF.CPV biztonsági funkcióból származó adatok kötelezően használva lesznek
- Aláírás bináris ellenőrzése során a kulcshasználat (nonRepudiation és/vagy digitalSignature) az SF.CPV biztonsági funkció kimenetében ellenőrzésre kerül

- Aláírás bináris ellenőrzése során az aláíró DN az SF.CPV biztonsági funkció kimenetével egyeztetésre kerül, ha aláírási szabályzat nincs érvényben, akkor a keyUsage kiterjesztésben kizárólag csak a nonRepudiation bit beállítottsága, ha aláírási szabályzat érvényben van, akkor annak előírásai szerint a nonRepudiation és digitalSignature bit vizsgálata, a minősített elektronikus aláíráshoz a kötelező qCStatements kiterjesztésben az id-etsi-qcs-QcCompliance OID megléte ellenőrzésre kerül

Az SF.SIGSIV biztonsági funkció a következő biztonsági funkcionális követelményekkel találkozik:

35. táblázat: Az SF.SIGSIV biztonsági funkció által lefedett biztonsági követelmények

FDP_ETC_SIG.1.1	A TSF-nek a magánkulcs felhasználásával elektronikus aláírást kell létrehozni.
FDP_ETC_SIG.1.2	*A TSF-nek az elektronikus aláírásba a következő aláírást kísérő információkat kell befoglalnia:* *1)A1-kombatibilis elektronikus aláírás készítése esetén:* *a)kötelezően: hash algoritmus, aláírási algoritmus, aláíró nyilvános kulcs, aláíró DN, aláíró tanúsítványt kibocsátó DN, aláíró tanúsítványának sorozatszáma, aláíró tanúsítványa, aláíró tanúsítványának az érvényesített tanúsítási útvonala, aláírás időpontja* *b)opcionálisan: aláírás helye(város), aláírás helye(irányítószám), aláírás helye(megye), aláírás helye(ország), aláíró szerepkör* *2)A2 elektronikus aláírás készítése esetén:* *a)„Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára (2005. november 22.)” választása esetén:* *aa)kötelezően:* • *kanonizálási módszer (CanonicalizationMethod), a http://www.w3.org/TR/2001/REC-xml-c14n-20010315 értékkel* • *aláírási algoritmus (SignatureMethod) az RSAwithSHA1 értékkel* • *aláírt dokumentumok külső vagy belső hivatkozásai (Reference)* • *transzformációk (Transforms) az http://www.w3.org/TR/2001/REC-xml-c14n-20010315 vagy http://www.w3.org/2000/09/xmldsig#BASE64 értékkel* • *lenyomatképző algoritmus (DigestMethod) az SHA1 értékkel* • *az aláíró tanúsítványa (KeyInfo)* • *aláírás időpontja (SigningTime)* • *hivatkozás az aláíró tanúsítványára (SigningCertificate)* • *aláírási szabályzat (SignaturePolicyIdentifier)* • *aláírt dokumentumok adatformátum leírásai (DataObjectFormat)* *ab)opcionálisan:* • *az aláíró nyilvános kulcsa (KeyInfo)* • *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)* • *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)* • *aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)* • *aláíró szerepkörei (SignerRole)* • *kötelezettségvállalás jelzése (CommitmentTypeIndication)* • *aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy*

IndividualDataObjectsTimeStamp)
- *ellenjegyző aláírás (CounterSignature)*
- *aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)*
- *aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)*
- *referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)*
- *archív időbélyeg(ek) (ArchiveTimeStamp)*

b)v1.2.2 vagy v1.3.2 szabványos formátum választása esetén:
ba)kötelezően:
- *kanonizálási módszer (CanonicalizationMethod)*
  http://www.w3.org/TR/2001/REC-xml-c14n-20010315,
  http://www.w3.org/TR/2001/REC-xml-c14n-0010315#WithComments,
  http://www.w3.org/TR/2001/REC-xml-c14n-20010315,
  http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments,
  http://www.w3.org/2006/12/xml-c14n11,
  http://www.w3.org/2006/12/xml-c14n11#WithComments
- *aláírási algoritmus (SignatureMethod) RSAwithSHA1, RSAwithSHA256, RSAwithSHA384, RSAwithSHA512 vagy DSAwithSHA1*
- *aláírt dokumentumok külső vagy belső hivatkozásai (Reference)*
- *transzformációk (Transforms)*
- *lenyomatképző algoritmus (DigestMethod)*
- *az aláíró tanúsítványa (KeyInfo)*
- *aláírás időpontja (SigningTime)*
- *hivatkozás az aláíró tanúsítványára (SigningCertificate)*

bb)opcionálisan:
- *az aláíró nyilvános kulcsa (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)*
- *aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)*
- *aláíró szerepkörei (SignerRole)*
- *aláírási szabályzat (SignaturePolicyIdentifier)*
- *aláírt dokumentumok adatformátum leírásai (DataObjectFormat*
- *kötelezettségvállalás jelzése (CommitmentTypeIndication)*
- *aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)*
- *ellenjegyző aláírás (CounterSignature)*

- *aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)*
- *aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)*
- *referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)*
- *archív időbélyeg(ek) (ArchiveTimeStamp)*

c)„Egységes MELASZ formátum elektronikus aláírásokra” v2.0 választása esetén:
ca)kötelezően:

- *kanonizálási módszer (CanonicalizationMethod), a http://www.w3.org/TR/2001/REC-xml-c14n-20010315 értékkel*
- *aláírási algoritmus (SignatureMethod) az RSAwithSHA1 vagy RSAwithSHA256 értékkel*
- *aláírt dokumentumok külső vagy belső hivatkozásai (Reference)*
- *transzformációk (Transforms) az http://www.w3.org/TR/2001/REC-xml-c14n-20010315 vagy http://www.w3.org/2000/09/xmldsig#BASE64 értékkel*
- *lenyomatképző algoritmus (DigestMethod) az SHA1 vagy SHA256 értékkel*
- *az aláíró tanúsítványa (KeyInfo)*
- *aláírás időpontja (SigningTime)*
- *hivatkozás az aláíró tanúsítványára (SigningCertificate)*
- *aláírási szabályzat (SignaturePolicyIdentifier)*
- *aláírt dokumentumok adatformátum leírásai (DataObjectFormat)*

cb)opcionálisan:

- *az aláíró nyilvános kulcsa (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)*
- *aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)*
- *aláíró szerepkörei (SignerRole)*
- *kötelezettségvállalás jelzése (CommitmentTypeIndication)*
- *aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)*
- *ellenjegyző aláírás (CounterSignature)*
- *aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró*

tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)*
- *aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)*
- *referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)*
- *archív időbélyeg(ek) (ArchiveTimeStamp)*

FDP_ITC_SIG.1.1 *A TSF-nek az alábbi aláírást kísérő információkat kell használnia az aláírás ellenőrzése során:*

1)A1-kombatibilis elektronikus aláírás ellenőrzése esetén:

a)kötelezően: hash algoritmus, aláírási algoritmus, aláíró nyilvános kulcs, aláíró DN, aláíró tanúsítványt kibocsátó DN, aláíró tanúsítáványának sorozatszáma, aláíró tanúsítványa, aláíró tanúsítványának az érvényesített tanúsítási útvonala, aláírás időpontja

b)opcionálisan: aláírás helye(város), aláírás helye(irányítószám), aláírás helye(megye), aláírás helye(ország), aláíró szerepkör

2)A2 elektronikus aláírás ellenőrzés esetén:

a)„Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára (2005. november 22.)" formátumnak vagy az „Egységes MELASZ formátum elektronikus aláírásokra" v2.0 dokumentumnak megfelelő aláírás ellenőrzése esetén:

aa) kötelezően:
- *kanonizálási módszer (CanonicalizationMethod)*
- *aláírási algoritmus (SignatureMethod)*
- *aláírt dokumentumok külső vagy belső hivatkozásai (Reference)*
- *transzformációk (Transforms)*
- *lenyomatképző algoritmus (DigestMethod)*
- *az aláíró tanúsítványa (KeyInfo)*
- *aláírás időpontja (SigningTime)*
- *hivatkozás az aláíró tanúsítványára (SigningCertificate)*
- *aláírási szabályzat (SignaturePolicyIdentifier)*
- *aláírt dokumentumok adatformátum leírásai (DataObjectFormat)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)*

ab) opcionálisan:
- *az aláíró nyilvános kulcsa (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)*

- *aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)*
- *aláíró szerepkörei (SignerRole)*
- *kötelezettségvállalás jelzése (CommitmentTypeIndication)*
- *aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)*
- *ellenjegyző aláírás (CounterSignature)*
- *aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)*
- *aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)*
- *referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)*
- *archív időbélyeg(ek) (ArchiveTimeStamp)*

b) v1.2.2 vagy v1.3.2 szabványos formátumnak megfelelő aláírás ellenőrzése esetén:
ba) kötelezően:

- *kanonizálási módszer (CanonicalizationMethod)*
- *aláírási algoritmus (SignatureMethod)*
- *aláírt dokumentumok külső vagy belső hivatkozásai (Reference)*
- *transzformációk (Transforms)*
- *lenyomatképző algoritmus (DigestMethod)*
- *az aláíró tanúsítványa (KeyInfo)*
- *aláírás időpontja (SigningTime)*
- *hivatkozás az aláíró tanúsítványára (SigningCertificate)*

bb) opcionálisan:

- *az aláíró nyilvános kulcsa (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)*
- *az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)*
- *aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)*
- *aláíró szerepkörei (SignerRole)*
- *aláírási szabályzat (SignaturePolicyIdentifier)*
- *aláírt dokumentumok adatformátum leírásai (DataObjectFormat*
- *kötelezettségvállalás jelzése (CommitmentTypeIndication)*
- *aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)*
- *ellenjegyző aláírás (CounterSignature)*
- *aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)*
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró*

tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)
- *hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)*
- *aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)*
- *referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)*
- *aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)*
- *archív időbélyeg(ek) (ArchiveTimeStamp)*

FDP_DAU_SIG.1.1 A TSF-nek a Tanúsítási útvonal érvényesítése (CPV) - Alap csomagból a következő információkat kell használnia: subject public key algorithm, subject public key, subject public key parameters, amikor az aláírt adaton az elektronikus aláírást ellenőrzi.

FDP_DAU_SIG.1.2 A TSF-nek ellenőriznie kell, hogy a Tanúsítási útvonal érvényesítése (CPV) - Alap csomag által visszaadott keyUsage kiterjesztésben a nonRepudiation bit **vagy a digitalSignature bit** be van állítva.

FDP_DAU_SIG.1.3 A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie:

a) Tanúsítási útvonal érvényesítése (CPV) - Alap csomag által visszaadott subject DN egyezik az aláírási információkkal.

b) a tanúsítvány keyUsage kiterjesztésében:
ba) ha aláírási szabályzat nincs érvényben, akkor kizárólag csak a nonRepudiation bit van beállítva
bb) ha aláírási szabályzat van érvényben, akkor annak rendelkezésétől függően az alábbiak valamelyike:
- kizárólag csak a nonRepudiation bit van beállítva
- kizárólag csak a digitalSignature bit van beállítva
- a nonRepudiation bit van beállítva, a többi bit nem számít
- a digitalSignature bit van beállítva, a többi bit nem számít

c) szigorú üzemmódban a minősített elektronikus aláírás esetén az aláíró tanúsítványában a kötelező qcStatements kiterjesztésben az id-etsi-qcs-QcCompliance OID meglétének ellenőrzése

6.1.8 Titkosítás és visszafejtés (SF.ENCDEC)

A biztonsági funkció három fő feladatköre:
- a címzett(ek) nyilvános kulcsát tartalmazó tanúsítvány(ok) felhasználásával titkosítja a címzett(ek)nek továbbítandó információkat
- a titkosított információkat az AHA felhasználó visszafejtő magánkulcsának felhasználásával visszafejti
- a titkosított információkat az AHA felhasználó visszafejtő magánkulcsának felhasználásával visszafejti, majd egy megadott címzett részére újratitkosítja

A biztonsági funkció részletei, a biztonsági igények szempontjából:

- PKI titkosítás exportja során a titkosított adathoz a titkosítást kísérő információk csatolásra kerülnek
- PKI titkosítás exportja során a nyilvános kulcs adatok az SF.CPV biztonsági funkció kimenetéből lesznek használva
- PKI titkosítás ellenőrzése során a kulcshasználat (keyEncipherment) az SF.CPV biztonsági funkció kimenetében ellenőrzésre kerül
- PKI titkosítás ellenőrzése során a lenyomat egyeztetésre kerül
- PKI titkosítás importja során a titkosítást kísérő információk lesznek használva
- PKI titkosítás importja során a visszafejtés elvégzésre kerül

Az SF.ENCDEC biztonsági funkció a következő biztonsági funkcionális követelményekkel találkozik:

36. táblázat: Az SF.ENCDEC biztonsági funkció által lefedett biztonsági követelmények

FDP_ETC_ENC.1.1	A TSF-nek a következő információkat kell a titkosított adattal együtt biztosítania: *a) visszafejtő (címzett) nyilvános kulcsú tanúsítványa* *b) titkosítás időpontja* *c) fájl név vagy annak megfelelője* *d) titkosítatlan tartalomra képzett lenyomat* *e) a címzett részére aszimmetrikus titkosítással csomagolt titkos kulcs*
FDP_ETC_ENC.1.2	A TSF-nek a Tanúsítási útvonal érvényesítése (CPV) - Alap csomagból a következő információkat kell használnia a titkosított adat létrehozásakor: subject public key algorithm, subject public key, subject public key paraméterek.
FDP_DAU_ENC.1.1	A TSF-nel ellenőriznie kell, hogy a Tanúsítási útvonal érvényesítése (CPV) - Alap csomagból visszaadott keyUsage kiterjesztésben a keyEncipherment bit be van állítva.
FDP_DAU_ENC.1.2	A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie: a) *a visszafejtett tartalomra képzett lenyomat megegyezik-e az eredeti lenyomattal*
FDP_ITC_ENC.1.1	A TSF-nek a titkosított adatról a következő információkat kell használnia: *a) visszafejtő (címzett) nyilvános kulcsú tanúsítványa* *b) titkosítás időpontja* *c) fájl név vagy annak megfelelője* *d) titkosítatlan tartalomra képzett lenyomat* *e) a címzett részére aszimmetrikus titkosítással csomagolt titkos kulcs*
FDP_ITC_ENC.1.2	*A TSF-nek el kell végeznie a visszafejtést.*

6.1.9 Időbélyeg kliens (SF.TSP)

A biztonsági funkció két fő feladatköre:

- aláírás létrehozása vagy ellenőrzése során időbélyeg kérése a hitelesítés szolgáltatótól
- a hitelesítés szolgáltatótól kapott vagy az XML aláírásban fellelt időbélyeget ellenőrzi

A biztonsági funkció részletei, a biztonsági igények szempontjából:

- Az időbélyegek kérése az RFC 3161-nek megfelelően történik
- Az időbélyeg kérés kötelezően tartalmazza a verzió, messageImprint, nonce, certReq true értékkel, opcionálisan tartalmazza a reqPolicy, extensions adatokat
- Az időbélyeg válaszok ellenőrzése az RFC 3161-nek megfelelően történik
- Az időbélyeg válaszban a tartalmi és formai követelmények ellenőrzésre kerülnek
- Az időbélyeget aláíró tanúsítvány megismerése az időbélyeg válaszból történik
- Az időbélyeget szolgáltató TSA megbízhatóságának a megállapítása a Tanúsítási útvonal érvényesítése (CPV) – Alap csomaggal történik
- Az időbélyegen az aláírás a Tanúsítási útvonal érvényesítése (CPV) – Alap csomag kimenetéből származó nyilvános kulccsal kerül ellenőrzésre
- Az időbélyeget aláíró tanúsítvány extendedKeyUsage kiterjesztése ellenőrzésre kerül, ha azt tartalmazza, akkor abban a kulcshasználat céljának időbélyeg aláírásnak kell lennie
- A kapott időbélyeg válaszban a messageImprint, nonce, TSAPolicyID azonossága a küldött időbélyeg kéréssel ellenőrzésre kerül
- Az olyan időbélyeg válasz, amely fel nem dolgozott kritikus kiterjesztést tartalmaz, visszautasításra kerül.
- Az időbélyeg kérése a felhasználó nevében végrehajtott folyamat által meghatározott időpontban történik.
- XAdES v1.3.2 aláírás formátum esetén az időbélyegből az időbélyeg tok, a többi aláírás formátum esetén az időbélyeg válasz kerül az aláírásban elhelyezésre. Az ellenőrzés alatt álló aláírásban az időbélyeg elvárt tartalma XAdES v1.3.2 aláírás formátum esetén időbélyeg tok, a többi aláírás formátum esetén időbélyeg válasz. Amennyiben az időbélyeg tok formátuma az RFC 3161-nek megfelelő, feltételezésre kerül, hogy az egy olyan időbélyeg válaszból származik, amelyben a státusz granted.

37. táblázat: Az SF.TSP biztonsági funkció által lefedett biztonsági követelmények

FDP_DAU_TSP.1.1	A TSF-nek a PKIX RFC 3161-nek megfelelő formában kell összeállítania az időbélyeg kérést.
FDP_DAU_TSP.1.2	Az időbélyeg kérésnek a következő adatokat kell tartalmaznia a) kötelezően: verzió, messageImprint, nonce, certReq true értékkel, b) opcionálisan: reqPolicy, extensions.
FDP_DAU_TSP.1.3	A TSF-nek ellenőriznie kell, hogy a kapott időbélyeg válasz formátuma az PKIX RFC 3161-nek megfelelő.
FDP_DAU_TSP.1.4	A TSF-nek az időbélyeg válaszban a következő alap ellenőrzéseket kell elvégeznie: a) ha a státusz nem granted vagy grantedWithMods, akkor nem szerepelhet a válaszban TimeStampToken b) ha a státusz nem granted vagy grantedWithMods, akkor a válaszban szerepelnie kell PKIFailureInfo hiba információnak c) ha a státusz granted vagy grantedWithMods, akkor a válaszban szerepelnie kell TimeStampToken objektumnak d) ha a státusz granted vagy grantedWithMods, akkor a válaszban

kapott TimeStampToken tartalom típusa pkcs7-signedData kell, hogy legyen

e) ha a státusz granted vagy grantedWithMods, akkor a válaszban kapott SignedData tartalom típusa id-ct-TSPInfo kell, hogy legyen

FDP_DAU_TSP.1.5 A TSF-nek az időbélyeget aláíró tanúsítványt az időbélyeg válaszból kell megismernie.

FDP_DAU_TSP.1.6 A TSF-nek a TSA megbízhatóságának megállapítására tanúsítási útvonal érvényesség ellenőrzést kell végrehajtania a Tanúsítási útvonal érvényesítése (CPV) - Alap csomag felhasználásával.

FDP_DAU_TSP.1.7 A TSF-nek ellenőriznie kell az időbélyeg válasz aláírását a Tanúsítási útvonal érvényesítése (CPV) - Alap csomag kimenetéből származó nyilvános kulccsal.

FDP_DAU_TSP.1.8 A TSF-nek ellenőriznie kell, hogy ha az időbélyeget aláíró tanúsítvány tartalmazza az extendedKeyUsage kiterjesztést, akkor a kiterjesztés tartalmazza-e a PKIX OID-t időbélyeg aláírásra (id-kp-timeStamping).

FDP_DAU_TSP.1.9 A TSF-nek az időbélyeg válaszban a további ellenőrzéseket kell elvégeznie:

a) messageImprint azonosságát az időbélyeg kérés messageImprint értékkel
b) nonce azonosságát az időbélyeg kérés nonce értékkel
c) ha a kérés tartalmazott TSAPolicyId-t, akkor az azonos-e a válaszban kapott TSAPolicyId értékkel

FDP_DAU_TSP.1.10 A TSF-nek el kell utasítania az időbélyeg választ, ha a válasz olyan kritikus kiterjesztést tartalmaz, amelyet a TSF nem képes feldolgozni.

FDP_DAU_TSP.1.11 A TSF-nek az időbélyeg kérést abban az időpontban kell intéznie, amelyet a felhasználó nevében végrehajtott folyamat beállított.

FDP_DAU_TSP.1.12 A TSF-nek, amennyiben az aláírás formátuma XAdES v1.3.2 vagy „Egységes MELASZ formátum elektronikus aláírásokra” v2.0, az aláírásban az időbélyeg válaszból (TimeStampResp) kiemelt időbélyeg tokot (TimeStampToken) kell elhelyeznie. A TSF-nek, az ellenőrzés alatt álló aláírásban, amennyiben annak formátuma XAdES v1.3.2-nek vagy „Egységes MELASZ formátum elektronikus aláírásokra” v2.0-nak megfelelő, időbélyeg válasz helyett időbélyeg tokot kell elvárnia. Amennyiben az időbélyeg tok formátuma az RFC 3161-nek megfelelő, a TSF-nek fel kell tételeznie, hogy az időbélyeg tok egy olyan időbélyeg válaszból származik, amelyben a státusz granted.

Függőség: FCS_COP.1

6.1.10 Valós idejű tanúsítvány állapot protokoll (OCSP) kliens (SF.OCSP)

A biztonsági funkció két fő feladatköre:

- aláírás létrehozása vagy ellenőrzése során OCSP kérése az OCSP válaszadótól
- az OCSP válaszadótól kapott vagy az XML aláírásban fellelt OCSP választ ellenőrzi

A biztonsági funkció részletei, a biztonsági igények szempontjából:

- Az OCSP kérés összeállítása az RFC 2560-nak megfelelően történik
- Az OCSP kérés tartalmazza a nonce kiterjesztést
- Az OCSP választ aláíró tanúsítvány megismerése az OCSP válaszból történik
- Az OCSP válaszadó megbízhatósága a Tanúsítási útvonal érvényesítése (CPV) – Alap csomaggal kerül megállapításra
- Az OCSP válaszon az aláírás a CPV csomag kimenetéből származó nyilvános kulccsal ellenőrzésre kerül
- Az OCSP választ aláíró tanúsítvány extendedKeyUsage kiterjesztése ellenőrzésre kerül, ha azt tartalmazza, akkor abban a kulcshasználat céljának OCSP válasz aláírásnak vagy anyExtendedKeyUsage jelzésnek kell lennie
- Az OCSP válaszból a responderID összehasonlításra kerül az OCSP válaszadó tanúsítványában található megfelelő információval
- Az OCSP kérésből származó certID összehasonlításra kerül az OCSP válasz singleResponse-ból a certID-vel
- Az OCSP válasz aktuálisnak kerül elfogadásra az OCSPAfterProducedAtLimit ellenőrzés teljesülésekor
- Az OCSP válasz aktuálisnak kerül elfogadásra az OCSPAfterThisUpdateLimit ellenőrzés teljesülésekor
- Az OCSP válasz aktuálisnak kerül elfogadásra az OCSPAfterNextUpdateLimit ellenőrzés teljesülésekor
- Az OCSP válasz aktuálisnak kerül elfogadásra, ha az AHA folyamat felülbírálja a frissesség ellenőrzését
- Az OCSP válasz visszautasításra kerül, ha az fel nem dolgozott kritikus kiterjesztést tartalmaz
- Az OCSP válaszból a nonce egyeztetésre kerül az OCSP kérésben szereplő nonce értékével

38. táblázat: Az SF.OCSP biztonsági funkció által lefedett biztonsági követelmények

FDP_DAU_OCS.1.1	A TSF-nek a PKIX RFC 2560-nek megfelelő formában kell összeállítania az OCSP kérést.
FDP_DAU_OCS.1.2	Az OCSP kérésnek tartalmaznia kell a következő kiterjesztéseket: *nonce*.
FDP_DAU_OCS.1.3	A TSF-nek az OCSP választ aláíró tanúsítványt az OCSP válaszból kell megismernie.
FDP_DAU_OCS.1.4	A TSF-nek a következő további funkciókat kell végrehajtania: *az OCSP válaszadó megbízhatóságának megállapítása a Tanúsítási útvonal érvényesítése (CPV) - Alap csomag felhasználásával*
FDP_DAU_OCS.1.5	A TSF-nek ellenőriznie kell az OCSP válaszon levő aláírást a Tanúsítási útvonal érvényesítése (CPV) – Alap csomag kimenetéből származó nyilvános kulccsal.
FDP_DAU_OCS.1.6	A TSF-nek ellenőriznie kell, hogy ha az OCSP válaszadó tanúsítványa tartalmazza az extendedKeyUsage kiterjesztést, akkor a kiterjesztés tartalmazza-e az id-kp-OCSPSigning OID-t vagy az anyExtendedKeyUsage OID-t.
FDP_DAU_OCS.1.7	A TSF-nek össze kell hasonlítania az OCSP válaszból a responderID-t az OCSP válaszadó tanúsítványában található megfelelő információval.
FDP_DAU_OCS.1.8	A TSF-nek az OCSP kérésben található certID-t össze kell hasonlítania

	az OCSP válasz singleResponse-ban található certID-vel.
FDP_DAU_OCS.1.9	A TSF-nek aktuálisnak kell elfogadnia az OCSP választ minden bejegyzés tekintetében, ha az alábbi szabályzat érvényesül: *current-time <= producedAt + x, ahol x a felhasználó nevében végrehajtott folyamat által megadott érték*
FDP_DAU_OCS.1.10	A TSF-nek aktuálisnak kell elfogadnia az OCSP választ egy bejegyzés tekintetében, ha az alábbi szabályzat érvényesül: *current-time <= thisUpdate a bejegyzésből + x, ahol x a felhasználó nevében végrehajtott folyamat által megadott érték.*
FDP_DAU_OCS.1.11	A TSF-nek aktuálisnak kell elfogadnia az OCSP választ egy bejegyzés tekintetében, ha az alábbi szabályzat érvényesül: *current-time <= nextUpdate a bejegyzésből + x, ahol x a felhasználó nevében végrehajtott folyamat által megadott érték.*
FDP_DAU_OCS.1.12	A TSF-nek az OCSP választ aktuálisnak kell elfogadni, ha a *felhasználó nevében végrehajtott folyamat* felülbírálja a frissesség ellenőrzését.
FDP_DAU_OCS.1.13	A TSF-nek vissza kell utasítania az OCSP választ, ha az olyan kritikus kiterjesztést tartalmaz, amelyet a TSF nem dolgoz fel.
FDP_DAU_OCS.1.14	A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie: *nonce a kérésből = nonce a válaszból*
Függőség:	FCS_COP.1

6.2 Garanciális (biztosító) intézkedések

A fejlesztő a TOE fejlesztésénél biztosítja azokat a garancia összetevőket, amelyeket az EAL 3 + kiterjesztve az ALC_FLR.1 (A biztonsági rések alapszintű javítása) összetevővel értékelési garanciaszint előír.

6.2.1 Konfiguráció menedzselés

A konfiguráció menedzselés garancia osztályra vonatkozó a garanciális intézkedéseket a következő dokumentum tartalmazza:

- A2-Polysys_CM_Configuration_Management

6.2.2 Kiszállítás és üzemeltetés

A kiszállítás és üzemeltetés garancia osztályra vonatkozó garanciális intézkedéseket a következő dokumentum tartalmazza:

- A2-Polysys_DO_Delivery_and_Operation

6.2.3 Fejlesztés

A fejlesztés garancia osztályra vonatkozóan garanciális intézkedéseket a következő dokumentumok tartalmazzák:

- A2-Polysys_FS_Functional_Specification
- A2-Polysys_HLD_HighLevel_Design
- A2-Polysys CryptoSigno JAVA API [TOE verzió szám] (indító lap: *docs/API/index.html)*

ahol a [TOE verzió szám] jelölés a TOE verziószámát jelenti, pl. 2.0.0

6.2.4 Útmutató dokumentumok

Az útmutató dokumentumok garancia osztályra vonatkozó garanciális intézkedéseket a következő dokumentumok tartalmazzák:

- A2-Polysys_SG_Support_Guide
- A2-Polysys CryptoSigno JAVA API [TOE verzió szám] fejlesztői dokumentáció (indító lap: *docs/API/index.html)*
- A2-Polysys CryptoSigno JAVA API [TOE verzió szám] teszt esetek dokumentáció (indító lap: *docs/TEST/index.html)*

ahol a [TOE verzió szám] jelölés a TOE verziószámát jelenti, pl. 2.0.0

6.2.5 Életciklus támogatása

Jelen ST, az EAL3 kiterjesztése az ALC_FLR.1 (A biztonsági rések alapszintű javítása) életciklus támogatás összetevővel.

A Polysys egy átfogó életciklus támogató tervet használ a TOE fejlesztési eljárására és a TOE karbantartására. A Polysys a fejlesztési környezeten egy biztonsági felügyeletet alkalmaz, amely biztosítja a TOE bizalmasságát és integritását a tervezés és megvalósítás során. A Polysys egy

meghatározott eljárást alkalmaz a hibák azonosítására, nyomon követésére, leírására, javítására és egyéb javítási eseményekre.

Az életciklus támogatása garancia osztályra vonatkozóan garanciális intézkedéseket a következő dokumentum tartalmazza:

- A2-Polysys_MM_Modification_Management

6.2.6 Tesztek

A Polysys egy átfogó tesztelést támogató automatikus eljárást használ a TOE fejlesztési eredmények ellenőrzésére és a TOE karbantartására. A TOE fejlesztése során kialakított és alkalmazott tesztek három csoportba sorolhatóak:

- PKITS (Public Key Interoperability Public Key Interoperability Test Suite) típusú tesztek
- funkcionális tesztek
- kiegészítő tesztek

A PKITS és funkcionális tesztek teljesen automatikusan futtathatók.

A kiegészítő tesztek szükségességét az indokolja, hogy az A2-API MCV paradigma szerinti látvány elemeinek a tesztelése megtörténhessen. A TOE-val párhuzamosan kifejlesztésre került egy példa alkalmazás, gyakorlatilag egy lehetséges AHA, azaz A2-API-t használó alkalmazás, abból a célból, hogy az A2-API teljes funkcionalitását tesztelje.

A tesztek garancia osztályra vonatkozóan garanciális intézkedéseket a következő dokumentumok tartalmazzák:

- A2-Polysys_TG_Test_Guide
- A2-Polysys_TCD_Test_Coverage_Depth_Analysis
- A2-Polysys CryptoSigno JAVA API [TOE verzió szám] Test Cases (indító lap: *docs/TEST/index.html*)
- Unit Test Results (indító lap: *docs/html/junit/index.html*)

ahol a [TOE verzió szám] jelölés a TOE verziószámát jelenti, pl. 2.0.0

6.2.7 Sebezhetőség

A sebezhetőség garancia osztályra vonatkozóan garanciális intézkedést a következő dokumentum tartalmazza:

- A2-Polysys_VU_Vulnerability_Analysis

6.2.8 Garancia osztályok és dokumentumok összefüggései

Az alábbi táblázat részletezi az egyes garancia osztályokra vonatkozó garanciális intézkedések részletes, dokumentum szintű leképezését. Az életciklus támogatás dokumentációk sárga színnel jelölt sora jelzi az eredeti EAL 3 garancia szint kiterjesztését.

EAL3+			
garancia osztály	**értékelésre előírt dokumentum**		**kapcsolódó tényleges dokumentum címe**
	biztonsági előirányzat		A2-Polysys_ST_Security_Target
Konfiguráció kezelés dokumentáció			
ACM_CAP.3	Jogosultság ellenőrzések	a konfiguráció menedzselés dokumentáció-ja	A2-Polysys_CM_Configuration_Management
ACM_SCP.1	Minimális konfiguráció-kezelés lefedés		
Szállítás működtetés dokumentáció			
ADO_DEL.1	Szállítási dokumentáció		A2-Polysys_DO_Delivery_And_Operation
ADO_IGS.1	Installálás, generálás, rendszer indítás		A2-Polysys_SG_Support_Guide – 3-5. fejezet
Fejlesztési dokumentációk			
ADV_FPS.1	Informális funkcionális specifikáció		A2-Polysys_FS_Functional_Specification
ADV_HLD.2	Magas-szintű terv		A2-Polysys_HLD_HighLevel_Design
ADV_RCR.1	Megfeleltetés elemzés		A2-Polysys_ TCD_Test_Coverage_Depth_Analysis - 2. fejezet
Útmutató dokumentumok			
AGD_ADM.1	Adminisztrátori útmutató		A2-Polysys_SG_Support_Guide
AGD_USR.1	Felhasználói útmutató		
Életciklus támogatás dokumentáció			
ALC_DVS.1	A fejlesztési biztonság dokumentációja		A2-Polysys_CM_Configuration_Management - 7. fejezet
ALC_FLR.1	EAL 3 kiterjesztése		A2-Polysys_MM_Modification_Management
Tesztelési dokumentáció			
ATE_COV.2	Teszt lefedettség elemzése		A2-Polysys_ TCD_Test_Coverage_Depth_Analysis
ATE_DPT.1	Teszt mélység elemzése		
ATE_FUN.1	Funkcionális vizsgálat		
ATE_IND.2	Tesztelési dokumentáció		A2-Polysys_TG_Test_Guide
Sebezhetőség felmérése dokumentáció			
AVA_MSU.1	Az útmutatók helytelen használhatóságának elemzése		A2-Polysys _VU_Vulnerability_Analysis – 2. fejezet
AVA_SOF.1	Funkcióerősség elemzés		
AVA_VLA.1	Fejlesztői sebezhetőségi elemzés		

7 Védelmi profil (PP) nyilatkozatok (ASE_PPC)

7.1 PP hivatkozás

Jelen ST mindenben konform az alábbi PP-vel:

Cím: PKE PP (Public Key-Enabled Application Family of Protection Profiles)
with <
Certification Path Validation (CPV) – Basic,
PKI Signature Generation,
PKI Signature Verification,
PKI Encryption using Key Transfer Algorithms,
PKI Decryption using Key Transfer Algorithms,
Certificate Revocation List (CRL) Validation,
Online Certificate Status Protocol Client >
at EAL <3> with augmentation
Kiegészítve: Időbélyeg kliens csomaggal
Verzió: 2.5
Dátum: 2002.10.31

Az alábbi pontosításokkal:

- A PKE PP nem tartalmazott időbélyeg kliens csomagot. Jelen ST a PKE-PP szemléletének mindenben megfelelően kiegészítésre került egy időbélyeg kliens csomaggal, amelynek funkcionális követelményeit a szerzők úgy határozták meg, hogy az az RFC 3161 szabványnak megfeleljen.
- A PKE PP az 5.3.1 fejezetben lehetőséget nyújt arra, hogy a Tanúsítási útvonal érvényesítése (CPV) –Alap csomag függjön a Tanúsítvány visszavonási lista (CRL) érvényesítés csomagtól. Jelen ST ezt a csomagfüggést explicit módon kijelenti.
- A PKE PP az 1.5 (CC Conformance) fejezetében a CC 2.1 verzióval való megfelelőségre hivatkozik. A PKE PP az 5.1 (TOE Base Security Functional Requirements) fejezetben bevezeti az FMT_SMF (Specification of management function) családot, amely csak a CC 2.2 verzióban (CCIMB-2004-01-002) jelenik meg.
- A PKE PP 6. (Rationale) fejezet és annak alfejezeteinek megfelelő ST 8. (Indoklás) fejezet és annak alfejezeteinek szövegezése a PP-től eltér, az ST 5. (Az informatikai biztonság követelményei) fejezetben elvégzett kiválasztásoknak és értékadásoknak megfelelő a tartalma.
- Az PKE PP-hez képest az ST fejezeteinek számozása és sorrendje kismértékben eltér. Jelen ST fejezeteinek számozása és sorrendje a CC v2.2 1 kötet 48.oldal 11.ábrán megadott specifikációt követik.
- A PKE PP-hez képest az elektronikus aláírás (minősített, fokozott biztonságú) európai és magyar szabályozása miatt az ST eltér. Az AE.Crypto_Module feltételezés a TOE üzemmódjainak (szigorú, normál) megfelelően származtatva:
  - AE.Crypto_Module_Normal normál üzemmód – fokozott biztonságú elektronikus aláírás
  - AE.Crypto_Module_Rigid szigorú üzemmód - minősített elektronikus aláírás
- A PKE PP-hez képest az elektronikus aláírás (tanúsított, fokozott biztonságú) európai és magyar szabályozása miatt az ST eltér. Az OE.Crypto célkitűzés a TOE üzemmódjainak megfelelően származtatva:
  - OE.Crypto_Normal normál üzemmód – fokozott biztonságú elektronikus aláírás
  - OE.Crypto_Rigid szigorú üzemmód - minősített elektronikus aláírás
- A PKE PP-hez képest az elektronikus aláírás (tanúsított, fokozott biztonságú) európai és magyar szabályozása miatt az ST eltér. Az FCS_CRM_FPS.1.2 biztonsági funkcionális követelmény bővítésre került.
- A PKE PP FPT_STM1.1 biztonsági követelményét Megbízható időpontként értelmezik jelen ST szerzői.

7.2 PP illesztés

Jelen ST a PKE PP csomagválasztékából az alábbi csomagokat választotta:

Csomagnév	**Függés**
Certification Path Validation (CPV) – Basic	Certificate Revocation List (CRL) Validation
PKI Signature Generation	-
PKI Signature Verification	Certification Path Validation (CPV) – Basic
PKI Encryption using Key Transfer Algorithms	Certification Path Validation (CPV) – Basic
PKI Decryption using Key Transfer Algorithms	-
Certificate Revocation List (CRL) Validation	-
Online Certificate Status Protocol Client	Certification Path Validation (CPV) – Basic

Jelen ST-ben bevezetésre került az Időbélyeg kliens csomag.

Csomagnév	**Függés**
Időbélyeg kliens	Certification Path Validation (CPV) – Basic

Az Időbélyegző kliens csomag olyan módon lett meghatározva, hogy illeszkedjék a PKE PP csomag koncepciójához, azaz

- modulárisan magában foglalja az összes fenyegetést, célt, követelményt és magyarázatot
- a csomag összes összetevőjét fel kell venni, amennyiben a TOE legalább egy csomagon belüli funkcionalitást a csomagból igényel
- függésben áll a PKE PP a Certification Path Validation (CPV) – Basic csomagtól

7.3 PP kiegészítés

Jelen ST, a PKE PP-hez képest a TOE biztonsági céljaiban és követelményeiben kiegészítést tett az Időbélyeg kliens csomagban, amely eredetileg nem része a PKE PP nek.

A csomag funkcionális követelményei a CC 2. kötetének Felhasználói adatvédelem osztály (FDP), Adathitelesítés család (FDP_DAU) felhasználásával történt, amely egy olyan módszert biztosít, amely garantálja az adatok azon meghatározott egységének érvényességét, amely utólag felhasználható annak igazolására, hogy az információtartalom nem került meghamisításra vagy észrevétlen módosításra.

A funkcionális követelmények állításai az FDP_DAU.1 alapszintű adathitelesítés követelményeinek finomításával (refinement) lettek meghatározva úgy, hogy az PKIX RFC 3161 meghatározottak szerint, a TSF képes legyen előállítani az objektum információtartalma hitelességének garanciáját.

8 Indoklás

8.1 Biztonsági célkitűzések indoklása

Ez a fejezet tartalmazza a TOE és az informatikai környezet biztonsági célkitűzésének indoklását, csomagok szerinti bontásban. A TOE alap és informatikai környezet biztonsági célkitűzései együttesen lesz tárgyalva.

8.1.1 Alap és az informatikai környezet biztonsági célkitűzéseinek indoklása

Az alábbi táblázat az alap feltételezéseket és fenyegetéseket képezi le a célkitűzésekre, bemutatva azt, hogy az összes feltételezés és fenyegetés legalább egy célkitűzésre leképzésre került.

39. táblázat: A TOE alap és környezeti feltételezéseinek és fenyegetéseinek leképezése a célkitűzésekre

Feltételezések / Fenyegetések	Célkitűzések
AE.Authorized_Users	OE.Authorized_Users
AE.Configuration	OE.Configuration
AE.Crypto_Module_Normal	OE.Crypto_Normal
AE.Crypto_Module_Rigid	OE.Crypto_Rigid
AE.Low	OE.Low
AE.PKI_Info	OE.PKI_Info
AE.Physical_Protection	OE.Physical_Security
AE.Time	OE.Time
T.Attack	O.DAC
T.Bypass	O.Invoke
T.Imperson	O.I&A O.Limit_Actions_Auth
T.Modify	O.Self_Protect O.DAC O.Protect_I&A_Data O.Trust_Anchor O.TSF_Data
T.Object_Init	O.Init_Secure_Attr
T.Private_key	O.DAC
T.Role	O.Security_Roles
T.Secure_Attributes	O.Secure_Attributes
T.Shoulder_Surf	O.No_Echo
T.Tries	O.Limit_Tries

AE.Authorized_Users megállapítja: A jogosult felhasználók megbízhatóak a számukra kijelölt funkciók végrehajtására. Ez a feltételezés az alábbi célkitűzésre van leképezve:

- **OE.Authorized_Users** ami megállapítja: A jogosult felhasználók megbízhatóak, hogy végre hajtsák jogosult feladataikat.

AE.Configuration megállapítja: A TOE helyesen van installálva és konfigurálva. Ez a feltételezés az alábbi célkitűzésre van leképezve:

- **OE.Configuration** ami megállapítja: A TOE helyesen van installálva és configurálva, ahhoz, hogy a TOE biztonságos állapotban induljon.

AE.Crypto_Module_Normal megállapítja: A TOE környezetéről fel van tételezve, hogy tartalmaz egy vagy több kriptográfiai szolgáltatót (modult), amelyek megfelelnek a FIPS 140-1, 1.szintnek vagy magasabb szintnek. Ez a modul, vagy ezek a modulok alkalmazásra kerülnek a következő műveletek során: kulcs pár generálás, elektronikus aláírás és ellenőrzés, titkosítás, visszafejtés, biztonságos lenyomat képzés, véletlenszám generálás, lenyomat képzéses Message Authentication Code (HMAC) eljárás, és/vagy egyéb szükséges kriptográfiai funkciók. Összegezve: a TOE minden kriptográfiai modulja FIPS 140-1 sorozat,1. szint vagy magasabb szintnek megfelelő (compliant) kell legyen.

OE.Crypto_Normal ami megállapítja: A TOE környezetének tartalmaznia kell egy vagy több kriptográfiai szolgáltatót (modult), amelyek megfelelnek a FIPS 140-1 sorozat_1.szintnek vagy magasabb szintnek. Ez a modul, vagy ezek a modulok alkalmazásra kerülnek a következő műveletek során: kulcs pár generálás, elektronikus aláírás és ellenőrzés, titkosítás, visszafejtés, biztonságos lenyomat képzés, véletlenszám generálás, lenyomat képzéses Message Authentication Code (HMAC) eljárás, és/vagy egyéb szükséges kriptográfiai funkciók. Összegezve: a TOE minden kriptográfiai modulja FIPS 140 sorozat,1. szint vagy magasabb szintnek megfelelő (compliant) kell legyen.

AE.Crypto_Module_Rigid megállapítja: A TOE környezetéről fel van tételezve, hogy tartalmaz legalább kettő kriptográfiai szolgáltatót, amelyek közül az egyiket NHH minősítéssel rendelkező BALE biztosít.

a) A BALE kriptográfiai szolgáltatója alkalmazásra kerül a következő műveletek során: elektronikus aláírás, visszafejtés, biztonságos lenyomat képzés, véletlenszám generálás.
b) A FIPS 140-1 sorozat,1. szint vagy magasabb szintnek megfelelő (compliant) kriptográfiai szolgáltató alkalmazásra kerül a következő műveletek során: elektronikus aláírás ellenőrzése, titkosítás, lenyomat képzés, véletlenszám generálás (FIPS-140-2 compliant), lenyomat képzéses Message Authentication Code (HMAC) eljárás, és/vagy egyéb szükséges kriptográfiai funkciók.

Ez a feltételezés az alábbi célkitűzésre van leképezve:

- **OE.Crypto_Rigid** ami megállapítja: A TOE környezetének tartalmaznia kell legalább kettő kriptográfiai szolgáltatót, amelyek közül az egyiket NHH minősítéssel rendelkező BALE biztosít.
    a) A BALE kriptográfiai szolgáltatója alkalmazásra kerül a következő műveletek során: elektronikus aláírás, visszafejtés, biztonságos lenyomat képzés, véletlenszám generálás.
    b) A FIPS 140-1 sorozat,1. szint vagy magasabb szintnek megfelelő (compliant) kriptográfiai szolgáltató alkalmazásra kerül a következő műveletek során: elektronikus aláírás ellenőrzése, titkosítás, lenyomat képzés, véletlenszám generálás (FIPS-140-2 compliant), lenyomat képzéses Message Authentication Code (HMAC) eljárás, és/vagy egyéb szükséges kriptográfiai funkciók.

AE.Low megállapítja:A TOE támadási lehetősége alacsonynak van feltételezve. Ez a feltételezés az alábbi célkitűzésre van leképezve:

- **OE.Low** ami megállapítja: A TOE azonosítási és hitelesítési funkciói olyan minimálisan alacsony támadási lehetőségre vannak tervezve és megvalósítva, amint azt a sebezhetőségi értékelés és a funkció szilárdsági analízis (Strength of Function analyses) jóváhagyta.

AE.PKI_Info megállapítja: A TOE-nak tanúsítvány és tanúsítvány visszavonási lista információk a rendelkezésére állnak. Ez a feltételezés az alábbi célkitűzésre van leképezve:

- **OE.PKI_Info** ami megállapítja: Az informatikai környezetnek szolgáltatnia kell a TOE számára tanúsítványokat és a tanúsítvány visszavonási információkat.

AE.Physical_Protection megállapítja: A környezetnek gondoskodnia kell a fizikai biztonság egy elfogadható szintjéről azon célból, hogy a környezet a TOE-t ne befolyásolhassa vagy ne lehessen tárgya megkerülő csatorna támadásoknak, mint az erő analízis és idő analízis különböző formái. Ez a feltételezés az alábbi célkitűzésre van leképezve:

- **OE.Physical_Security** ami megállapítja: A környezetnek gondoskodnia kell a fizikai biztonság egy elfogadható szintjéről azon célból, hogy a környezet a TOE-t ne befolyásolhassa vagy ne lehessen tárgya megkerülő csatorna támadásoknak, mint az erő analízis és idő analízis különböző formái.

AE.Time megállapítja: A környezet gondoskodik a megfelelő pontosságú rendszeridőről, GMT formátumban. Ez a feltételezés az alábbi célkitűzésre van leképezve:

- **OE.Time** ami megállapítja: A környezetnek gondoskodnia kell az aktuális idő eléréséről, a megkövetelt pontosság szerinti, GMT formában.

T.Attack megállapítja: A TOE egy észre nem vett kompromittálódása azt eredményezheti, hogy egy (akár belső, akár külső) támadó megkísérelheti egy olyan tevékenység végrehajtását, amelyre nem jogosult. Ez a fenyegetés az alábbi célkitűzésre van leképezve:

- **O.DAC** ami megállapítja: A TSF ellenőrzi és korlátozza a felhasználó hozzáférését a TOE erőforrásaihoz, összhangban a meghatározott hozzáférés ellenőrzés szabályzattal.

T.Bypass megállapítja: Egy jogosulatlan magánszemély vagy felhasználó meghamisíthatja a biztonsági attributumokat vagy egyéb adatokat, a TOE biztonsági funkcióinak kikerülésére, és ezáltal a TOE erőforrásaihoz való jogosulatlan hozzáférésre. Ez a fenyegetés az alábbi célkitűzésre van leképezve:

- **O.Invoke** ami megállapítja: A TSF minden művelet során meghívásra kerül.

T.Imperson megállapítja: A jogosulatlan személy megszemélyesítheti a TOE-nak egy jogosult felhasználóját, és ezáltal hozzáférhet a TOE adataihoz, kulcsaihoz és műveleteihez. Ez a fenyegetés az alábbi célkitűzésekre vannak leképezve:

- **O.I&A** ami megállapítja: A TSF egyedileg azonosít minden felhasználót, és hitelesíti az igényelt személyazonosságot, mielőtt engedélyezné a felhasználó hozzáférését a TOE lehetőségeihez.
- **O.Limit_Actions_Auth** ami megállapítja: A TSF korlátozza a felhasználó által végezhető tevékenységeket, mielőtt a TSF ellenőrizné a felhasználó személyazonosságát.

T.Modify megállapítja: Egy támadó módosíthatja a TSF vagy felhasználói adatokat, pl. a biztonsági attributumokat, kulcsokat, azzal a céllal, hogy hozzáférjen TOE-hoz és annak erőforrásaihoz. Ez a fenyegetés az alábbi célkitűzésekre vannak leképezve:

- **O.Self_Protect** ami megállapítja, hogy a TSF karbantartja a saját végrehajtási környezetét, amely védi önmagát és erőforrásait a külső beavatkozásoktól, megmásítástól, jogosulatlan közzétételtől.
- **O.DAC** ami megállapítja: A TSF ellenőrzi és korlátozza a felhasználó hozzáférését a TOE erőforrásaihoz, összhangban a meghatározott hozzáférés ellenőrzés szabályzattal.

- **O.Protect_I&A_Data** ami megállapítja: A TSF csak jogosult felhasználó számára engedélyezi az I&A (a felhasználót azonosító) adatok megváltoztatását.
- **O.Trust_Anchor** ami megállapítja: A TSF csak jogosult felhasználó számára engedélyezi a megbízható legfelső szintű hitelesítő tanúsítványok menedzsmentjét.
- **O.TSF_Data** ami megállapítja: A TSF csak jogosult felhasználó számára engedélyezi a TSF adatok módosítását.

T.Object_Init megállapítja: Egy támadó jogosulatlan hozzáférést szerezhet egy objektumhoz annak létrejötte során, ha annak biztonsági attributumainak értékadása nem történt meg, vagy azt bárki el tudja végezni. Ez a fenyegetés az alábbi célkitűzésre van leképezve:

- **O.Init_Secure_Attr** ami megállapítja: A TSF-nek szolgáltatnia kell biztonsági attributumok érvényes alapértékeit, miközben egy objektum inicializálódik.

T.Private_key megállapítja: Egy támadó színlelheti a felhasználó személyazonosságát, olyan módon, hogy generálja vagy felhasználja a felhasználó magánkulcsát. Ez a fenyegetés az alábbi célkitűzésre van leképezve:

- **O.DAC** ami megállapítja: A TSF ellenőrzi és korlátozza a felhasználó hozzáférését a TOE erőforrásaihoz, összhangban a meghatározott hozzáférés ellenőrzés szabályzattal.

T.Role megállapítja: Egy felhasználó a számára engedélyezettnél több kiváltsággal rendelkező szerepet színlelhet, és kiterjesztett kiváltságokkal jogosulatlan tevékenységet végezhet. Ez a fenyegetés az alábbi célkitűzésre van leképezve:

- **O.Security_Roles** ami megállapítja: A TSF karbantartja a biztonsággal összefüggő szerepeket, és felhasználók kapcsolatát ezekhez a szerepekhez.

T.Secure_Attributes megállapítja: Egy felhasználó megváltoztathatja a biztonsági attributumait egy objektumnak, és ezáltal jogosulatlanul fér hozzá az objektumhoz. Ez a fenyegetés az alábbi célkitűzésre van leképezve:

- **O.Secure_Attributes** ami megállapítja: A TSF csak jogosult felhasználó számára engedélyezi a biztonsági attributumok megváltoztatását.

T.Shoulder_Surf megállapítja: Egy jogosulatlan felhasználó a jogosult felhasználó válla felett megfigyelheti a hitelesítési eljárást és elolvashatja a hitelesítési információkat. Ez a fenyegetés az alábbi célkitűzésre van leképezve:

- **O.No_Echo** ami megállapítja: A TSF nem jelez vissza hitelesítési információkat.

T.Tries megállapítja: Egy jogosulatlan személy próbálgatást és hibát kihasználva, találgatással meghatározhatja a hitelesítési információkat. Ez a fenyegetés az alábbi célkitűzésre van leképezve:

- **O.Limit_Tries** ami megállapítja: A TSF korlátozza az egymást követő sikertelen hitelesítési kísérleteket.

Az alábbi táblázatban a TOE alap és környezetei célkitűzései leképzésre kerülnek feltételezésekre és fenyegetésekre, azáltal bemutatva, hogy minden célkitűzés leképzésre került egy feltételezésre vagy fenyegetésre. A leképzések magyarázatai fentebb kerültek meghatározásra, ezért itt nem kerülnek megismétlésre. Megjegyzés: ezek a célkitűzések és fenyegetések minden csomag esetén szerepelnek.

40. táblázat: A TOE alap és az informatikai környezet célkitűzéseinek leképzése feltételezésekre és fenyegetésekre

Célkitűzések	Feltételezések / Fenyegetések
OE.Authorized_Users	AE.Authorized_Users
OE.Configuration	AE.Configuration
OE.Crypto_Normal	AE.Crypto_Module_Normal
OE.Crypto_Rigid	AE.Crypto_Module_Rigid
OE.Low	AE.Low
OE.Physical_Security	AE.Physical_Protection
OE.Time	AE.Time
O.DAC	T.Attack T.Modify T.Private_key
O.I&A	T.Imperson
O.Init_Secure_Attr	T.Object_Init
O.Invoke	T.Bypass
O.Limit_Actions_Auth	T.Imperson
O.Limit_Tries	T.Tries
O.No_Echo	T.Shoulder_Surf
O.Protect_I&A_Data	T.Modify
O.Secure_Attributes	T.Secure_Attributes
O.Security_Roles	T.Role
O.Self_Protect	T.Modify
O.Trust_Anchor	T.Modify
O.TSF_Data	T.Modify

8.1.2 A csomagok biztonsági célkitűzéseinek indoklása

8.1.2.1 Tanúsítási útvonal érvényesítése (CPV) – Alap csomag biztonsági célkitűzések indoklása

A következő táblázatok bemutatják a fenyegetések leképezését a célkitűzésekre a Tanúsítási útvonal érvényesítése (CPV) – Alap csomag esetén. A leképezést értelmező szöveg a táblázatot követi.

41. táblázat: A fenyegetések leképezése célkitűzésekre a Tanúsítási útvonal érvényesítése (CPV) – Alap csomag esetén

#	Fenyegetések	Célkitűzések
1	T.Certificate_Modi	O.Verified_Certificate
2	T.DOS_CPV_Basic	O.Availability
3	T.Expired_Certificate	O.Correct_Time O.Current_Certificate
4	T.Masquarade	O.Trusted_Keys
5	T.No_Crypto	O.Get_KeyInfo
6	T.Path_Not_Found	O.Path_Find
7	T.Revoked_Certificate	O.Valid_Certificate
8	T.User_CA	O.User

T.Certificate_Modi megállapítja: Egy nem megbízható felhasználó módosíthatja a tanúsítványt, ami azt eredményezi, hogy rossz nyilvános kulcs lesz használva. Ez a fenyegetés leképzésre kerül:

- **O.Verified_Certificate** ami megállapítja: A TSF csak ellenőrizhető aláírással ellátott tanúsítványokat fogad el.

T.DOS_CPV_Basic megállapítja: A visszavonási információ vagy a visszavonási információ elérése lehetetlenné válik, ami azt eredményezi, hogy a rendszer elveszíti a használhatóságát. Ez a fenyegetés leképzésre kerül:

- **O.Availability** ami megállapítja: A TSF biztosítja a biztonsági szolgáltatásokat, akkor is, ha a visszavonási információ nem áll rendelkezésre.

T.Expired_Certificate megállapítja: Egy lejárt (és esetleg visszavont) tanúsítvány felhasználható aláírás ellenőrzésre. Ez a fenyegetés leképzésre kerül:

- **O.Correct_Time** ami megállapítja: A TSF gondoskodik precíz átmeneti érvényesítési eredményekről.
- **O.Current_Certificate** ami megállapítja: A TSF csak akkor fogadja el a tanúsítványokat, ha azok nem jártak le.

T.Masquarade megállapítja: Egy nem megbízható entitás (CA) kiadhat tanúsítványokat ál (hamis) entitásoknak, megengedve azoknak, hogy színleljék más legitim felhasználók személyazonosságát. Ez a fenyegetés leképzésre kerül:

- **O.Trusted_Keys** ami megállapítja: A TSF megbízható nyilvános kulcsokat használ a tanúsítási útvonal érvényesítésénél.

T.No_Crypto megállapítja: A felhasználó nyilvános kulcsa és a kapcsolódó információk lehet, hogy nem állnak rendelkezésre a kriptográfiai funkció végrehajtására. Ez a fenyegetés leképzésre kerül:

- **O.Get_KeyInfo** ami megállapítja: A TSF szolgáltatja a felhasználó nyilvános kulcsát és a kapcsolódó információkat, azon célból, hogy végrehajtson kriptográfiai funkciókat.

T.Path_Not_Found megállapítja: A valós érvényesítési útvonal nem található meg, a rendszer működőképességének hiányában. Ez a fenyegetés leképzésre kerül:

- **O.Path_Find** ami megállapítja: A TSF képes lesz megtalálni a tanúsítási útvonalat a megbízható legfelső szintű hitelesítő tanúsítványtól az aláíróig.

T.Revoked_Certificate megállapítja: Egy visszavont tanúsítvány érvényesként felhasználható, és ez a biztonság veszélyeztetését eredményezi. Ez a fenyegetés leképzésre kerül:

- **O.Valid_Certificate** ami megállapítja: A TSF csak érvényes, azaz nem visszavont tanúsítványokat használ.

T.User_CA megállapítja: Egy felhasználó CA-ként léphet fel és jogosulatlan tanúsítványt adhat ki. Ez a fenyegetés leképzésre kerül:

- **O.User** ami megállapítja: A TSF csak CA által kiadott tanúsítványokat fogad el.

Az alábbi táblázat a célkitűzéseket képezi le a Tanúsítási útvonal érvényesítése (CPV) – Alap csomag fenyegetéseire. A leképzések magyarázatai fentebb kerültek meghatározásra, ezért itt nem kerülnek megismétlésre.

42. táblázat: A célkitűzéseket képezése fenyegetésekre a Tanúsítási útvonal érvényesítése (CPV) – Alap csomag esetén

#	Célkitűzések	Fenyegetések
1	O.Availability	T.DOS_CPV_Basic
2	O.Correct_Time	T.Expired_Certificate
3	O.Current_Certificate	T.Expired_Certificate
4	O.Get_KeyInfo	T.No_Crypto
5	O.Path_Find	T.Path_Not_Found
6	O.Trusted_Keys	T.Masquarade
7	O.User	T.User_CA
8	O.Verified_Certificate	T.Certificate_Modi
9	O.Valid_Certificate	T.Revoked_Certificate

8.1.2.2 PKI aláírás készítés csomag biztonsági célkitűzéseinek indoklása

A következő táblázatok bemutatják a fenyegetések leképezését a célkitűzésekre a PKI aláírás készítés csomag esetén. A leképezést értelmező szöveg a táblázatot követi.

43. táblázat: A fenyegetések leképezése célkitűzésekre a PKI aláírás készítés csomag esetén

#	Fenyegetés	Célkitűzés
1	T.Clueless_PKI_Sig	O.Give_Sig_Hints

T.Clueless_PKI_Sig megállapítja: A felhasználó útmutatás hiányában csak nem megfelelő tanúsítványokkal próbálkozik az aláírásnál. Ez a fenyegetés leképzésre kerül:

- **O.Give_Sig_Hints** ami megállapítja: A TSF útmutatást ad a helyes tanúsítány kiválasztására az aláírás ellenőrzésénél.

Az alábbi táblázat a célkitűzéseket képezi le a PKI aláírás készítés csomag fenyegetéseire. A leképzések magyarázatai fentebb kerültek meghatározásra, ezért itt nem kerülnek megismétlésre.

44. táblázat: A célkitűzések leképezése fenyegetésekre a PKI aláírás készítés csomag esetén

#	Célkitűzések	Fenyegetések
1	O.Give_Sig_Hints	T.Clueless_PKI_Sig

8.1.2.3 PKI aláírás ellenőrzés csomag biztonsági célkitűzéseinek indoklása

A következő táblázatok bemutatják a fenyegetések leképezését a célkitűzésekre a PKI aláírás ellenőrzés csomag esetén. A leképezést értelmező szöveg a táblázatot követi.

45. táblázat: A fenyegetések leképezése célkitűzésekre a PKI aláírás ellenőrzés csomag esetén

#	Fenyegetések	Célkitűzések
1	T.Assumed_Identity_PKI_Ver	O.Linkage_Sig_Ver
2	T.Clueless_PKI_Ver	O.Use_Sig_Hints

T.Assumed_Identity_PKI_Ver megállapítja: Egy felhasználó az aláíró személyére mást feltételezhet egy PKI aláírás ellenőrzése során. Ez a fenyegetés leképzésre kerül:

- **O.Linkage_Sig_Ver** ami megállapítja: A TSF a helyes felhasználói nyilvános kulcsot használja az aláírás ellenőrzésénél.

T.Clueless_PKI_Ver megállapítja: A felhasználó útmutatás hiányában csak a nem megfelelő tanúsítványokkal próbálkozik az aláírás ellenőrzésénél. Ez a fenyegetés leképzésre kerül:

- **O.Use_Sig_Hints** ami megállapítja: A TSF az útmutatást használja a helyes tanúsítvány kiválasztására az aláírás ellenőrzésénél.

Az alábbi táblázat a célkitűzéseket képezi le a PKI aláírás ellenőrzés csomag fenyegetéseire. A leképzések magyarázatai fentebb kerültek meghatározásra, ezért itt nem kerülnek megismétlésre.

46. táblázat: A célkitűzések leképezése fenyegetésekre a PKI aláírás ellenőrzés csomag esetén

#	Célkitűzések	Fenyegetések
1	O.Use_Sig_Hints	T.Clueless_PKI_Ver
2	O.Linkage_Sig_Ver	T.Assumed_Identity_PKI_Ver

8.1.2.4 PKI titkosítás kulcs átviteli algoritmusokkal csomag biztonsági célkitűzéseinek indoklása

A következő táblázatok bemutatják a fenyegetések leképezését a célkitűzésekre a PKI titkosítás kulcs átviteli algoritmusokkal csomag esetén. A leképezést értelmező szöveg a táblázatot követi.

47. táblázat: A fenyegetések leképezése célkitűzésekre a PKI titkosítás kulcs átviteli algoritmusokkal csomag esetén

#	Fenyegetések	Célkitűzések
1	T.Assumed_Identity_WO_En	O.Linkage_Enc_WO
2	T.Clueless_WO_En	O.Hints_Enc_WO

T.Assumed_Identity_WO_En megállapítja: Egy felhasználó a címzett személyére mást feltételezhet, egy kulcs átviteli algoritmussal végrehajtott titkosítás során. Ez a fenyegetés leképzésre kerül:

- **O.Linkage_Enc_WO** ami megállapítja: A TSF a helyes felhasználói nyilvános kulcsot használja a kulcsátvitel során.

T.Clueless_WO_En megállapítja: A felhasználó útmutatás hiányában csak nem megfelelő tanúsítványokkal próbálkozik a titkosítás végzésénél. Ez a fenyegetés leképzésre kerül:

- **O.Hints_Enc_WO** ami megállapítja: A TSF útmutatást ad a helyes tanúsítványok vagy kulcsok kiválasztására a PKI kulcs átviteli algoritmusokkal történő titkosításhoz.

Az alábbi táblázat a célkitűzéseket képezi le a PKI titkosítás kulcs átviteli algoritmusokkal csomag fenyegetéseire. A leképzések magyarázatai fentebb kerültek meghatározásra, ezért itt nem kerülnek megismétlésre.

48. táblázat: A célkitűzések leképezése fenyegetésekre a PKI titkosítás kulcs átviteli algoritmusokkal csomag esetén

#	Célkitűzések	Fenyegetések
1	O.Hints_Enc_WO	T.Clueless_WO_En
2	O.Linkage_Enc_WO	T.Assumed_Identity_WO_En

8.1.2.5 PKI visszafejtés kulcs átviteli algoritmusokkal csomag biztonsági célkitűzéseinek indoklása

A következő táblázatok bemutatják a fenyegetések leképezését a célkitűzésekre a PKI visszafejtés kulcs átviteli algoritmusokkal csomag esetén. A leképezést értelmező szöveg a táblázatot követi.

49. táblázat: A fenyegetések leképezése célkitűzésekre a PKI visszafejtés kulcs átviteli algoritmusokkal csomag esetén

#	Fenyegetések	Célkitűzések
1	T.Garble_WO_De	O.Correct_KT

T.Garble_WO_De megállapítja: A felhasználó nem a megfelelő kulcs átviteli algoritmust vagy nem a megfelelő magánkulcsot alkalmazhatja, ami az adatok összezagyválását eredményezi. Ez a fenyegetés leképzésre kerül:

- **O.Correct_KT** ami megállapítja: A TSF a megfelelő magánkulcsot és kulcsátviteli algoritmust használja.

Az alábbi táblázat a célkitűzéseket képezi le a PKI visszafejtés kulcs átviteli algoritmusokkal csomag fenyegetéseire. A leképzések magyarázatai fentebb kerültek meghatározásra, ezért itt nem kerülnek megismétlésre.

50. táblázat: A célkitűzések leképezése fenyegetésekre a PKI visszafejtés kulcs átviteli algoritmusokkal csomag esetén

#	Célkitűzések	Fenyegetések
1	O.Correct_KT	T.Garble_WO_De

8.1.2.6 Tanúsítvány visszavonási lista (CRL) érvényesítés csomag biztonsági célkitűzések indoklása

A következő táblázatok bemutatják a fenyegetések leképezését a célkitűzésekre a Tanúsítvány visszavonási lista (CRL) érvényesítés csomag esetén. A leképezést értelmező szöveg a táblázatot követi.

51. táblázat: A fenyegetések leképezése célkitűzésekre a Tanúsítvány visszavonási lista (CRL) érvényesítés csomag esetén

#	Fenyegetések	Célkitűzések
1	T.DOS_CRL	O.User_Override_Fresh_CRL
2	T.Replay_Revoc_Info_CRL	O.Fresh_Rev_Info
3	T.Wrong_Revoc_Info_CRL	O.Accurate_Rev_Info O.Auth_Rev_Info

T.DOS_CRL megállapítja: A CRL vagy a CRL hozzáférés elérhetetlenné válik és emiatt a rendszer elveszíti a rendelkezésre állását. Ez a fenyegetés leképzésre kerül:

- **O.User_Override_Fresh_CRL** ami megállapítja: A TSF engedélyezi a felhasználónak, hogy hatástalanítsa a CRL frissességének követelményét.

T.Replay_Revoc_Info_CRL megállapítja: A felhasználó elfogadhat egy régi CRL-t, ami egy már visszavont tanúsítvány elfogadását eredményezheti. Ez a fenyegetés leképzésre kerül:

- **O.Fresh_Rev_Info** ami megállapítja: A TSF csak megfelelően időszerű CRL-t fogad el.

T.Wrong_Revoc_Info_CRL megállapítja: A felhasználó elfogadhat egy visszavont tanúsítványt vagy visszautasíthat egy érvényes tanúsítványt, egy rossz CRL miatt. Ez a fenyegetés leképzésre kerül:

- **O.Accurate_Rev_Info** ami megállapítja: A TSF csak pontos visszavonási információkat fogad el.
- **O.Auth_Rev_Info** ami megállapítja: A TSF a visszavonási információkat jogosult CRL forrásból fogadja el.

Az alábbi táblázat a célkitűzéseket képezi le a Tanúsítvány visszavonási lista (CRL) érvényesítés csomag fenyegetéseire. A leképzések magyarázatai fentebb kerültek meghatározásra, ezért itt nem kerülnek megismétlésre.

52. táblázat: A célkitűzések leképezése fenyegetésekre a Tanúsítvány visszavonási lista (CRL) érvényesítés csomag esetén

#	Célkitűzések	Fenyegetések
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
4	O.User_Override_Fresh_CRL	T.DOS_CRL

8.1.2.7 Időbélyeg kliens csomag biztonsági célkitűzések indoklása

A következő táblázatok bemutatják a fenyegetések leképezését a célkitűzésekre az Időbélyeg kliens csomag esetén. A leképezést értelmező szöveg a táblázatot követi.

53. táblázat: A fenyegetések leképezése célkitűzésekre az Időbélyeg kliens csomag esetén

#	Fenyegetések	Célkitűzések
1	T.DOS_TSP	O.User_Decide_TSP
2	T.Replay_TSP_Info	O.Fresh_TSP_Info
3	T.Wrong_TSP_Info	O.Accurate_TSP_Info O.Auth_TSP_Info

T.DOS_TSP megállapítja: Az időbélyeg válasz vagy az időbélyeg szolgáltatáshoz való hozzáférés elérhetetlenné válik és emiatt a rendszer elveszíti a rendelkezésre állását. Ez a fenyegetés leképzésre kerül:

- **O.User_Decide_TSP:** A TSF engedélyezi a felhasználónak, annak meghatározását, hogy mikor történjen az időbélyeg kérés.

T.Replay_TSP_Info megállapítja: A felhasználó elfogadhat egy régi időbélyeg választ, ami egy már visszavont tanúsítvány elfogadását eredményezheti. Ez a fenyegetés leképzésre kerül:

- **O.Fresh_TSP_Info:** A TSF mindig új időbélyeg kérést küld és csak az arra adott időbélyeg választ fogadja el.

T.Wrong_TSP_Info megállapítja: A felhasználó elfogadhat egy visszavont tanúsítványt vagy visszautasíthat egy érvényes tanúsítványt, egy rossz időbélyeg válasz miatt. Ez a fenyegetés leképzésre kerül:

- **O.Accurate_TSP_Info:** A TSF csak pontos időbélyeg választ fogad el.
- **O.Auth_TSP_Info:** A TSF az időbélyeg válaszokat csak jogosult TSA forrásból fogadja el.

Az alábbi táblázat a célkitűzéseket képezi le az Időbélyeg kliens csomag fenyegetéseire. A leképzések magyarázatai fentebb kerültek meghatározásra, ezért itt nem kerülnek megismétlésre.

54. táblázat: A célkitűzések leképezése fenyegetésekre az Időbélyeg kliens csomag esetén

#	Célkitűzések	Fenyegetések
1	O.User_Decide_TSP	T.DOS_TSP
2	O.Fresh_TSP_Info	T.Replay_TSP_Info
3	O.Accurate_TSP_Info	T.Wrong_TSP_Info
4	O.Auth_TSP_Info	

8.1.2.8 Valós idejű tanúsítvány állapot protokoll (OCSP) kliens csomag biztonsági célkitűzések indoklása

A következő táblázatok bemutatják a fenyegetések leképezését a célkitűzésekre a valós idejű tanúsítvány állapot protokoll (OCSP) kliens csomag esetén. A leképezést értelmező szöveg a táblázatot követi.

55. táblázat: A fenyegetések leképezése célkitűzésekre az OCSP kliens csomag esetén

#	Fenyegetések	Célkitűzések
1	T.DOS_OCSP	O.User_Override_Fresh_OCSP
2	T.Replay_OCSP_Info	O.Fresh_OCSP_Info
3	T.Wrong_OCSP_Info	O.Accurate_TSP_Info O.Auth_TSP_Info

T.DOS_OCSP megállapítja: Az OCSP válasz vagy az OCSP szolgáltatáshoz való hozzáférés elérhetetlenné válik és emiatt a rendszer elveszíti a rendelkezésre állását. Ez a fenyegetés leképzésre kerül:

- **O.User_Override_Fresh_OCSP:** A TSF engedélyezi a felhasználónak, hogy felülbíráljsa az OCSP válasz frissességének ellenpőrzését.

T.Replay_OCSP_Info megállapítja: A felhasználó elfogadhat egy régi OCSP választ, ami egy már visszavont tanúsítvány elfogadását eredményezheti. Ez a fenyegetés leképzésre kerül:

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

T.Wrong_TSP_Info megállapítja: A felhasználó elfogadhat egy visszavont tanúsítványt vagy visszautasíthat egy érvényes tanúsítványt, egy rossz OCSP válasz miatt. Ez a fenyegetés leképzésre kerül:

- **O.Accurate_TSP_Info:** A TSF csak pontos OCSP választ fogad el.
- **O.Auth_TSP_Info:** A TSF a visszavonási infromációkat csak jogosult OCSP forrásból fogadja el.

Az alábbi táblázat a célkitűzéseket képezi le az OCSP kliens csomag fenyegetéseire. A leképzések magyarázatai fentebb kerültek meghatározásra, ezért itt nem kerülnek megismétlésre.

56. táblázat: A célkitűzések leképezése fenyegetésekre az OCSP kliens csomag esetén

#	Célkitűzések	Fenyegetések
1	O.User_Override_Fresh_OCSP	T.DOS_OCSP
2	O.Fresh_OCSP_Info	T.Replay_OCSP_Info
3	O.Accurate_OCSP_Info	T.Wrong_OCSP_Info
4	O.Auth_OCSP_Info	

8.2 Biztonsági követelmények indoklása

Ez a fejezet a célkitűzéseket képezi le a biztonsági funkcionális követelményekre és az indoklás az EAL 3+ kibővített szintnek megfelelő.

8.2.1 Biztonsági funkcionális követelmények indoklása

Az összes célkitűzés leképzésre kerül a biztonsági funkcionális követelményekre (komponensekre) vagy a feltételezésekre az alábbi összefoglaló táblázatban. A TOE alap biztonsági funkcionális követelményei és a csomagok biztonsági funkcionális követelményei különböző altáblázatokba kerülnek a leképezés során.

57. táblázat: Biztonsági célkitűzések leképezése funkcionális követelményekre

#	Célkitűzések	Funkcionális követelmény
TOE célkitűzéseinek leképezése		
1	O.DAC	FDP_ACC.1 FDP_ACF.1
2	O.Invoke	FPT_RVM.1
3	O.I&A	FIA_ATD.1 FIA_UAU.1 FIA_UID.1
4	O.Init_Secure_Attr	FMT_MSA.3
5	O.Limit_Actions_Auth	FIA_UAU.1 FIA_UID.1
6	O.Limit_Tries	FIA_AFL.1
7	O.No_Echo	FIA_UAU.7
8	O.Protect_I&A_Data	FMT_MTD.1 FMT_SMF.1
9	O.Secure_Attributes	FMT_MSA.1 FMT_SMF.1
10	O.Security_Roles	FMT_SMR.2
11	O.Self_Protect	FPT_SEP.1
12	O.Trust_Anchor	FMT_MTD.1 FMT_SMF.1
13	O.TSF_Data	FMT_MTD.1 FMT_SMF.1
Az informatikai környezet célkitűzéseinek leképezése		
1	OE.Authorized_Users	AGD_ADM.1 Adminisztrátori útmutató AGD_USR.1 Felhasználói útmutató
2	OE.Configuration	ADO_IGS.1 Installálás, generálás, rendszer indítás
3	OE.Crypto_Normal	FCS_CRM_FPS.1 Kriptográfiai modulok FIPS szerinti megfelelősége
4	OE.Crypto_Rigid	FCS_CRM_FPS.1 Kriptográfiai modulok FIPS szerinti megfelelősége
5	OE.Low	AVA_SOF.1 A TOE biztonsági funkciók erejének értékelése AVA_VLA.1 A fejlesztői sebezhetőség elemzése
6	OE.Physical_Security	AGD_ADM.1 Adminisztrátori útmutató AGD_USR.1 Felhasználói útmutató

7	OE.PKI_Info	FDP_ITC_PKI_INF.1 PKI információk importálása a TSF ellenőrzésén kívülről
8	OE.Time	FPT_STM.1 Megbízható időpont
Tanúsítási útvonal érvényesítése (CPV) – Alap csomag leképezése		
1	O.Availability	FDP_DAU_CPV_CER.1
2	O.Correct_Time	FDP_DAU_CPV_INI.1
3	O.Current_Certificate	FDP_DAU_CPV_CER.1
3	O.Get_KeyInfo	FDP_DAU_CPV_OUT.1
5	O.Path_Find	FDP_CPD.1
6	O.Trusted_Keys	FDP_DAU_CPV_INI.1
7	O.User	FDP_DAU_CPV_CER.2
8	O.Verified_Certificate	FDP_DAU_CPV_CER.1
9	O.Valid_Certificate	FDP_DAU_CPV_CER.1
PKI aláírás készítés csomag leképezése		
1	O.Give_Sig_Hints	FDP_ETC_SIG.1
PKI aláírás ellenőrzés csomag leképezése		
1	O.Use_Sig_Hints	FDP_ITC_SIG.1
2	O.Linkage_Sig_Ver	FDP_DAU_SIG.1
PKI titkosítás kulcs átviteli algoritmusokkal csomag leképezése		
1	O.Hints_Enc_WO	FDP_ETC_ENC.1
2	O.Linkage_Enc_WO	FDP_ETC_ENC.1 FDP_DAU_ENC.1
PKI visszafejtés kulcs átviteli algoritmusokkal csomag leképezése		
2	O.Correct_KT	FDP_ITC_ENC.1
Tanúsítvány visszavonási lista (CRL) érvényesítés csomag 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
4	O.User_Override_Fresh_CRL	FDP_DAU_CRL.1
Időbélyeg kliens csomag leképezése		
1	O.Accurate_TSP_Info	FDP_DAU_TSP.1
2	O.Auth_TSP_Info	FDP_DAU_TSP.1
3	O.Fresh_TSP_Info	FDP_DAU_TSP.1
4	O.User_Decide_TSP	FDP_DAU_TSP.1
Valós idejű tanúsítvány állapot protokoll (OCSP) kliens csomag 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
4	O.User_Override_Fresh_OCSP	FDP_DAU_OCS.1

8.2.1.1 TOE alap biztonsági követelményeinek indoklása

O.DAC megállapítja: A TSF ellenőrzi és korlátozza a felhasználó hozzáférését a TOE erőforrásaihoz, összhangban a meghatározott hozzáférés ellenőrzés szabályzattal. Ez a biztonsági célkitűzés találkozik a következő funkciókkal:

- **FDP_ACC.1.1** A TSF-nek érvényesítenie kell a PKI megbízólevél menedzsment SFP-t a
  a) Szubjektum: felhasználó nevében végrehajtott folyamat
  b) Objektum: adat, amely a TOE számára átadásra kerül a kriptográfiai művelet végzéséhez, vagy amelyet a TOE ad át tárolásra, vagy egyéb használatra
  c) Művelet: a TOE által biztosított kriptográfiai művelet, a TOE működését vezérlő paraméterek beállítása/lekérdezése

  között.
- **FDP_ACF.1.1** A TSF-nek érvényesítenie kell a PKI megbízólevél menedzsment SFP-t olyan objektumokon, amelyek a szubjektum azonosságán és egy olyan szerep halmazon alapul, amelyet a szubjektum jogosult felvenni.
- **FDP_ACF.1.2** A TSF-nek érvényesítenie kell az alábbi szabályokat, hogy megállapíthassa, engedélyezett-e a művelet az ellenőrzött szubjektumok és objektumok között:
  a) Magánkulcs importálható, használható, a felhasználó nevében végrehajtott folyamatok által.
  b) Nyilvános kulcsú tanúsítványok importálhatók, exportálhatók, törölhetők a felhasználó nevében végrehajtott folyamatok által.
  c) Nyilvános kulcsú tanúsítványok használhatók a felhasználó nevében végrehajtott folyamatok által.
  d) Titkos kulcs generálható, megsemmisíthető, használható a felhasználó nevében végrehajtott folyamatok által.
  e) Titkos kulcs kizárólag aszimmetrikus titkosítással csomagolva importálható és exportálható.
- **FDP_ACF.1.3** A TSF-nek félreérthetetlenül hitelesítenie kell a szubjektumoknak az objektumokhoz való hozzáférését, amely az alábbi kiegészítő szabályokon alapul: nincs további szabály.
- **FDP_ACF.1.4** A TSF-nek félreérthetetlenül meg kell tagadnia a szubjektumoknak az objektumokhoz való azon hozzáférést, ha az I&A (a felhasználót azonosító) adatokat tároló eszköz (kulcstároló) az adott pillanatban nem elérhető.

O.Invoke megállapítja: A TSF minden művelet során meghívásra kerül. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FPT_RVM.1** TSF-nek biztosítania kell, hogy a TSP kényszerítő funkciói meghívásra kerülnek és sikeresen végrehajtódnak, mielőtt minden egyes TSF irányítási tárgykör (TSC) funkció továbbhaladása engedélyeződne.

O.I&A megállapítja: A TSF egyedileg azonosít minden felhasználót, és hitelesíti az igényelt személyazonosságot, mielőtt engedélyezné a felhasználó hozzáférését a TOE lehetőségeihez. Ez a biztonsági célkitűzés találkozik a következő funkciókkal:

- **FIA_ATD.1.1** A TSF-nek karban kell tartania az alábbi biztonsági attributum-listát, amely különálló felhasználókhoz tartozik: az I&A (a felhasználót azonosító) adatokat tároló eszköz (kulcstároló) jellemzői.
- **FIA_UAU.1.1** A TSF-nek lehetővé kell tenni a használó alkalmazás által konfigurálható paraméterek átadását a felhasználó nevében, mielőtt a felhasználó hitelesítésre kerül.
- **FIA_UAU.1.2** A TSF-nek meg kell követelnie, hogy minden egyes felhasználó sikeresen hitelesítve legyen, mielőtt bármelyik másik TSF által közvetített tevékenységet engedélyezne annak a felhasználónak a nevében.
- **FIA_UID.1.1** A TSF-nek lehetővé kell tennie a használó alkalmazás által konfigurálható paraméterek átadását a felhasználó nevében, mielőtt a felhasználó azonosítása megtörténik.

- **FIA_UID.1.2** A TSF-nek meg kell követelnie minden egyes felhasználó sikeres azonosítását, mielőtt bármelyik másik, TSF által közvetített tevékenységet engedélyez annak a felhasználónak a nevében.

O.Init_Secure_Attr megállapítja: A TSF-nek szolgáltatnia kell biztonsági attributumok érvényes alapértékeit, miközben egy objektum inicializálódik. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FMT_MSA.3.1** A TSF-nek érvényesítenie kell a PKI megbízólevél menedzsment SFP-t, hogy biztosítsa a megfelelő alapértelmezett értékeket a biztonsági attributumok számára, amelyek az SFP végrehajtásakor használatosak.
- **FMT_MSA.3.2** A TSF-nek lehetővé kell tennie a felhasználó nevében végrehajtott folyamat számára a lehetséges kezdeti értékek meghatározását abból a célból, hogy felülírja az alapértékeket, amikor egy objektum vagy információ készül.

O.Limit_Actions_Auth megállapítja: A TSF korlátozza a felhasználó által végezhető tevékenységeket, mielőtt a TSF ellenőrizné a felhasználó személyazonosságát. Ez a biztonsági célkitűzés találkozik a következő funkciókkal:

- **FIA_UAU.1.1** A TSF-nek lehetővé kell tenni a használó alkalmazás által konfigurálható paraméterek átadását a felhasználó nevében, mielőtt a felhasználó hitelesítésre kerül.
- **FIA_UAU.1.2** A TSF-nek meg kell követelnie, hogy minden egyes felhasználó sikeresen hitelesítve legyen, mielőtt bármelyik másik TSF által közvetített tevékenységet engedélyezne annak a felhasználónak a nevében.
- **FIA_UID.1.1** A TSF-nek lehetővé kell tennie a használó alkalmazás által konfigurálható paraméterek átadását a felhasználó nevében, mielőtt a felhasználó azonosítása megtörténik.
- **FIA_UID.1.2** A TSF-nek meg kell követelnie minden egyes felhasználó sikeres azonosítását, mielőtt bármelyik másik, TSF által közvetített tevékenységet engedélyez annak a felhasználónak a nevében.

O.Limit_Tries megállapítja: A TSF korlátozza az egymást követő sikertelen hitelesítési kísérleteket.

- **FIA_AFL.1.1** A TSF-nek észlelnie kell, amikor a használó alkalmazás által konfigurálható számú sikertelen hitelesítési próbálkozás fordul elő a kijelölt felhasználó azonosság hitelesítésére irányuló utolsó sikeres próbálkozás óta végbement sikertelen hitelesítési próbálkozásokat illetően.
- **FIA_AFL.1.2** Amikor a sikertelen hitelesítési próbálkozások száma elér vagy meghalad egy meghatározott számot, a TSF-nek a TOE képességeinek igénybevételét a használó alkalmazás számára meg kell tagadnia.

O.No_Echo megállapítja: A TSF nem jelez vissza hitelesítési információkat. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FIA_UAU.7.1** A TSF-nek csak a begépelt karaktereknek csak a * (csillag) mintával történő visszajelzését kell biztosítania a felhasználó számára, mialatt a hitelesítés folyamatban van.

O.Protect_I&A_Data megállapítja: A TSF csak jogosult felhasználó számára engedélyezi az I&A (a felhasználót azonosító) adatok megváltoztatását. Ez a biztonsági célkitűzés találkozik a következő funkciókkal:

- **FMT_MTD.1.1** A TSF-nek korlátoznia kell a: megváltoztatását, törlését, üresítését, importálását, hozzáadását, a megbízható legfelső szintű hitelesítő tanúsítványok, közbenső szintű hitelesítő tanúsítványok, saját tanúsítványok, más személyek tanúsítványai, tanúsítvány visszavonási listák, a CRL a kibocsátást követően hány napig aktuális, a CRL a következő kibocsátást követő hány napig aktuális, CRL frissesség ellenőrzés engedélyezése, visszavonás ellenőrzés kihagyhatóság engedélyezése, megbízható időszerverek, szolgáltatás igénybevétele utáni kényszerített kijelentkeztetés

engedélyezése, OCSP válasz az előállítást követő hány percig aktuális, OCSP válasz a kibocsátást követő hány percig aktuális, OCSP válasz a következő kibocsátást követő hány percig aktuális, OCSP válasz frissesség ellenőrzés engedélyezése, időbélyeg szolgáltatás elérhetősége, OCSP szolgáltatás elérhetősége, szervezeti aláírási szabályzat a felhasználó nevében végrehajtott folyamatokra.

- **FMT_SMF.1.1** A TSF-nek alkalmasnak kell lennie arra, hogy végrehajtsa következő biztonsági menedzsment funkciókat:
    a) a használó alkalmazás által konfigurálható paraméterek importálását
    b) önellenőrzés
    c) azonosítás, hitelesítés és jogosultság ellenőrzés, a felhasználó bejelentkeztetése a kulcstárolóhoz
    d) a következő biztonsági attributumok menedzsmentje:
        - megbízható legfelső szintű hitelesítő tanúsítványok,
        - közbenső szintű hitelesítő tanúsítványok
        - saját tanúsítványok
        - más személyek tanúsítványai
        - tanúsítvány visszavonási listák
        - a CRL a kibocsátást követően hány napig aktuális
        - a CRL a következő kibocsátást követő hány napig aktuális
        - CRL frissesség ellenőrzés engedélyezése
        - visszavonás ellenőrzés kihagyhatóság engedélyezése
        - megbízható időszerverek
        - szolgáltatás igénybevétele utáni kényszerített kijelentkeztetés engedélyezése
        - OCSP válasz az előállítást követő hány percig aktuális
        - OCSP válasz a kibocsátást követő hány percig aktuális
        - OCSP válasz a következő kibocsátást követő hány percig aktuális
        - OCSP válasz frissesség ellenőrzés engedélyezése
        - időbélyeg szolgáltatás elérhetősége
        - OCSP szolgáltatás elérhetősége
        - szervezeti aláírási szabályzat
    e) tanúsítási útvonal érvényesítés
    f) CRL érvényesítés
    g) elektronikus aláírás létrehozása és ellenőrzése
    h) titkosítás és visszafejtés
    i) időbélyeg kérés és ellenőrzés
    j) OCSP kérés és ellenőrzés

O.Secure_Attributes megállapítja: A TSF csak jogosult felhasználó számára engedélyezi a biztonsági attributumok megváltoztatását. Ez a biztonsági célkitűzés találkozik a következő funkciókkal:

- **FMT_MSA.1.1** A TSF-nek érvényre kell juttatnia a PKI megbízólevél menedzsment SFP-t, hogy korlátozza: a lekérdezését, megváltoztatását, törlését, kiválasztását a következő vezérlő biztonsági attributumoknak: az I&A (a felhasználót azonosító) adatok, TOE működését vezérlő paraméterek, kriptográfiai műveleteket befolyásoló paraméterek, az azonosított és hitelesített felhasználó nevében végrehajtott folyamatokra.
- **FMT_SMF.1.1** A TSF-nek alkalmasnak kell lennie arra, hogy végrehajtsa következő biztonsági menedzsment funkciókat:
    a) a használó alkalmazás által konfigurálható paraméterek importálását
    b) önellenőrzés
    c) azonosítás, hitelesítés és jogosultság ellenőrzés, a felhasználó bejelentkeztetése a kulcstárolóhoz
    d) a következő biztonsági attributumok menedzsmentje:
        - megbízható legfelső szintű hitelesítő tanúsítványok,
        - közbenső szintű hitelesítő tanúsítványok

- saját tanúsítványok
- más személyek tanúsítványai
- tanúsítvány visszavonási listák
- a CRL a kibocsátást követően hány napig aktuális
- a CRL a következő kibocsátást követő hány napig aktuális
- CRL frissesség ellenőrzés engedélyezése
- visszavonás ellenőrzés kihagyhatóság engedélyezése
- megbízható időszerverek
- szolgáltatás igénybevétele utáni kényszerített kijelentkeztetés engedélyezése
- OCSP válasz az előállítást követő hány percig aktuális
- OCSP válasz a kibocsátást követő hány percig aktuális
- OCSP válasz a következő kibocsátást követő hány percig aktuális
- OCSP válasz frissesség ellenőrzés engedélyezése
- időbélyeg szolgáltatás elérhetősége
- OCSP szolgáltatás elérhetősége
- szervezeti aláírási szabályzat

e) tanúsítási útvonal érvényesítés
f) CRL érvényesítés
g) elektronikus aláírás létrehozása és ellenőrzése
h) titkosítás és visszafejtés
i) időbélyeg kérés és ellenőrzés
j) OCSP kérés és ellenőrzés

O.Security_Roles megállapítja: A TSF karbantartja a biztonsággal összefüggő szerepeket, és felhasználók kapcsolatát ezekhez a szerepekhez. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FMT_SMR.2.1** A TSF-nek karban kell tartania a következő szerepeket: felhasználó nevében végrehajtott folyamat.
- **FMT_SMR.2.2** A TSF-nek képesnek kell lennie felhasználók és szerepek összerendelésére.
- **FMT_SMR.2.3** A TSF-nek biztosítania kell, hogy a felhasználó nevében végrehajtott folyamatok feltételei ki legyenek elégítve.

O.Self_Protect megállapítja: A TSF karbantartja a saját végrehajtási környezetét, amely védi önmagát és erőforrásait a külső beavatkozásoktól, megmásítástól, jogosulatlan közzétételtől. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FPT_SEP.1.1** A TSF-nek fenn kell tartania a saját végrehajtása számára egy biztonsági körzetet, amely védelmet nyújt a nem megbízható szubjektumok általi beavatkozás és meghamisítás ellen.
- **FPT_SEP.1.2** A TSF-nek érvényesítenie kell a TSC szubjektumainak biztonsági körzeteinek egymástól való elkülönítését.

O.Trust_Anchor megállapítja: A TSF csak jogosult felhasználó számára engedélyezi a megbízható legfelső szintű hitelesítő tanúsítványok menedzsmentjét. Ez a biztonsági célkitűzés találkozik a következő funkciókkal:

- **FMT_MTD.1.1** A TSF-nek korlátoznia kell a: megváltoztatását, törlését, üresítését, importálását, hozzáadását, a megbízható legfelső szintű hitelesítő tanúsítványok, közbenső szintű hitelesítő tanúsítványok, saját tanúsítványok, más személyek tanúsítványai, tanúsítvány visszavonási listák, a CRL a kibocsátást követően hány napig aktuális, a CRL a következő kibocsátást követő hány napig aktuális, CRL frissesség ellenőrzés engedélyezése, visszavonás ellenőrzés kihagyhatóság engedélyezése, megbízható időszerverek, szolgáltatás igénybevétele utáni kényszerített kijelentkeztetés engedélyezése, OCSP válasz az előállítást követő hány percig aktuális, OCSP válasz a kibocsátást követő hány percig aktuális, OCSP válasz a következő kibocsátást követő hány

percig aktuális, OCSP válasz frissesség ellenőrzés engedélyezése, időbélyeg szolgáltatás elérhetősége, OCSP szolgáltatás elérhetősége, szervezeti aláírási szabályzat a felhasználó nevében végrehajtott folyamatokra.

- **FMT_SMF.1.1** A TSF-nek alkalmasnak kell lennie arra, hogy végrehajtsa következő biztonsági menedzsment funkciókat:
    a) a használó alkalmazás által konfigurálható paraméterek importálását
    b) önellenőrzés
    c) azonosítás, hitelesítés és jogosultság ellenőrzés, a felhasználó bejelentkeztetése a kulcstárolóhoz
    d) a következő biztonsági attributumok menedzsmentje:
        - megbízható legfelső szintű hitelesítő tanúsítványok,
        - közbenső szintű hitelesítő tanúsítványok
        - saját tanúsítványok
        - más személyek tanúsítványai
        - tanúsítvány visszavonási listák
        - a CRL a kibocsátást követően hány napig aktuális
        - a CRL a következő kibocsátást követő hány napig aktuális
        - CRL frissesség ellenőrzés engedélyezése
        - visszavonás ellenőrzés kihagyhatóság engedélyezése
        - megbízható időszerverek
        - szolgáltatás igénybevétele utáni kényszerített kijelentkeztetés engedélyezés
        - OCSP válasz az előállítás követő hány percig aktuális
        - OCSP válasz a kibocsátás követő hány percig aktuális
        - OCSP válasz a következő kibocsátás követő hány percig aktuális
        - OCSP válasz frissesség ellenőrzés engedélyezés
        - időbélyeg szolgáltatás elérhetősége
        - OCSP szolgáltatás elérhetősége
        - szervezeti aláírási szabályzat
    e) tanúsítási útvonal érvényesítés
    f) CRL érvényesítés
    g) elektronikus aláírás létrehozása és ellenőrzése
    h) titkosítás és visszafejtés
    i) időbélyeg kérés és ellenőrzés
    j) OCSP kérés és ellenőrzés

O.TSF_Data megállapítja: A TSF csak jogosult felhasználó számára engedélyezi a TSF adatok módosítását. Ez a biztonsági célkitűzés találkozik a következő funkciókkal:

- **FMT_MTD.1.1** A TSF-nek korlátoznia kell a: megváltoztatását, törlését, üresítését, importálását, hozzáadását, a megbízható legfelső szintű hitelesítő tanúsítványok, közbenső szintű hitelesítő tanúsítványok, saját tanúsítványok, más személyek tanúsítványai, tanúsítvány visszavonási listák, a CRL a kibocsátást követően hány napig aktuális, a CRL a következő kibocsátást követő hány napig aktuális, CRL frissesség ellenőrzés engedélyezése, visszavonás ellenőrzés kihagyhatóság engedélyezése, megbízható időszerverek, szolgáltatás igénybevétele utáni kényszerített kijelentkeztetés engedélyezése, OCSP válasz az előállítást követő hány percig aktuális, OCSP válasz a kibocsátást követő hány percig aktuális, OCSP válasz a következő kibocsátást követő hány percig aktuális, OCSP válasz frissesség ellenőrzés engedélyezése, időbélyeg szolgáltatás elérhetősége, OCSP szolgáltatás elérhetősége, szervezeti aláírási szabályzat a felhasználó nevében végrehajtott folyamatokra.
- **FMT_SMF.1.1** A TSF-nek alkalmasnak kell lennie arra, hogy végrehajtsa következő biztonsági menedzsment funkciókat:
    a) a használó alkalmazás által konfigurálható paraméterek importálását
    b) önellenőrzés

c) azonosítás, hitelesítés és jogosultság ellenőrzés, a felhasználó bejelentkeztetése a kulcstárolóhoz
d) a következő biztonsági attributumok menedzsmentje:
   - megbízható legfelső szintű hitelesítő tanúsítványok,
   - közbenső szintű hitelesítő tanúsítványok
   - saját tanúsítványok
   - más személyek tanúsítványai
   - tanúsítvány visszavonási listák
   - a CRL a kibocsátást követően hány napig aktuális
   - a CRL a következő kibocsátást követő hány napig aktuális
   - CRL frissesség ellenőrzés engedélyezése
   - visszavonás ellenőrzés kihagyhatóság engedélyezése
   - megbízható időszerverek
   - szolgáltatás igénybevétele utáni kényszerített kijelentkeztetés engedélyezése
   - OCSP válasz az előállítást követő hány percig aktuális
   - OCSP válasz a kibocsátás követő hány percig aktuális
   - OCSP válasz a következő kibocsátást követő hány percig aktuális
   - OCSP válasz frissesség ellenőrzés engedélyezése
   - időbélyeg szolgáltatás elérhetősége
   - OCSP szolgáltatás elérhetősége
   - szervezeti aláírási szabályzat
e) tanúsítási útvonal érvényesítés
f) CRL érvényesítés
g) elektronikus aláírás létrehozása és ellenőrzése
h) titkosítás és visszafejtés
i) időbélyeg kérés és ellenőrzés
j) OCSP kérés és ellenőrzés

8.2.1.2 Az informatikai környezet biztonsági követelményeinek indoklása

OE.Authorized_Users megállapítja: A jogosult felhasználók megbízhatóak, hogy végre hajtsák jogosult feladataikat. Ez a biztonsági célkitűzés találkozik a következő informatikai környezet célkitűzésekkel:

- **AGD_ADM.1.1C** Az adminisztrátori útmutatónak ismertetnie kell a TOE adminisztrátor rendelkezésre álló adminisztrációs funkciókat és interfészeket.
- **AGD_ADM.1.2C** Az adminisztrátori útmutatónak ismertetnie kell, hogy hogyan kell a TOE-t biztonságos módon adminisztrálni.
- **AGD_ADM.1.3C** Az adminisztrátori útmutatónak figyelmeztetéseket kell tartalmaznia azon funkciókra és privilégiumokra vonatkozóan, amelyek kontrollálhatók egy biztonságos feldolgozási környezetben.
- **AGD_ADM.1.4C** Az adminisztrátori útmutatónak ismertetnie kell a felhasználói viselkedésre vonatkozó minden olyan feltételezést, amely a TOE biztonsági működés szempontjából fontos.
- **AGD_ADM.1.5C** Az adminisztrátori útmutatónak ismertetnie kell minden, az adminisztrátor felügyelete alá tartozó biztonsági paramétert, megjelölve a biztonságos értékeket, ahogyan az alkalmas.
- **AGD_ADM.1.6C** Az adminisztrátori útmutatónak ismertetnie kell a biztonsággal kapcsolatos események valamennyi típusát, amelyek a végrehajtandó adminisztratív funkciókkal kapcsolatosak, beleértve a biztonsági funkciók felügyelete alá tartozó entitások biztonsági jellemzőit is.
- **AGD_ADM.1.7C** Az adminisztrátori útmutatónak konzisztensnek kell lennie minden más értékelésre rendelkezésre bocsátott dokumentációval.

- **AGD_ADM.1.8C** Az adminisztrátori útmutatónak ismertetnie kell az informatikai környezetre vonatkozó mindazon biztonsági követelményt, amely az adminisztrátor számára fontos.
- **AGD_USR.1.1C** A felhasználói útmutatónak ismertetnie kell a TOE nem adminisztrációs felhasználói számára a rendelkezésre álló funkciókat és interfészeket.
- **AGD_USR.1.2C** A felhasználói útmutatónak ismertetnie kell a TOE által biztosított, a felhasználók által hozzáférhető biztonsági funkciók használatát.
- **AGD_USR.1.3C** A felhasználói útmutatónak figyelmeztetéseket kell tartalmaznia a felhasználók által hozzáférhető azon funkciókra és privilégiumokra vonatkozóan, amelyek kontrollálhatóak egy biztonságos feldolgozási környezetben.
- **AGD_USR.1.4C** A felhasználói útmutatónak világosan be kell mutatnia minden felhasználói felelőséget, amely a TOE biztonságos működéséhez szükséges, beleértve azokat, amelyek a felhasználói viselkedésre vonatkozó azon feltételezésekkel kapcsolatosak, amelyek a TOE biztonsági környezetének ismertetésében találhatók.
- **AGD_USR.1.5C** A felhasználói útmutatónak konzisztensnek kell lennie minden más értékelésre rendelkezésre bocsátott dokumentummal.
- **AGD_USR.1.6C** A felhasználói útmutatónak ismertetnie kell az informatikai környezetre vonatkozó mindazon biztonsági követelményt, amely a felhasználó számára fontos.

OE.Configuration megállapítja: A TOE helyesen van installálva és configurálva, ahhoz, hogy a TOE biztonságos állapotban induljon. Ez a biztonsági célkitűzés találkozik a következő informatikai környezet célkitűzésekkel:

- **ADO_IGS.1.1C** A dokumentációnak ismertetnie kell a TOE biztonságos installációhoz, generáláshoz és rendszerindításhoz szükséges lépéseket.

OE.Crypto_Normal megállapítja: A TOE környezetének tartalmaznia kell egy vagy több kriptográfiai szolgáltatót (modult), amelyek megfelelnek a FIPS 140-1 sorozat 1.szintnek vagy magasabb szintnek. Ez a modul, vagy ezek a modulok alkalmazásra kerülnek a következő műveletek során: kulcs pár generálás, elektronikus aláírás és ellenőrzés, titkosítás, visszafejtés, biztonságos lenyomat képzés, véletlenszám generálás, lenyomat képzéses Message Authentication Code (HMAC) eljárás, és/vagy egyéb szükséges kriptográfiai funkciók. Összegezve: a TOE minden kriptográfiai modulja FIPS 140 sorozat,1. szint vagy magasabb szintnek megfelelő (compliant) kell legyen: Ez a biztonsági célkitűzés találkozik a következő informatikai környezet célkitűzésekkel:

- **FCS_CRM_FPS.1.1** Az informatikai környezetnek biztosítania kell az összes, TSF számára szükséges kriptográfiai modult.
- **FCS_CRM_FPS.1.2** Minden kriptográfiai modulnak FIPS 140 sorozat 1. szint vagy magasabb szintnek megfelelő (compliant) kriptográfiai szolgáltatónak kell lennie vagy NHH minősítéssel rendelkező BALE-nak kell lennie.

OE.Crypto_Rigid megállapítja: A TOE környezetének tartalmaznia kell legalább kettő kriptográfiai szolgáltatót, amelyek közül az egyiket NHH minősítéssel rendelkező BALE biztosít.

a) A BALE kriptográfiai szolgáltatója alkalmazásra kerül a következő műveletek során: elektronikus aláírás, visszafejtés, biztonságos lenyomat képzés, véletlenszám generálás.
b) A FIPS 140-1 sorozat,1. szint vagy magasabb szintnek megfelelő (compliant) kriptográfiai szolgáltató alkalmazásra kerül a következő műveletek során: elektronikus aláírás ellenőrzése, titkosítás, lenyomat képzés, véletlenszám generálás (FIPS-140-2 compliant), lenyomat képzéses Message Authentication Code (HMAC) eljárás, és/vagy egyéb szükséges kriptográfiai funkciók.

Ez a biztonsági célkitűzés találkozik a következő informatikai környezet célkitűzésekkel:

- **FCS_CRM_FPS.1.1** Az informatikai környezetnek biztosítania kell az összes, TSF számára szükséges kriptográfiai modult.

- **FCS_CRM_FPS.1.2** Minden kriptográfiai modulnak FIPS 140 sorozat 1. szint vagy magasabb szintnek megfelelő (compliant) kriptográfiai szolgáltatónak kell lennie vagy NHH minősítéssel rendelkező BALE-nak kell lennie.

OE.Low megállapítja. A TOE azonosítási és hitelesítési funkciói olyan minimálisan alacsony támadási lehetőségre vannak tervezve és megvalósítva, amint azt a sebezhetőségi értékelés és a funkció szilárdsági analízis (Strength of Function analyses) jóváhagyta. Ez a biztonsági célkitűzés találkozik a következő informatikai környezet célkitűzésekkel:

- **AVA_SOF.1.1C** Minden egyes mechanizmusra, amely TOE biztonsági funkciójának erősségére vonatkozó kijelentést tartalmaz, a TOE biztonsági funkcióerőssége elemzésének kell kimutatnia, hogy a mechanizmus kielégíti vagy túllépi a PP/ST-ben meghatározott legkisebb erősségi szintet.
- **AVA_SOF.1.2C** Minden egyes mechanizmusra, amely TOE biztonsági funkciójának külöleges erősségére vonatkozó kijelentést tartalmaz, a TOE biztonsági funkcióerőssége elemzésének kell kimutatnia, hogy a mechanizmus kielégíti vagy túllépi a PP/ST-ben meghatározott külöleges funkcióerősségi mértéket.

OE.Physical_Security megállapítja: A környezetnek gondoskodnia kell a fizikai biztonság egy elfogadható szintjéről azon célból, hogy a környezet a TOE-t ne befolyásolhassa vagy ne lehessen tárgya megkerülő csatorna támadásoknak, mint az erő analízis és idő analízis különböző formái. Ez a biztonsági célkitűzés találkozik a következő informatikai környezet célkitűzésekkel:

- **AGD_ADM.1.1C** Az adminisztrátori útmutatónak ismertetnie kell a TOE adminisztrátor rendelkezésre álló adminisztrációs funkciókat és interfészeket.
- **AGD_ADM.1.2C** Az adminisztrátori útmutatónak ismertetnie kell, hogy hogyan kell a TOE-t biztonságos módon adminisztrálni.
- **AGD_ADM.1.3C** Az adminisztrátori útmutatónak figyelmeztetéseket kell tartalmaznia azon funkciókra és privilégiumokra vonatkozóan, amelyek kontrollálhatók egy biztonságos feldolgozási környezetben.
- **AGD_ADM.1.4C** Az adminisztrátori útmutatónak ismertetnie kell a felhasználói viselkedésre vonatkozó minden olyan feltételezést, amely a TOE biztonsági működés szempontjából fontos.
- **AGD_ADM.1.5C** Az adminisztrátori útmutatónak ismertetnie kell minden, az adminisztrátor felügyelete alá tartozó biztonsági paramétert, megjelölve a biztonságos értékeket, ahogyan az alkalmas.
- **AGD_ADM.1.6C** The administrator guidance shall describe each type of securityrelevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
- **AGD_ADM.1.7C** Az adminisztrátori útmutatónak konzisztensnek kell lennie minden más értékelésre rendelkezésre bocsátott dokumentációval.
- **AGD_ADM.1.8C** Az adminisztrátori útmutatónak ismertetnie kell az informatikai környezetre vonatkozó mindazon biztonsági követelményt, amely az adminisztrátor számára fontos.
- **AGD_USR.1.1C** A felhasználói útmutatónak ismertetnie kell a TOE nem adminisztrációs felhasználói számára a rendelkezésre álló funkciókat és interfészeket.
- **AGD_USR.1.2C** A felhasználói útmutatónak ismertetnie kell a TOE által biztosított, a felhasználók által hozzáférhető biztonsági funkciók használatát.
- **AGD_USR.1.3C** A felhasználói útmutatónak figyelmeztetéseket kell tartalmaznia a felhasználók által hozzáférhető azon funkciókra és privilégiumokra vonatkozóan, amelyek kontrollálhatóak egy biztonságos feldolgozási környezetben.
- **AGD_USR.1.4C** A felhasználói útmutatónak világosan be kell mutatnia minden felhasználói felelőséget, amely a TOE biztonságos működéséhez szükséges, beleértve azokat, amelyek a felhasználói viselkedésre vonatkozó azon feltételezésekkel kapcsolatosak, amelyek a TOE biztonsági környezetének ismertetésében találhatók.

- **AGD_USR.1.5C** A felhasználói útmutatónak konzisztensnek kell lennie minden más értékelésre rendelkezésre bocsátott dokumentummal.
- **AGD_USR.1.6C** A felhasználói útmutatónak ismertetnie kell az informatikai környezetre vonatkozó mindazon biztonsági követelményt, amely a felhasználó számára fontos.

OE.PKI_Info megállapítja: Az informatikai környezetnek szolgáltatnia kell a TOE számára tanúsítványokat és a tanúsítvány visszavonási információkat. Ez a biztonsági célkitűzés találkozik a következő informatikai környezet célkitűzésekkel:

- **FDP_ITC_PKI_INF.1.1** Az informatikai környezetnek a TOE számára folyamatosan biztosítania kell: tanúsítványokat, CRL-ket, a következő feltételek teljesülése esetén: információ rendelkezésre állása az informatikai környezet számára.

OE.Time megállapítja: A környezetnek gondoskodnia kell az aktuális idő eléréséről, a megkövetelt pontosság szerinti, GMT formában. Ez a biztonsági célkitűzés találkozik a következő informatikai környezet célkitűzésekkel:

- **FPT_STM.1.1** Az informatikai környezetnek képesnek kell lennie megbízható időpontok szolgáltatására a TSF számára.

8.2.1.3 Tanúsítási útvonal érvényesítése (CPV) – Alap csomag biztonsági követelményeinek indoklása

O.Availability megállapítja: A TSF biztosítja a biztonsági szolgáltatásokat, akkor is, ha a visszavonási információ nem áll rendelkezésre. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_DAU_CPV_CER.1.1** A TSF-nek a tanúsítványt csak akkor szabad elfogadnia, ha a következő ellenőrzések sikeresen megtörténtek:
  a) A tanúsítványon az aláírás ellenőrzése a következőekkel: parent-public-key, parent-public-key-algorithm-identifier, és parent-public-key-parameters
  b) A tanúsítvány notBefore mezője < = current-time
  c) A tanúsítvány notAfter mezője > = current-time
  d) A tanúsítvány issuer mezője = parent-DN
  e) A TSF képes a tanúsítvány minden kritikus kiterjesztését feldolgozni.
- **FDP_DAU_CPV_CER.1.2** A TSF kikerülheti a visszavonási állapot ellenőrzését, ha a tanúsítvány tartalmazza a no-check kiterjesztést.
- **FDP_DAU_CPV_CER.1.3** A TSF ki kell hagynia a visszavonás ellenőrzését, ha a visszavonási információ nem áll rendelkezésre és a felhasználó nevében végrehajtott folyamat felülbírálja a visszavonás ellenőrzést.
- **FDP_DAU_CPV_CER.1.4** A TSF-nek el kell fogadnia a tanúsítványt, ha a visszavonási állapot CRL ellenőrzése vagy OCSP ellenőrzés alapján, meggyőződött arról, hogy a tanúsítvány nincs visszavonva.
- **FDP_DAU_CPV_CER.1.5** A TSF-nek nyilvános kulcs paraméterei állapotgépet a következő szabályok szerint kell vezérelnie:
  a) a paraméter megállapítása a tanúsítvány subjectPublickeyInfo mezőjéből, ha abban szerepel a paraméter, különben
  b) az eredeti paraméter állapot megtartása, ha az aktuális tanúsítvány nyilvános kulcsának algoritmusa és a kibocsátó nyilvános kulcsának algoritmusa azonos algoritmus családba tartozik, különben
  c) a paramétert be kell állítani „null” értékre.

O.Correct_Time megállapítja: A TSF gondoskodik precíz átmeneti érvényesítési eredményekről. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_DAU_CPV_INI.1.1** A TSF-nek a felhasználó nevében végrehajtott folyamat által szolgáltatott megbízható legfelső szintű hitelesítő tanúsítványt kell használnia.

- **FDP_DAU_CPV_INI.1.2** A TSF-nek a felhasználó nevében végrehajtott folyamat által meghatározott időszerverektől vagy ha az nem áll rendelkezésre, akkor a lokális környezetből, mint megbízható forrásból kell megszereznie az aktuális időt, amelyet 'current-time'-nak nevezünk.
- **FDP_DAU_CPV_INI.1.3** A TSF-nek a megbízható legfelső szintű tanúsítványok esetében a következő ellenőrzéseket kell elvégeznie:
    a) Subject DN és az Issuer DN egyezik
    b) A tanúsítványon az aláírás érvényes, a megbízható legfelső szintű hitelesítő tanúsítvány alanyának nyilvános kulcsával és annak paraméterével (ha az rendelkezésre áll) ellenőrizve
    c) a megbízható legfelső szintű tanúsítvány notBefore mezője <= current-time
    d) a megbízható legfelső szintű tanúsítvány notAfter mezője => current-time
- **FDP_DAU_CPV_INI.1.4** A TSF-nek a megbízható legfelső szintű hitelesítő tanúsítványból származtatnia kell a következő információkat: subject DN, subject public key, subject public key algorithm object identifier, subject public key paraméterek.

O.Current_Certificate megállapítja: A TSF csak akkor fogadja el a tanúsítványokat, ha azok nem jártak le. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_DAU_CPV_CER.1.1** A TSF-nek a tanúsítványt csak akkor szabad elfogadnia, ha a következő ellenőrzések sikeresen megtörténtek:
    a) A tanúsítványon az aláírás ellenőrzése a következőekkel: parent-public-key, parent-public-key-algorithm-identifier, és parent-public-key-parameters
    b) A tanúsítvány notBefore mezője < = current-time
    c) A tanúsítvány notAfter mezője > = current-time
    d) A tanúsítvány issuer mezője = parent-DN
    e) A TSF képes a tanúsítvány minden kritikus kiterjesztését feldolgozni.
- **FDP_DAU_CPV_CER.1.2** A TSF kikerülheti a visszavonási állapot ellenőrzését, ha a tanúsítvány tartalmazza a no-check kiterjesztést.
- **FDP_DAU_CPV_CER.1.3** A TSF ki kell hagynia a visszavonás ellenőrzését, ha a visszavonási információ nem áll rendelkezésre és a felhasználó nevében végrehajtott folyamat felülbírálja a visszavonás ellenőrzést.
- **FDP_DAU_CPV_CER.1.4** A TSF-nek el kell fogadnia a tanúsítványt, ha a visszavonási állapot CRL ellenőrzése vagy OCSP ellenőrzés alapján, meggyőződött arról, hogy a tanúsítvány nincs visszavonva.
- **FDP_DAU_CPV_CER.1.5** A TSF-nek nyilvános kulcs paraméterei állapotgépet a következő szabályok szerint kell vezérelnie:
    a) a paraméter megállapítása a tanúsítvány subjectPublickeyInfo mezőjéből, ha abban szerepel a paraméter, különben
    b) az eredeti paraméter állapot megtartása, ha az aktuális tanúsítvány nyilvános kulcsának algoritmusa és a kibocsátó nyilvános kulcsának algoritmusa azonos algoritmus családba tartozik, különben
    c) a paramétert be kell állítani „null" értékre.

O.Get_KeyInfo megállapítja: A TSF szolgáltatja a felhasználó nyilvános kulcsát és a kapcsolódó információkat, azon célból, hogy végrehajtson kriptográfiai funkciókat. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_DAU_CPV_OUT.1.1** A TSF-nek tanúsítási útvonal érvényesítési hibát kell visszaadnia, ha az tanúsítási útvonalban bármely tanúsítvány visszautasításra került.
- **FDP_DAU_CPV_OUT.1.2** A végtanúsítványból a TSF-nek a következő változókat kell visszaadnia: subject DN, subject public key algorithm identifier, subject public key, kritikus keyUsage kiterjesztés.

- **FDP_DAU_CPV_OUT.1.3** A végtanúsítványból a TSF-nek a következő további változókat kell visszaadnia: tanúsítvány, subject alternative names, tanúsítvány lánc, extendedKeyUsage.
- **FDP_DAU_CPV_OUT.1.4** A TSF-nek az alany nyilvános kulcs paramétereit a tanúsítási útvonal paraméter állapotgép alapján kell visszaadnia.

O.Path_Find megállapítja: A TSF képes lesz megtalálni a tanúsítási útvonalat a megbízható legfelső szintű hitelesítő tanúsítványtól az aláíróig. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_CPD.1.1** A TSF-nek az érvényesítési útvonalat a felhasználó nevében végrehajtott folyamat által szolgáltatott megbízható legfelső szintű hitelesítő tanúsítvánnyal kezdve a végtanúsítványig kell felépítenie, a következő tanúsítvány mezők vagy kiterjesztések egyezőségi szabályait alkalmazva: distinguished name.
- **FDP_CPD.1.2** A TSF-nek a tanúsítási útvonalat a következő kiegészítő egyezőségi szabályok alkalmazásával kell felépítenie:
  a) aláírás ellenőrzése esetén:
     aa) ha aláírási szabályzat nincs érvényben, akkor a keyUsage kiterjesztésben a nonRepudiation bit be van állítva
     ab) ha aláírási szabályzat érvényben van, akkor annak rendelkezéseitől függően: a keyUsage kiterjesztésben a nonRepudiation vagy digitalSignature bit be van állítva
  b) a keyUsage kiterjesztésben a digitalSignature bit be van állítva, entitás hitelesítése esetén
  c) a keyUsage kiterjesztésben a keyEncipherment bit be van állítva, titkosítás, visszafejtés esetén
- **FDP_CPD.1.3** A TSF-nek a tanúsítási útvonalat a következő kiegészítő egyezőségi szabályok alkalmazásával kell felépítenie:
  a) nincs további szabály az extendedKeyUsage kiterjesztés tartalmára.
- **FDP_CPD.1.4** A TSF kikerülhet bármely egyezőségi szabályt, kivéve:
  a) distinguished name
  b) a tanúsítvány formátuma X.509
  amennyiben további tanúsítási útvonalak szükségesek.

O.Trusted_Keys megállapítja: A TSF megbízható nyilvános kulcsokat használ a tanúsítási útvonal érvényesítésénél. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_DAU_CPV_INI.1.1** A TSF-nek a felhasználó nevében végrehajtott folyamat által szolgáltatott megbízható legfelső szintű hitelesítő tanúsítványt kell használnia.
- **FDP_DAU_CPV_INI.1.2** A TSF-nek a felhasználó nevében végrehajtott folyamat által meghatározott időszerverektől vagy ha az nem áll rendelkezésre, akkor a lokális környezetből, mint megbízható forrásból kell megszereznie az aktuális időt, amelyet ’current-time’-nak nevezünk.
- **FDP_DAU_CPV_INI.1.3** A TSF-nek a megbízható legfelső szintű tanúsítványok esetében a következő ellenőrzéseket kell elvégeznie:
  a) Subject DN és az Issuer DN egyezik
  b) A tanúsítványon az aláírás érvényes, a megbízható legfelső szintű hitelesítő tanúsítvány alanyának nyilvános kulcsával és annak paraméterével (ha az rendelkezésre áll) ellenőrizve
  c) a megbízható legfelső szintű tanúsítvány notBefore mezője <= current-time
  d) a megbízható legfelső szintű tanúsítvány notAfter mezője => current-time
- **FDP_DAU_CPV_INI.1.4** A TSF-nek a megbízható legfelső szintű hitelesítő tanúsítványból származtatnia kell a következő információkat: subject DN, subject public key, subject public key algorithm object identifier, subject public key paraméterek.

O.User megállapítja: A TSF csak CA által kiadott tanúsítványokat fogad el. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_DAU_CPV_CER.2.1** A TSF-nek a közbenső tanúsítványt csak akkor kell elfogadnia, ha a következő ellenőrzések sikeresen megtörténtek:
    a) basicConstraints kiterjesztés jelen van, és abban a cA = TRUE
    b) pathLenConstraint kényszer teljesül
    c) ha kritikus keyUsage kiterjesztés jelen van, akkor abban a keyCertSign bit be van állítva

O.Verified_Certificate megállapítja: A TSF csak ellenőrizhető aláírással ellátott tanúsítványokat fogad el. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_DAU_CPV_CER.1.1** A TSF-nek a tanúsítványt csak akkor szabad elfogadnia, ha a következő ellenőrzések sikeresen megtörténtek:
    a) A tanúsítványon az aláírás ellenőrzése a következőekkel: parent-public-key, parent-public-key-algorithm-identifier, és parent-public-key-parameters
    b) A tanúsítvány notBefore mezője < = current-time
    c) A tanúsítvány notAfter mezője > = current-time
    d) A tanúsítvány issuer mezője = parent-DN
    e) A TSF képes a tanúsítvány minden kritikus kiterjesztését feldolgozni.
- **FDP_DAU_CPV_CER.1.2** A TSF kikerülheti a visszavonási állapot ellenőrzését, ha a tanúsítvány tartalmazza a no-check kiterjesztést.
- **FDP_DAU_CPV_CER.1.3** A TSF ki kell hagynia a visszavonás ellenőrzését, ha a visszavonási információ nem áll rendelkezésre és a felhasználó nevében végrehajtott folyamat felülbírálja a visszavonás ellenőrzést.
- **FDP_DAU_CPV_CER.1.4** A TSF-nek el kell fogadnia a tanúsítványt, ha a visszavonási állapot CRL ellenőrzése vagy OCSP ellenőrzés alapján, meggyőződött arról, hogy a tanúsítvány nincs visszavonva.
- **FDP_DAU_CPV_CER.1.5** A TSF-nek nyilvános kulcs paraméterei állapotgépet a következő szabályok szerint kell vezérelnie:
    a) a paraméter megállapítása a tanúsítvány subjectPublickeyInfo mezőjéből, ha abban szerepel a paraméter, különben
    b) az eredeti paraméter állapot megtartása, ha az aktuális tanúsítvány nyilvános kulcsának algoritmusa és a kibocsátó nyilvános kulcsának algoritmusa azonos algoritmus családba tartozik, különben
    c) a paramétert be kell állítani „null” értékre.

O.Valid_Certificate megállapítja: A TSF csak érvényes, azaz nem visszavont tanúsítványokat használ. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_DAU_CPV_CER.1.1** A TSF-nek a tanúsítványt csak akkor szabad elfogadnia, ha a következő ellenőrzések sikeresen megtörténtek:
    a) A tanúsítványon az aláírás ellenőrzése a következőekkel: parent-public-key, parent-public-key-algorithm-identifier, és parent-public-key-parameters
    b) A tanúsítvány notBefore mezője < = current-time
    c) A tanúsítvány notAfter mezője > = current-time
    d) A tanúsítvány issuer mezője = parent-DN
    e) A TSF képes a tanúsítvány minden kritikus kiterjesztését feldolgozni.
- **FDP_DAU_CPV_CER.1.2** A TSF kikerülheti a visszavonási állapot ellenőrzését, ha a tanúsítvány tartalmazza a no-check kiterjesztést.
- **FDP_DAU_CPV_CER.1.3** A TSF ki kell hagynia a visszavonás ellenőrzését, ha a visszavonási információ nem áll rendelkezésre és a felhasználó nevében végrehajtott folyamat felülbírálja a visszavonás ellenőrzést.
- **FDP_DAU_CPV_CER.1.4** A TSF-nek el kell fogadnia a tanúsítványt, ha a visszavonási állapot CRL ellenőrzése vagy OCSP ellenőrzés alapján, meggyőződött arról, hogy a tanúsítvány nincs visszavonva.

- **FDP_DAU_CPV_CER.1.5** A TSF-nek nyilvános kulcs paraméterei állapotgépet a következő szabályok szerint kell vezérelnie:
  a) a paraméter megállapítása a tanúsítvány subjectPublickeyInfo mezőjéből, ha abban szerepel a paraméter, különben
  b) az eredeti paraméter állapot megtartása, ha az aktuális tanúsítvány nyilvános kulcsának algoritmusa és a kibocsátó nyilvános kulcsának algoritmusa azonos algoritmus családba tartozik, különben
  c) a paramétert be kell állítani „null” értékre.

8.2.1.4 PKI aláírás készítés csomag biztonsági követelményeinek indoklása

O.Give_Sig_Hints megállapítja: A TSF útmutatást ad a helyes tanúsítány kiválasztására az aláírás ellenőrzésénél. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_ETC_SIG.1.1** A TSF-nek a magánkulcs felhasználásával elektronikus aláírást kell létrehozni.
- **FDP_ETC_SIG.1.2** A TSF-nek az elektronikus aláírásba a következő aláírást kísérő információkat kell befoglalnia:

1)A1-kombatibilis elektronikus aláírás készítése esetén:

a)kötelezően: hash algoritmus, aláírási algoritmus, aláíró nyilvános kulcs, aláíró DN, aláíró tanúsítványt kibocsátó DN, aláíró tanúsítványának sorozatszáma, aláíró tanúsítványa, aláíró tanúsítványának az érvényesített tanúsítási útvonala, aláírás időpontja

b)opcionálisan: aláírás helye(város), aláírás helye(irányítószám), aláírás helye(megye), aláírás helye(ország), aláíró szerepkör

2)A2 elektronikus aláírás készítése esetén:

a)„Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára (2005. november 22.)” választása esetén:

aa)kötelezően:

- kanonizálási módszer (CanonicalizationMethod), a http://www.w3.org/TR/2001/REC-xml-c14n-20010315 értékkel
- aláírási algoritmus (SignatureMethod) az RSAwithSHA1 értékkel
- aláírt dokumentumok külső vagy belső hivatkozásai (Reference)
- transzformációk (Transforms) az http://www.w3.org/TR/2001/REC-xml-c14n-20010315 vagy http://www.w3.org/2000/09/xmldsig#BASE64 értékkel
- lenyomatképző algoritmus (DigestMethod) az SHA1 értékkel
- az aláíró tanúsítványa (KeyInfo)
- aláírás időpontja (SigningTime)
- hivatkozás az aláíró tanúsítványára (SigningCertificate)
- aláírási szabályzat (SignaturePolicyIdentifier)
- aláírt dokumentumok adatformátum leírásai (DataObjectFormat)

ab)opcionálisan:

- az aláíró nyilvános kulcsa (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)
- aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)
- aláíró szerepkörei (SignerRole)
- kötelezettségvállalás jelzése (CommitmentTypeIndication)
- aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)
- ellenjegyző aláírás (CounterSignature)
- aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)

- hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)
- aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)
- referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)
- archív időbélyeg(ek) (ArchiveTimeStamp)

b)v1.2.2 vagy v1.3.2 szabványos formátum választása esetén:

ba)kötelezően:

- kanonizálási módszer (CanonicalizationMethod) http://www.w3.org/TR/2001/REC-xml-c14n-20010315, http://www.w3.org/TR/2001/REC-xml-c14n-0010315#WithComments, http://www.w3.org/TR/2001/REC-xml-c14n-20010315, http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments, http://www.w3.org/2006/12/xml-c14n11, http://www.w3.org/2006/12/xml-c14n11#WithComments
- aláírási algoritmus (SignatureMethod) RSAwithSHA1, RSAwithSHA256, RSAwithSHA384, RSAwithSHA512 vagy DSAwithSHA1
- aláírt dokumentumok külső vagy belső hivatkozásai (Reference)
- transzformációk (Transforms)
- lenyomatképző algoritmus (DigestMethod)
- az aláíró tanúsítványa (KeyInfo)
- aláírás időpontja (SigningTime)
- hivatkozás az aláíró tanúsítványára (SigningCertificate)

bb)opcionálisan:

- az aláíró nyilvános kulcsa (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)
- aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)
- aláíró szerepkörei (SignerRole)
- aláírási szabályzat (SignaturePolicyIdentifier)
- aláírt dokumentumok adatformátum leírásai (DataObjectFormat
- kötelezettségvállalás jelzése (CommitmentTypeIndication)
- aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)
- ellenjegyző aláírás (CounterSignature)
- aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)
- aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)

- referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)
- archív időbélyeg(ek) (ArchiveTimeStamp)

c)„Egységes MELASZ formátum elektronikus aláírásokra” v2.0 választása esetén:
ca)kötelezően:

- kanonizálási módszer (CanonicalizationMethod), a http://www.w3.org/TR/2001/REC-xml-c14n-20010315 értékkel
- aláírási algoritmus (SignatureMethod) az RSAwithSHA1 vagy RSAwithSHA256 értékkel
- aláírt dokumentumok külső vagy belső hivatkozásai (Reference)
- transzformációk (Transforms) az http://www.w3.org/TR/2001/REC-xml-c14n-20010315 vagy http://www.w3.org/2000/09/xmldsig#BASE64 értékkel
- lenyomatképző algoritmus (DigestMethod) az SHA1 vagy SHA256 értékkel
- az aláíró tanúsítványa (KeyInfo)
- aláírás időpontja (SigningTime)
- hivatkozás az aláíró tanúsítványára (SigningCertificate)
- aláírási szabályzat (SignaturePolicyIdentifier)
- aláírt dokumentumok adatformátum leírásai (DataObjectFormat)

cb)opcionálisan:

- az aláíró nyilvános kulcsa (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)
- aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)
- aláíró szerepkörei (SignerRole)
- kötelezettségvállalás jelzése (CommitmentTypeIndication)
- aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)
- ellenjegyző aláírás (CounterSignature)
- aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)
- aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)
- referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)
- archív időbélyeg(ek) (ArchiveTimeStamp)

8.2.1.5 PKI aláírás ellenőrzés csomag biztonsági követelményeinek indoklása

O.Use_Sig_Hints megállapítja: A TSF az útmutatást használja a helyes tanúsítvány kiválasztására az aláírás ellenőrzésénél. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_ITC_SIG.1.1** A TSF-nek az alábbi aláírást kísérő információkat kell használnia az aláírás ellenőrzése során:

1)A1-kombatibilis elektronikus aláírás ellenőrzése esetén:

a)kötelezően: hash algoritmus, aláírási algoritmus, aláíró nyilvános kulcs, aláíró DN, aláíró tanúsítványt kibocsátó DN, aláíró tanúsítványának sorozatszáma, aláíró tanúsítványa, aláíró tanúsítványának az érvényesített tanúsítási útvonala, aláírás időpontja

b)opcionálisan: aláírás helye(város), aláírás helye(irányítószám), aláírás helye(megye), aláírás helye(ország), aláíró szerepkör

2)A2 elektronikus aláírás ellenőrzés esetén:

a)„Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára (2005. november 22.)” formátumnak vagy az „Egységes MELASZ formátum elektronikus aláírásokra” v2.0 dokumentumnak megfelelő aláírás ellenőrzése esetén:

aa)kötelezően:

- kanonizálási módszer (CanonicalizationMethod)
- aláírási algoritmus (SignatureMethod)
- aláírt dokumentumok külső vagy belső hivatkozásai (Reference)
- transzformációk (Transforms)
- lenyomatképző algoritmus (DigestMethod)
- az aláíró tanúsítványa (KeyInfo)
- aláírás időpontja (SigningTime)
- hivatkozás az aláíró tanúsítványára (SigningCertificate)
- aláírási szabályzat (SignaturePolicyIdentifier)
- aláírt dokumentumok adatformátum leírásai (DataObjectFormat)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)

ab)opcionálisan:

- az aláíró nyilvános kulcsa (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)
- aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)
- aláíró szerepkörei (SignerRole)
- kötelezettségvállalás jelzése (CommitmentTypeIndication)
- aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)
- ellenjegyző aláírás (CounterSignature)
- aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)
- aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)
- referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)

- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)
- archív időbélyeg(ek) (ArchiveTimeStamp)

b)v1.2.2 vagy v1.3.2 szabványos formátumnak megfelelő aláírás ellenőrzése esetén:
ba)kötelezően:

- kanonizálási módszer (CanonicalizationMethod)
- aláírási algoritmus (SignatureMethod)
- aláírt dokumentumok külső vagy belső hivatkozásai (Reference)
- transzformációk (Transforms)
- lenyomatképző algoritmus (DigestMethod)
- az aláíró tanúsítványa (KeyInfo)
- aláírás időpontja (SigningTime)
- hivatkozás az aláíró tanúsítványára (SigningCertificate)

bb) opcionálisan:

- az aláíró nyilvános kulcsa (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)
- aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)
- aláíró szerepkörei (SignerRole)
- aláírási szabályzat (SignaturePolicyIdentifier)
- aláírt dokumentumok adatformátum leírásai (DataObjectFormat
- kötelezettségvállalás jelzése (CommitmentTypeIndication)
- aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)
- ellenjegyző aláírás (CounterSignature)
- aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)
- aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)
- referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)
- archív időbélyeg(ek) (ArchiveTimeStamp)

O.Linkage_Sig_Ver megállapítja: A TSF helyes felhasználói nyilvános kulcsot használja az aláírás ellenőrzésénél. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_DAU_SIG.1.1** A TSF-nek a Tanúsítási útvonal érvényesítése (CPV) - Alap csomagból a következő információkat kell használnia: subject public key algorithm, subject public key, subject public key parameters, amikor az aláírt adaton az elektronikus aláírást ellenőrzi.
- **FDP_DAU_SIG.1.2** A TSF-nek ellenőriznie kell, hogy a Tanúsítási útvonal érvényesítése (CPV) - Alap csomag által visszaadott keyUsage kiterjesztésben a nonRepudiation bit vagy a digitalSignature bit be van állítva.
- **FDP_DAU_SIG.1.3** A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie:
  a) Tanúsítási útvonal érvényesítése (CPV) - Alap csomag által visszaadott subject DN egyezik az aláírási információkkal.
  b) a tanúsítvány keyUsage kiterjesztésében:
  ba) ha aláírási szabályzat nincs érvényben, akkor kizárólag csak a nonRepudiation bit van beállítva
  bb) ha aláírási szabályzat van érvényben, akkor annak rendelkezésétől függően az alábbiak valamelyike:
  - kizárólag csak a nonRepudiation bit van beállítva
  - kizárólag csak a digitalSignature bit van beállítva
  - a nonRepudiation bit van beállítva, a többi bit nem számít
  - a digitalSignature bit van beállítva, a többi bit nem számít
  c) szigorú üzemmódban a minősített elektronikus aláírás esetén az aláíró tanúsítványában a kötelező qcStatements kiterjesztésben az id-etsi-qcs-QcCompliance OID meglétének ellenőrzése

8.2.1.6 PKI titkosítás kulcs átviteli algoritmusokkal csomag biztonsági követelményeinek indoklása

O.Hints_Enc_WO megállapítja: A TSF útmutatást ad a helyes tanúsítványok vagy kulcsok kiválasztására a PKI kulcs átviteli algoritmusokkal történő titkosításhoz. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_ETC_ENC.1.1** A TSF-nek a következő információkat kell a titkosított adattal együtt biztosítania:
  a) visszafejtő (címzett) nyilvános kulcsú tanúsítványa
  b) titkosítás időpontja
  c) fájl név vagy annak megfelelője
  d) titkosítatlan tartalomra képzett lenyomat
  e) a címzett részére aszimmetrikus titkosítással csomagolt titkos kulcs
- **FDP_ETC_ENC.1.2** A TSF-nek a Tanúsítási útvonal érvényesítése (CPV) - Alap csomagból a következő információkat kell használnia a titkosított adat létrehozásakor: subject public key algorithm, subject public key, subject public key paraméterek.

O.Linkage_Enc_WO megállapítja: A TSF a helyes felhasználói nyilvános kulcsot használja a kulcsátvitel során. Ez a biztonsági célkitűzés találkozik a következő funkciókkal:

- **FDP_ETC_ENC.1.1** A TSF-nek a következő információkat kell a titkosított adattal együtt biztosítania:
  a) visszafejtő (címzett) nyilvános kulcsú tanúsítványa
  b) titkosítás időpontja
  c) fájl név vagy annak megfelelője
  d) titkosítatlan tartalomra képzett lenyomat
  e) a címzett részére aszimmetrikus titkosítással csomagolt titkos kulcs
- **FDP_ETC_ENC.1.2** A TSF-nek a Tanúsítási útvonal érvényesítése (CPV) - Alap csomagból a következő információkat kell használnia a titkosított adat létrehozásakor: subject public key algorithm, subject public key, subject public key paraméterek.

- **FDP_DAU_ENC.1.1** A TSF-nek ellenőriznie kell, hogy a Tanúsítási útvonal érvényesítése (CPV) - Alap csomagból visszaadott keyUsage kiterjesztésben a keyEncipherment bit be van állítva.
- **FDP_DAU_ENC.1.2** A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie:
  a) a visszafejtett tartalomra képzett lenyomat megegyezik-e az eredeti lenyomattal.

8.2.1.7 PKI visszafejtés kulcs átviteli algoritmusokkal csomag biztonsági követelményeinek indoklása

O.Correct_KT megállapítja: A TSF a megfelelő magánkulcsot és kulcsátviteli algoritmust használja. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_ITC_ENC.1.1** A TSF-nek a titkosított adatról a következő információkat kell használnia:
  a) visszafejtő (címzett) nyilvános kulcsú tanúsítványa
  b) titkosítás időpontja
  c) fájl név vagy annak megfelelője
  d) titkosítatlan tartalomra képzett lenyomat
  e) a címzett részére aszimmetrikus titkosítással csomagolt titkos kulcs
- **FDP_ITC_ENC.1.2** A TSF-nek el kell végeznie a visszafejtést.

8.2.1.8 Tanúsítvány visszavonási lista (CRL) érvényesítés csomag biztonsági követelményeinek indoklása

O.Accurate_Rev_Info megállapítja: A TSF csak pontos visszavonási információkat fogad el. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_DAU_CRL.1.1** A TSF-nek a CRL-t a következő forrásokból kell beszereznie:a felhasználó nevében végrehajtott folyamat által szolgáltatott tároló, a kérdéses tanúsítvány CRLDistributionPoints kiterjesztése által mutatott cím.
- **FDP_DAU_CRL.1.2** A TSF-nek meg kell szereznie a CRL kibocsátójáról a következő adatokat: megbízható nyilvános kulcs, algoritmus, és a nyilvános kulcs paraméterei.
- **FDP_DAU_CRL.1.3** A TSF-nek a CRL aláírását a következőekkel kell ellenőriznie: a CRL kibocsátójának a megbízható nyilvános kulcsa, algoritmusa, és nyilvános kulcsának paraméterei.
- **FDP_DAU_CRL.1.4** A TSF-nek ellenőriznie kell, hogy a CRL-t kibocsátó tanúsítványában a kritikus keyUsage kiterjesztés jelen legyen és abban a cRLSign bit be legyen állítva.
- **FDP_DAU_CRL.1.5** A TSF-nek a CRL-ben a kibocsátó mezőt egyeztetnie kell a CRL feltételezett kibocsátójával.
- **FDP_DAU_CRL.1.6** A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha thisUpdate mező értékére nézve a következő szabályzat érvényesül:
  current-time <= thisUpdate + x, ahol az x a felhasználó nevében végrehajtott folyamat által megadott érték.
- **FDP_DAU_CRL.1.7** A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha nextUpdate mező értékére nézve a következő szabályzat érvényesül:
  current-time <= nextUpdate + x, ahol az x a felhasználó nevében végrehajtott folyamat által megadott érték.
- **FDP_DAU_CRL.1.8** A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha a felhasználó nevében végrehajtott folyamat felülbírálja a frissesség ellenőrzését.
- **FDP_DAU_CRL.1.9** A TSF-nek vissza kell utasítania a CRL-t, ha az olyan kritikus kiterjesztést tartalmaz, amelyet a TSF nem dolgoz fel.
- **FDP_DAU_CRL.1.10** A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie:
  a) a CRL formátuma X.509

O.Auth_Rev_Info megállapítja: A TSF a visszavonási információkat jogosult CRL forrásból fogadja el. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_DAU_CRL.1.1** A TSF-nek a CRL-t a következő forrásokból kell beszereznie:a felhasználó nevében végrehajtott folyamat által szolgáltatott tároló, a kérdéses tanúsítvány CRLDistributionPoints kiterjesztése által mutatott cím.
- **FDP_DAU_CRL.1.2** A TSF-nek meg kell szereznie a CRL kibocsátójáról a következő adatokat: megbízható nyilvános kulcs, algoritmus, és a nyilvános kulcs paraméterei.
- **FDP_DAU_CRL.1.3** A TSF-nek a CRL aláírását a következőekkel kell ellenőriznie: a CRL kibocsátójának a megbízható nyilvános kulcsa, algoritmusa, és nyilvános kulcsának paraméterei.
- **FDP_DAU_CRL.1.4** A TSF-nek ellenőriznie kell, hogy a CRL-t kibocsátó tanúsítványában a kritikus keyUsage kiterjesztés jelen legyen és abban a cRLSign bit be legyen állítva.
- **FDP_DAU_CRL.1.5** A TSF-nek a CRL-ben a kibocsátó mezőt egyeztetnie kell a CRL feltételezett kibocsátójával.
- **FDP_DAU_CRL.1.6** A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha thisUpdate mező értékére nézve a következő szabályzat érvényesül:
  current-time <= thisUpdate + x, ahol az x a felhasználó nevében végrehajtott folyamat által megadott érték.
- **FDP_DAU_CRL.1.7** A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha nextUpdate mező értékére nézve a következő szabályzat érvényesül:
  current-time <= nextUpdate + x, ahol az x a felhasználó nevében végrehajtott folyamat által megadott érték.
- **FDP_DAU_CRL.1.8** A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha a felhasználó nevében végrehajtott folyamat felülbírálja a frissesség ellenőrzését.
- **FDP_DAU_CRL.1.9** A TSF-nek vissza kell utasítania a CRL-t, ha az olyan kritikus kiterjesztést tartalmaz, amelyet a TSF nem dolgoz fel.
- **FDP_DAU_CRL.1.10** A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie:
  a) a CRL formátuma X.509

O.Fresh_Rev_Info megállapítja: A TSF csak megfelelően időszerű CRL-t fogad el. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_DAU_CRL.1.1** A TSF-nek a CRL-t a következő forrásokból kell beszereznie:a felhasználó nevében végrehajtott folyamat által szolgáltatott tároló, a kérdéses tanúsítvány CRLDistributionPoints kiterjesztése által mutatott cím.
- **FDP_DAU_CRL.1.2** A TSF-nek meg kell szereznie a CRL kibocsátójáról a következő adatokat: megbízható nyilvános kulcs, algoritmus, és a nyilvános kulcs paraméterei.
- **FDP_DAU_CRL.1.3** A TSF-nek a CRL aláírását a következőekkel kell ellenőriznie: a CRL kibocsátójának a megbízható nyilvános kulcsa, algoritmusa, és nyilvános kulcsának paraméterei.
- **FDP_DAU_CRL.1.4** A TSF-nek ellenőriznie kell, hogy a CRL-t kibocsátó tanúsítványában a kritikus keyUsage kiterjesztés jelen legyen és abban a cRLSign bit be legyen állítva.
- **FDP_DAU_CRL.1.5** A TSF-nek a CRL-ben a kibocsátó mezőt egyeztetnie kell a CRL feltételezett kibocsátójával.
- **FDP_DAU_CRL.1.6** A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha thisUpdate mező értékére nézve a következő szabályzat érvényesül:
  current-time <= thisUpdate + x, ahol az x a felhasználó nevében végrehajtott folyamat által megadott érték.
- **FDP_DAU_CRL.1.7** A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha nextUpdate mező értékére nézve a következő szabályzat érvényesül:
  current-time <= nextUpdate + x, ahol az x a felhasználó nevében végrehajtott folyamat által megadott érték.
- **FDP_DAU_CRL.1.8** A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha a felhasználó nevében végrehajtott folyamat felülbírálja a frissesség ellenőrzését.

- **FDP_DAU_CRL.1.9** A TSF-nek vissza kell utasítania a CRL-t, ha az olyan kritikus kiterjesztést tartalmaz, amelyet a TSF nem dolgoz fel.
- **FDP_DAU_CRL.1.10** A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie:
    a) a CRL formátuma X.509

O.User_Override_Fresh_CRL megállapítja: A TSF engedélyezi a felhasználónak, hogy hatástalanítsa a CRL frissességének követelményét. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_DAU_CRL.1** A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie:
- **FDP_DAU_CRL.1.1** A TSF-nek a CRL-t a következő forrásokból kell beszereznie:a felhasználó nevében végrehajtott folyamat által szolgáltatott tároló, a kérdéses tanúsítvány CRLDistributionPoints kiterjesztése által mutatott cím.
- **FDP_DAU_CRL.1.2** A TSF-nek meg kell szereznie a CRL kibocsátójáról a következő adatokat: megbízható nyilvános kulcs, algoritmus, és a nyilvános kulcs paraméterei.
- **FDP_DAU_CRL.1.3** A TSF-nek a CRL aláírását a következőekkel kell ellenőriznie: a CRL kibocsátójának a megbízható nyilvános kulcsa, algoritmusa, és nyilvános kulcsának paraméterei.
- **FDP_DAU_CRL.1.4** A TSF-nek ellenőriznie kell, hogy a CRL-t kibocsátó tanúsítványában a kritikus keyUsage kiterjesztés jelen legyen és abban a cRLSign bit be legyen állítva.
- **FDP_DAU_CRL.1.5** A TSF-nek a CRL-ben a kibocsátó mezőt egyeztetnie kell a CRL feltételezett kibocsátójával.
- **FDP_DAU_CRL.1.6** A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha thisUpdate mező értékére nézve a következő szabályzat érvényesül:
  current-time <= thisUpdate + x, ahol az x a felhasználó nevében végrehajtott folyamat által megadott érték.
- **FDP_DAU_CRL.1.7** A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha nextUpdate mező értékére nézve a következő szabályzat érvényesül:
  current-time <= nextUpdate + x, ahol az x a felhasználó nevében végrehajtott folyamat által megadott érték.
- **FDP_DAU_CRL.1.8** A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha a felhasználó nevében végrehajtott folyamat felülbírálja a frissesség ellenőrzését.
- **FDP_DAU_CRL.1.9** A TSF-nek vissza kell utasítania a CRL-t, ha az olyan kritikus kiterjesztést tartalmaz, amelyet a TSF nem dolgoz fel.
- **FDP_DAU_CRL.1.10** A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie:
    a) a CRL formátuma X.509

8.2.1.9 Időbélyeg kliens csomag biztonsági követelményeinek indoklása

O.Accurate_TSP_Info megállapítja: A TSF csak pontos időbélyeg választ fogad el. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_DAU_TSP.1.3** A TSF-nek ellenőriznie kell, hogy a kapott időbélyeg válasz formátuma az PKIX RFC 3161-nek megfelelő.
- **FDP_DAU_TSP.1.4** A TSF-nek az időbélyeg válaszban a következő alap ellenőrzéseket kell elvégeznie:
  a) ha a státusz nem granted vagy grantedWithMods, akkor nem szerepelhet a válaszban TimeStampToken
  b) ha a státusz nem granted vagy grantedWithMods, akkor a válaszban szerepelnie kell PKIFailureInfo hiba információnak
  c) ha a státusz granted vagy grantedWithMods, akkor a válaszban szerepelnie kell TimeStampToken objektumnak
  d) ha a státusz granted vagy grantedWithMods, akkor a válaszban kapott TimeStampToken tartalom típusa pkcs7-signedData kell, hogy legyen
  e) ha a státusz granted vagy grantedWithMods, akkor a válaszban kapott SignedData tartalom típusa id-ct-TSPInfo kell, hogy legyen
- **FDP_DAU_TSP.1.9** A TSF-nek az időbélyeg válaszban a további ellenőrzéseket kell elvégeznie:
  a) messageImprint azonosságát az időbélyeg kérés messageImprint értékkel
  b) nonce azonosságát az időbélyeg kérés nonce értékkel
  c) ha a kérés tartalmazott TSAPolicyId-t, akkor az azonos-e a válaszban kapott TSAPolicyId értékkel
- **FDP_DAU_TSP.1.10** A TSF-nek el kell utasítania az időbélyeg választ, ha a válasz olyan kritikus kiterjesztést tartalmaz, amelyet a TSF nem képes feldolgozni.
- **FDP_DAU_TSP.1.12** A TSF-nek, amennyiben az aláírás formátuma XAdES v1.3.2 vagy „Egységes MELASZ formátum elektronikus aláírásokra” v2.0, az aláírásban az időbélyeg válaszból (TimeStampResp) kiemelt időbélyeg tokot (TimeStampToken) kell elhelyeznie. A TSF-nek, az ellenőrzés alatt álló aláírásban, amennyiben annak formátuma XAdES v1.3.2-nek vagy „Egységes MELASZ formátum elektronikus aláírásokra”v2.0-nak megfelelő, időbélyeg válasz helyett időbélyeg tokot kell elvárnia. Amennyiben az időbélyeg tok formátuma az RFC 3161-nek megfelelő, a TSF-nek fel kell tételeznie, hogy az időbélyeg tok egy olyan időbélyeg válaszból származik, amelyben a státusz granted.

O.Auth_TSP_Info megállapítja: A TSF az időbélyeg válaszokat csak jogosult TSA forrásból fogadja el. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_DAU_TSP.1.5** A TSF-nek az időbélyeget aláíró tanúsítványt az időbélyeg válaszból kell megismernie.
- **FDP_DAU_TSP.1.6** A TSF-nek a TSA megbízhatóságának megállapítására tanúsítási útvonal érvényesség ellenőrzést kell végrehajtania a Tanúsítási útvonal érvényesítése (CPV) - Alap csomag felhasználásával.
- **FDP_DAU_TSP.1.7** A TSF-nek ellenőriznie kell az időbélyeg válasz aláírását a Tanúsítási útvonal érvényesítése (CPV) - Alap csomag kimenetéből származó nyilvános kulccsal.
- **FDP_DAU_TSP.1.8** A TSF-nek ellenőriznie kell, hogy ha az időbélyeget aláíró tanúsítvány tartalmazza az extendedKeyUsage kiterjesztést, akkor a kiterjesztés tartalmazza-e a PKIX OID-t időbélyeg aláírásra (id_kp_timeStamping).

O.Fresh_TSP_Info megállapítja: A TSF mindig új időbélyeg kérést küld és csak az arra adott időbélyeg választ fogadja el. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_DAU_TSP.1.1** A TSF-nek a PKIX RFC 3161-nek megfelelő formában kell összeállítania az időbélyeg kérést.
- **FDP_DAU_TSP.1.2** Az időbélyeg kérésnek a következő adatokat kell tartalmaznia:

a) kötelezően: verzió, messageImprint, nonce, certReq true értékkel,
b) opcionálisan: reqPolicy, extensions

- **FDP_DAU_TSP.1.9** A TSF-nek az időbélyeg válaszban a további ellenőrzéseket kell elvégeznie:
  a) messageImprint azonosságát az időbélyeg kérés messageImprint értékkel
  b) nonce azonosságát az időbélyeg kérés nonce értékkel
  c) ha a kérés tartalmazott TSAPolicyId-t, akkor az azonos-e a válaszban kapott TSAPolicyId értékkel

O.User_Decide_TSP megállapítja: A TSF engedélyezi a felhasználónak, annak meghatározását, hogy mikor történjen az időbélyeg kérés. Ez a biztonsági célkitűzés találkozik a következő funkcióval:

- **FDP_DAU_TSP.1.11** A TSF-nek az időbélyeg kérést abban az időpontban kell intéznie, amelyet a felhasználó nevében végrehajtott folyamat beállított.

8.2.1.10 Valós idejű tanúsítvány állapot protokoll (OCSP) kliens csomag biztonsági követelményeinek indoklása

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

- **FDP_DAU_OCS.1.7** A TSF-nek össze kell hasonlítania az OCSP válaszból a responderID-t az OCSP válaszadó tanúsítványában található megfelelő információval.
- **FDP_DAU_OCS.1.8** A TSF-nek az OCSP kérésben található certID-t össze kell hasonlítania az OCSP válasz singleResponse-ban található certID-vel.
- **FDP_DAU_OCS.1.13** A TSF-nek vissza kell utasítania az OCSP választ, ha az olyan kritikus kiterjesztést tartalmaz, amelyet a TSF nem dolgoz fel.

O.Auth_OCSP_Info megállapítja: A TSF a visszavonási információkat csak jogosult OCSP forrásból fogadja el.

- **FDP_DAU_OCS.1.3** A TSF-nek az OCSP választ aláíró tanúsítványt az OCSP válaszból kell megismernie.
- **FDP_DAU_OCS.1.4** A TSF-nek a következő további funkciókat kell végrehajtania: az OCSP válaszadó megbízhatóságának megállapítása a Tanúsítási útvonal érvényesítése (CPV) – Alap csomag felhasználásával.
- **FDP_DAU_OCS.1.5** A TSF-nek ellenőriznie kell az OCSP válaszon levő aláírást a Tanúsítási útvonal érvényesítése (CPV) – Alap csomag kimenetéből származó nyilvános kulccsal.
- **FDP_DAU_OCS.1.6** A TSF-nek ellenőriznie kell, hogy ha az OCSP válaszadó tanúsítványa tartalmazza az extendedKeyUsage kiterjesztést, akkor a kiterjesztés tartalmazza-e az id-kp-OCSPSigning OID-t vagy az anyExtendedKeyUsage OID-t.

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

- **FDP_DAU_OCS.1.1** A TSF-nek a PKIX RFC 2560-nek megfelelő formában kell összeállítania az OCSP kérést.
- **FDP_DAU_OCS.1.2** Az OCSP kérésnek tartalmaznia kell a következő kiterjesztéseket: nonce.
- **FDP_DAU_OCS.1.9** A TSF-nek aktuálisnak kell elfogadnia az OCSP választ minden bejegyzés tekintetében, ha az alábbi szabályzat érvényesül:
  current-time <= producedAt + x, ahol x a felhasználó nevében végrehajtott folyamat által megadott érték.
- **FDP_DAU_OCS.1.10** A TSF-nek aktuálisnak kell elfogadnia az OCSP választ egy bejegyzés tekintetében, ha az alábbi szabályzat érvényesül:

current-time <= thisUpdate a bejegyzésből + x, ahol x a felhasználó nevében végrehajtott folyamat által megadott érték.

- **FDP_DAU_OCS.1.11** A TSF-nek aktuálisnak kell elfogadnia az OCSP választ egy bejegyzés tekintetében, ha az alábbi szabályzat érvényesül:
  current-time <= nextUpdate a bejegyzésből + x, ahol x a felhasználó nevében végrehajtott folyamat által megadott érték.
- **FDP_DAU_OCS.1.14** A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie: nonce a kérésből = nonce a válaszból.

O.User_Override_Fresh_OCSP megállapítja: A TSF engedélyezi a felhasználónak, hogy felülbírálja az OCSP válasz frissességének ellenőrzését.

- **FDP_DAU_OCS.1.12** A TSF-nek az OCSP választ aktuálisnak kell elfogadni, ha a felhasználó nevében végrehajtott folyamat felülbírálja a frissesség ellenőrzését.

8.2.2 Garanciális biztonsági követelmények indoklása

A TOE számára választott EAL 3+ kibővített kiértékelési garancia szint azt jelenti, hogy a fejlesztők vagy felhasználók a függetlenül garantált biztonság közepes szintjét követelik meg, a termék és a fejlesztői környezet mélyreható vizsgálatával.

Az EAL 3+ a biztonsági viselkedésmódról következő bizonyítékokat szolgáltatja:

- Biztonsági funkciók analízise (Funkcionális Specifikáció)
- Útmutatók
- A TOE magas-szintű terve (HLD)
- TOE biztonsági funkcióinak független tesztelése
- Fejlesztői átfogó teszt az FS és a HLD alapján
- A fejlesztői teszteredmények független megerősítése
- A biztonsági funkciók erejének értékelése
- Fejlesztői sebezhetőség elemzés

Az EAL 3+ kibővítve az ALC_FLR.1 (A biztonsági rések alapszintű javítása) összetevővel gondoskodik a feltárt és bejelentett biztonsági rések számon tartásáról és kijavításától.

8.2.3 Funkció erősség indoklása

A PP a TOE tervezésénél a „low” támadási potenciált feltételez. Igy az alábbi táblázat alapján a minimális SOF Basic. A kriptográfiai algoritmusok erőssége kívül esik a CC tárgykörén. A funkció erősséget csak a nem kriptográfiai, találati valószinűségi vagy permutációs mechanizmusok esetére kell érteni.

Ez PP család a TOE számára SOF Basic vagy magasabb szintet ír elő.

Range of Values	Resistant to attack with attack potential of:	SOF rating
<10	No rating	No rating
10-17	Low	Basic
18-24	Moderate	Medium
Y25	High	High

A TOE nem alkalmaz nem kriptográfiai, találati valószínűségi vagy permutációs mechanizmusokat.

A TOE nem használ jelszót, PIN kódot, jelmondatot. Mindössze egy GUI felületet biztosít, amelyen a felhasználó megadhatja a PKCS#11 (SSCD eszköz) vagy PKCS#12 (fálj), mint kulcstároló eléréséhez szükséges jelszót. A felhasználó által megadott jelszót a TOE közvetíti, azt a PKCS#11 eszköz, valamint a FIPS 140 sorozat level 1 vagy magasabb szintnek megfelelő kriptográfiai szolgáltató kezeli.

A jelszó, PIN kód jelmondat kezdeti beállítása, annak megváltoztatása a TOE hatókörén kívül esik.

8.3 A TOE összefoglaló specifikáció indoklása

Ez a fejezet a biztonsági funkcionális követelményeket képezi le biztonsági funkciókra és az indoklás az EAL 3+ kibővített szintnek megfelelő.

8.3.1 A TOE biztonsági követelmények kielégítésének indoklása

Az alábbi táblázat megmutatja, hogy a TOE összes biztonsági funkcionális követelménye teljesítve van a biztonsági funkciók által.

58. táblázat: Biztonsági funkcionális követelmények lefedettsége a biztonsági funkciók által

#	Biztonsági funkcionális követelmény	Biztonsági funkció
Alap		
1	FDP_ACC.1.1	SF.IAA
2	FDP_ACF.1.1	SF.IAA
	FDP_ACF.1.2	SF.IAA
	FDP_ACF.1.3	SF.IAA
	FDP_ACF.1.4	SF.IAA
3	FIA_AFL.1.1	SF.IAA
	FIA_AFL.1.2	SF.IAA
4	FIA_ATD.1.1	SF.BASE
5	FIA_UAU.1.1	SF.BASE
	FIA_UAU.1.2	SF.IAA
6	FIA_UAU.7.1	SF.IAA
7	FIA_UID.1.1	SF.IAA
	FIA_UID.1.2	SF.BASE
8	FMT_MSA.1.1	SF.IAA
9	FMT_MSA.3.1	SF.MAN
	FMT_MSA.3.2	SF.MAN
10	FMT_MTD.1.1	SF.IAA
11	FMT_SMF.1.1	SF.BASE
12	FMT_SMR.2.1	SF.IAA
	FMT_SMR.2.1	SF.IAA
	FMT_SMR.2.3	SF.IAA
13	FPT_RVM.1.1	SF.IAA
14	FPT_SEP.1.1	SF.INIT
	FPT_SEP.1.2	SF.BASE
Tanúsítási útvonal érvényesítése (CPV) - Alap		
1	FDP_CPD.1.1	SF.CPV
	FDP_CPD.1.2	SF.CPV
	FDP_CPD.1.3	SF.CPV
	FDP_CPD.1.4	SF.CPV
2	FDP_DAU_CPV_INI.1.1	SF.CPV
	FDP_DAU_CPV_INI.1.2	SF.CPV
	FDP_DAU_CPV_INI.1.3	SF.CPV
	FDP_DAU_CPV_INI.1.4	SF.CPV
3	FDP_DAU_CPV_CER.1.1	SF.CPV
	FDP_DAU_CPV_CER.1.2	SF.CPV
	FDP_DAU_CPV_CER.1.3	SF.CPV

	FDP_DAU_CPV_CER.1.4	SF.CPV
	FDP_DAU_CPV_CER.1.5	SF.CPV
4	FDP_DAU_CPV_CER.2.1	SF.CPV
5	FDP_DAU_CPV_OUT.1.1	SF.CPV
	FDP_DAU_CPV_OUT.1.2	SF.CPV
	FDP_DAU_CPV_OUT.1.3	SF.CPV
	FDP_DAU_CPV_OUT.1.4	SF.CPV
PKI aláírás készítés		
1	FDP_ETC_SIG.1.1	SF.SIGSIV
	FDP_ETC_SIG.1.2	SF.SIGSIV
PKI aláírás ellenőrzés		
1	FDP_ITC_SIG.1.1	SF.SIGSIV
2	FDP_DAU_SIG.1.1	SF.SIGSIV
	FDP_DAU_SIG.1.2	SF.SIGSIV
	FDP_DAU_SIG.1.3	SF.SIGSIV
PKI titkosítás kulcs átviteli algoritmusokkal		
1	FDP_ETC_ENC.1.1	SF.ENCDEC
	FDP_ETC_ENC.1.2	SF.ENCDEC
2	FDP_DAU_ENC.1.1	SF.ENCDEC
	FDP_DAU_ENC.1.2	SF.ENCDEC
PKI visszafejtés kulcs átviteli algoritmusokkal		
1	FDP_ITC_ENC.1.1	SF.ENCDEC
	FDP_ITC_ENC.1.2	SF.ENCDEC
Tanúsítvány visszavonási lista érvényesítés		
1	FDP_DAU_CRL.1.1	SF.CRL
	FDP_DAU_CRL.1.2	SF.CRL
	FDP_DAU_CRL.1.3	SF.CRL
	FDP_DAU_CRL.1.4	SF.CRL
	FDP_DAU_CRL.1.5	SF.CRL
	FDP_DAU_CRL.1.6	SF.CRL
	FDP_DAU_CRL.1.7	SF.CRL
	FDP_DAU_CRL.1.8	SF.CRL
	FDP_DAU_CRL.1.9	SF.CRL
	FDP_DAU_CRL.1.10	SF.CRL
Időbélyeg kliens		
1	FDP_DAU_TSP.1.1	SF.TSP
	FDP_DAU_TSP.1.2	SF.TSP
	FDP_DAU_TSP.1.3	SF.TSP
	FDP_DAU_TSP.1.4	SF.TSP
	FDP_DAU_TSP.1.5	SF.TSP
	FDP_DAU_TSP.1.6	SF.TSP
	FDP_DAU_TSP.1.7	SF.TSP
	FDP_DAU_TSP.1.8	SF.TSP
	FDP_DAU_TSP.1.9	SF.TSP
	FDP_DAU_TSP.1.10	SF.TSP
	FDP_DAU_TSP.1.11	SF.TSP
	FDP_DAU_TSP.1.12	SF.TSP
OCSP kliens		
1	FDP_DAU_OCS.1.1	SF.OCSP
	FDP_DAU_OCS.1.2	SF.OCSP
	FDP_DAU_OCS.1.3	SF.OCSP
	FDP_DAU_OCS.1.4	SF.OCSP
	FDP_DAU_OCS.1.5	SF.OCSP

	FDP_DAU_OCS.1.6	SF.OCSP
	FDP_DAU_OCS.1.7	SF.OCSP
	FDP_DAU_OCS.1.8	SF.OCSP
	FDP_DAU_OCS.1.9	SF.OCSP
	FDP_DAU_OCS.1.10	SF.OCSP
	FDP_DAU_OCS.1.11	SF.OCSP
	FDP_DAU_OCS.1.12	SF.OCSP
	FDP_DAU_OCS.1.13	SF.OCSP
	FDP_DAU_OCS.1.14	SF.OCSP

8.3.1.1 A TOE alap biztonsági követelmények kielégítésének indoklása

FDP_ACC.1.1 megállapítja: A TSF-nek érvényesítenie kell a PKI megbízólevél menedzsment SFP-t a

a) Szubjektum: felhasználó nevében végrehajtott folyamat
b) Objektum: adat, amely a TOE számára átadásra kerül a kriptográfiai művelet végzéséhez, vagy amelyet a TOE ad át tárolásra, vagy egyéb használatra
c) Művelet: a TOE által biztosított kriptográfiai művelet, a TOE működését vezérlő paraméterek beállítása/lekérdezése

között. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.IAA** Hozzáférés ellenőrzés részhalmaza – PKI megbízólevél menedzsment során a PKI megbízólevél menedzsment SFP érvényesítésre kerül a szubjektumok, az objektumok és a műveletek között.

FDP_ACF.1.1 megállapítja: A TSF-nek érvényesítenie kell a PKI megbízólevél menedzsment SFP-t olyan objektumokon, amelyek a szubjektum azonosságán és egy olyan szerep halmazon alapul, amelyet a szubjektum jogosult felvenni. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.IAA** Biztonsági attributum alapú hozzáférés ellenőrzés – PKI megbízólevél menedzsment során a PKI megbízólevél menedzsment SFP érvényesítésre kerül az objektumokon.

FDP_ACF.1.2 megállapítja: A TSF-nek érvényesítenie kell az alábbi szabályokat, hogy megállapíthassa, engedélyezett-e a művelet az ellenőrzött szubjektumok és objektumok között:

a) Magánkulcs importálható, használható, a felhasználó nevében végrehajtott folyamatok által.
b) Nyilvános kulcsú tanúsítványok importálhatók, exportálhatók, törölhetők a felhasználó nevében végrehajtott folyamatok által.
c) Nyilvános kulcsú tanúsítványok használhatók a felhasználó nevében végrehajtott folyamatok által.
d) Titkos kulcs generálható, megsemmisíthető, használható a felhasználó nevében végrehajtott folyamatok által.
e) Titkos kulcs kizárólag aszimmetrikus titkosítással csomagolva importálható és exportálható.

Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.IAA** Biztonsági attributum alapú hozzáférés ellenőrzés – PKI megbízólevél menedzsment során a PKI megbízólevél SFP érvényesítésre kerül a művelet engedélyezésének elbírálására.

FDP_ACF.1.3 megállapítja: A TSF-nek félreérthetetlenül hitelesítenie kell a szubjektumoknak az objektumokhoz való hozzáférését, amely az alábbi kiegészítő szabályokon alapul: nincs további szabály. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.IAA** Biztonsági attributum alapú hozzáférés ellenőrzés – PKI megbízólevél menedzsment során a hozzáférés félreérthetetlenül hitelesítésre kerül minden esetben.

FDP_ACF.1.4 megállapítja: A TSF-nek félreérthetetlenül meg kell tagadnia a szubjektumoknak az objektumokhoz való azon hozzáférést, ha az I&A (a felhasználót azonosító) adatokat tároló eszköz (kulcstároló) az adott pillanatban nem elérhető. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.IAA** Biztonsági attributum alapú hozzáférés ellenőrzés – PKI megbízólevél menedzsment során a hozzáférés megtagadásra kerül, ha a kulcstároló nem elérhető.

FIA_AFL.1.1 megállapítja: A TSF-nek észlelnie kell, amikor a használó alkalmazás által konfigurálható számú sikertelen hitelesítési próbálkozás fordul elő a kijelölt felhasználó azonosság hitelesítésére irányuló utolsó sikeres próbálkozás óta végbement sikertelen hitelesítési próbálkozásokat illetően. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.IAA** Hitelesítési sikertelenség kezelése során a sikertelen hitelesítési próbálkozások száma észlelésre kerül.

FIA_AFL.1.2 megállapítja: Amikor a sikertelen hitelesítési próbálkozások száma elér vagy meghalad egy meghatározott számot, a TSF-nek a TOE képességeinek igénybevételét a használó alkalmazás számára meg kell tagadnia. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.IAA** Hitelesítési sikertelenség kezelése során a sikertelen hitelesítési próbálkozások szám elérésekor a TOE képességei igénybe vétele megtagadásra kerül.

FIA_ATD.1.1 megállapítja: A TSF-nek karban kell tartania az alábbi biztonsági attributum-listát, amely különálló felhasználókhoz tartozik: az I&A (a felhasználót azonosító) adatokat tároló eszköz (kulcstároló) jellemzői. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.BASE** Felhasználói attributum meghatározása során a kulcstároló jellemzők karbantartása felhasználónként elkülönítésre kerül.

FIA_UAU.1.1 megállapítja: A TSF-nek lehetővé kell tenni a használó alkalmazás által konfigurálható paraméterek átadását a felhasználó nevében, mielőtt a felhasználó hitelesítésre kerül. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.BASE** Hitelesítés időzítése során az AHA által konfigurálható paraméterek átadhatóak a hitelesítést megelőzően.

FIA_UAU.1.2 megállapítja: A TSF-nek meg kell követelnie, hogy minden egyes felhasználó sikeresen hitelesítve legyen, mielőtt bármelyik másik TSF által közvetített tevékenységet engedélyezne annak a felhasználónak a nevében. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.IAA** Hitelesítési időzítés során a felhasználó hitelesítésre kerül a tevékenység engedélyezése előtt.

FIA_UAU.7.1 megállapítja: A TSF-nek csak a begépelt karaktereknek csak a * (csillag) mintával történő visszajelzését kell biztosítania a felhasználó számára, mialatt a hitelesítés folyamatban van. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.IAA** Védett hitelesítési visszajelzés során a begépelt karakterek visszajelzése csak a * (csillag) mintával történik.

FIA_UID.1.1 megállapítja: A TSF-nek lehetővé kell tennie a használó alkalmazás által konfigurálható paraméterek átadását a felhasználó nevében, mielőtt a felhasználó azonosítása megtörténik. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.IAA** Azonosítás időzítése: - a felhasználó azonosítása a tevékenység engedélyezése előtt.

FIA_UID.1.2 megállapítja: A TSF-nek meg kell követelnie minden egyes felhasználó sikeres azonosítását, mielőtt bármelyik másik, TSF által közvetített tevékenységet engedélyez annak a felhasználónak a nevében. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.IAA** Azonosítás időzítése során a felhasználó azonosításra kerül a tevékenység engedélyezése előtt.

FMT_MSA.1.1 megállapítja: A TSF-nek érvényre kell juttatnia a PKI megbízólevél menedzsment SFP-t, hogy korlátozza: a lekérdezését, megváltoztatását, törlését, kiválasztását a következő vezérlő biztonsági attributumoknak: az I&A (a felhasználót azonosító) adatok, TOE működését vezérlő paraméterek, kriptográfiai műveleteket befolyásoló paraméterek, az azonosított és hitelesített felhasználó nevében végrehajtott folyamatokra. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.IAA** Biztonsági attributumok menedzsmentje során a biztonsági jellemzők menedzsment korlátozásra kerül az AHA azonosított és hitelesített folyamataira a PKI megbízólevél SFP alapján.

FMT_MSA.3.1 megállapítja: A TSF-nek érvényesítenie kell a PKI megbízólevél menedzsment SFP-t, hogy biztosítsa a megfelelő alapértelmezett értékeket a biztonsági attributumok számára, amelyek az SFP végrehajtásakor használatosak. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.MAN** Statikus attributum inicializáció során a biztonsági jellemzők alapértékei biztosításra kerülnek.

FMT_MSA.3.2 megállapítja: A TSF-nek lehetővé kell tennie a felhasználó nevében végrehajtott folyamat számára a lehetséges kezdeti értékek meghatározását abból a célból, hogy felülírja az alapértékeket, amikor egy objektum vagy információ készül. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.MAN** Statikus attributum inicializáció során az alapértéket az AHA folyamatok meghatározhatják.

FMT_MTD.1.1 megállapítja: A TSF-nek korlátoznia kell a: megváltoztatását, törlését, üresítését, importálását, hozzáadását, a megbízható legfelső szintű hitelesítő tanúsítványok, közbenső szintű hitelesítő tanúsítványok, saját tanúsítványok, más személyek tanúsítványai, tanúsítvány visszavonási listák, a CRL a kibocsátást követően hány napig aktuális, a CRL a következő kibocsátást követő hány napig aktuális, CRL frissesség ellenőrzés engedélyezése, visszavonás ellenőrzés kihagyhatóság engedélyezése, megbízható időszerverek, szolgáltatás igénybevétele utáni kényszerített kijelentkeztetés engedélyezése, OCSP válasz az előállítást követő hány percig aktuális, OCSP válasz a kibocsátást követő hány percig aktuális, OCSP válasz a következő kibocsátást követő hány percig aktuális, OCSP válasz frissesség ellenőrzés engedélyezése, időbélyeg szolgáltatás elérhetősége, OCSP szolgáltatás elérhetősége, szervezeti aláírási szabályzat a felhasználó nevében végrehajtott folyamatokra. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.IAA** TSF adatok menedzsmentje során a biztonsági jellemzők menedzsment korlátozásra kerül az AHA folyamatokra.

FMT_SMF.1.1 megállapítja: A TSF-nek alkalmasnak kell lennie arra, hogy végrehajtsa következő biztonsági menedzsment funkciókat:

a) a használó alkalmazás által konfigurálható paraméterek importálását
b) önellenőrzés
c) azonosítás, hitelesítés és jogosultság ellenőrzés, a felhasználó bejelentkeztetése a kulcstárolóhoz
d) a következő biztonsági attributumok menedzsmentje:
   - megbízható legfelső szintű hitelesítő tanúsítványok,
   - közbenső szintű hitelesítő tanúsítványok

- saját tanúsítványok
- más személyek tanúsítványai
- tanúsítvány visszavonási listák
- a CRL a kibocsátást követően hány napig aktuális
- a CRL a következő kibocsátást követő hány napig aktuális
- CRL frissesség ellenőrzés engedélyezése
- visszavonás ellenőrzés kihagyhatóság engedélyezése
- megbízható időszerverek
- szolgáltatás igénybevétele utáni kényszerített kijelentkeztetés engedélyezése
- OCSP válasz az előállítást követő hány percig aktuális
- OCSP válasz a kibocsátás követő hány percig aktuális
- OCSP válasz a következő kibocsátást követő hány percig aktuális
- OCSP válasz frissesség ellenőrzés engedélyezése
- időbélyeg szolgáltatás elérhetősége
- OCSP szolgáltatás elérhetősége
- szervezeti aláírási szabályzat

e) tanúsítási útvonal érvényesítés
f) CRL érvényesítés
g) elektronikus aláírás létrehozása és ellenőrzése
h) titkosítás és visszafejtés
i) időbélyeg kérés és ellenőrzés
j) OCSP kérés és ellenőrzés

Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.BASE** Menedzsment funkciók specifikációja során a biztonsági funkciók végrehajtásának a képessége biztosításra kerül.

FMT_SMR.2.1 megállapítja: A TSF-nek karban kell tartania a következő szerepeket: felhasználó nevében végrehajtott folyamat. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.IAA** Biztonsági szerepkörök szigorításai során a felhasználó nevében végrehajtott folyamat szerep karbantartásra kerül.

FMT_SMR.2.2 megállapítja: A TSF-nek képesnek kell lennie felhasználók és szerepek összerendelésére. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.IAA** Biztonsági szerepkörök szigorításai során a felhasználók és szerepek összerendelésre kerülnek.

FMT_SMR.2.3 megállapítja: A TSF-nek biztosítania kell, hogy a felhasználó nevében végrehajtott folyamatok feltételei ki legyenek elégítve. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.IAA** Biztonsági szerepkörök szigorításai során a felhasználó nevében végrehajtott folyamatok feltételei kielégítésre kerülnek.

FPT_RVM.1.1 megállapítja: TSF-nek biztosítania kell, hogy a TSP-t érvényre juttató funkciói meghívásra kerülnek és sikeresen végrehajtódnak, mielőtt minden egyes TSF irányítási tárgykör (TSC) funkció továbbhaladása engedélyeződne. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.IAA** A TSP kikerülhetetlensége során a TSP kényszerítő funkciói sikeresen végrehajtásra kerülnek a TSC továbbhaladás engedélyezése előtt.

FPT_SEP.1.1 megállapítja: A TSF-nek fenn kell tartania a saját végrehajtása számára egy biztonsági körzetet, amely védelmet nyújt a nem megbízható szubjektumok általi beavatkozás és meghamisítás ellen. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.INIT** TSF körzetszétválasztás során védelmet nyújt a nem megbízható szubjektumok általi beavatkozás és megmásítás ellen.

FPT_SEP.1.2 megállapítja: A TSF-nek érvényesítenie kell a TSC szubjektumainak biztonsági körzeteinek egymástól való elkülönítését. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.BASE** TSF körzetszétválasztás során a TSC szubjektumok biztonsági körzetei egymástól elkülönítésre kerülnek.

8.3.1.2 Tanúsítási útvonal érvényesítése (CPV) – Alap csomag biztonsági követelmények kielégítésének indoklása

FDP_CPD.1.1 megállapítja: A TSF-nek az érvényesítési útvonalat a felhasználó nevében végrehajtott folyamat által szolgáltatott megbízható legfelső szintű hitelesítő tanúsítvánnyal kezdve a végtanúsítványig kell felépítenie, a következő tanúsítvány mezők vagy kiterjesztések egyezőségi szabályait alkalmazva: distinguished name. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Tanúsítási útvonal felépítése az AHA folyamat által megadott megbízható tanúsítvánnyal kezdve kezdődik és a végtanúsítványig tart, a distinguished name egyezősége alapján.

FDP_CPD.1.2 megállapítja: A TSF-nek a tanúsítási útvonalat a következő kiegészítő egyezőségi szabályok alkalmazásával kell felépítenie:

a) aláírás ellenőrzése esetén:
   aa) ha aláírási szabályzat nincs érvényben, akkor a keyUsage kiterjesztésben a nonRepudiation bit be van állítva
   ab) ha aláírási szabályzat érvényben van, akkor annak rendelkezéseitől függően: a keyUsage kiterjesztésben a nonRepudiation vagy digitalSignature bit be van állítva
b) a keyUsage kiterjesztésben a digitalSignature bit be van állítva, entitás hitelesítése esetén
c) a keyUsage kiterjesztésben a keyEncipherment bit be van állítva, titkosítás, visszafejtés esetén

Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Tanúsítási útvonal felépítése során a kulcshasználat ellenőrzésre kerül.

FDP_CPD.1.3 megállapítja: A TSF-nek a tanúsítási útvonalat a következő kiegészítő egyezőségi szabályok alkalmazásával kell felépítenie:

a) nincs további szabály az extendedKeyUsage kiterjesztés tartalmára

Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Tanúsítási útvonal felépítése során az extendedKeyUsage tartalmára nincs szabály.

FDP_CPD.1.4 megállapítja: A TSF kikerülhet bármely egyezőségi szabályt, kivéve:

a) distinguished name
b) a tanúsítvány formátuma X.509

amennyiben további tanúsítási útvonalak szükségesek.. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Tanúsítási útvonal felépítése során a distinguished name és X.509 formátum szabály kivételével a további szabályok kikerülhetők.

FDP_DAU_CPV_INI.1.1 megállapítja: A TSF-nek a felhasználó nevében végrehajtott folyamat által szolgáltatott megbízható legfelső szintű hitelesítő tanúsítványt kell használnia. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Tanúsítási útvonal inicializálása során az AHA folyamat által megadott megbízható legfelső szintű hitelesítő tanúsítványok lesznek használva.

FDP_DAU_CPV_INI.1.2 megállapítja: A TSF-nek a felhasználó nevében végrehajtott folyamat által meghatározott időszerverektől vagy ha az nem áll rendelkezésre, akkor a lokális környezetből, mint megbízható forrásból kell megszereznie az aktuális időt, amelyet 'current-time'-nak nevezünk. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Tanúsítási útvonal inicializálása során az aktuális idő megszerzésre kerül az AHA folyamat által megadott időszerverektől, vagy az aktuális környezetből.

FDP_DAU_CPV_INI.1.3 megállapítja: A TSF-nek a megbízható legfelső szintű tanúsítványok esetében a következő ellenőrzéseket kell elvégeznie:

a) Subject DN és az Issuer DN egyezik
b) A tanúsítványon az aláírás érvényes, a megbízható legfelső szintű hitelesítő tanúsítvány alanyának nyilvános kulcsával és annak paraméterével (ha az rendelkezésre áll) ellenőrizve
c) a megbízható legfelső szintű tanúsítvány notBefore mezője <= current-time
d) a megbízható legfelső szintű tanúsítvány notAfter mezője => current-time

Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Tanúsítási útvonal inicializálása során a megbízható legfelső szintű tanúsítvány ellenőrzésre kerül.

FDP_DAU_CPV_INI.1.4 megállapítja: A TSF-nek a megbízható legfelső szintű hitelesítő tanúsítványból származtatnia kell a következő információkat: subject DN, subject public key, subject public key algorithm object identifier, subject public key paraméterek. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Tanúsítási útvonal inicializálása során az információk származtatása a megbízható legfelső szintű tanúsítványból történik.

FDP_DAU_CPV_CER.1.1 megállapítja: A TSF-nek a tanúsítványt csak akkor szabad elfogadnia, ha a következő ellenőrzések sikeresen megtörténtek:

a) A tanúsítványon az aláírás ellenőrzése a következőekkel: parent-public-key, parent-public-key-algorithm-identifier, és parent-public-key-parameters
b) A tanúsítvány notBefore mezője < = current-time
c) A tanúsítvány notAfter mezője > = current-time
d) A tanúsítvány issuer mezője = parent-DN
e) A TSF képes a tanúsítvány minden kritikus kiterjesztését feldolgozni.

Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Tanúsítvány feldolgozás során a tanúsítvány ellenőrzésre kerül.

FDP_DAU_CPV_CER.1.2 megállapítja: A TSF kikerülheti a visszavonási állapot ellenőrzését, ha a tanúsítvány tartalmazza a no-check kiterjesztést. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Tanúsítvány feldolgozás során a visszavonási állapot ellenőrzése kihagyásra kerül a no-check kiterjesztés esetén.

FDP_DAU_CPV_CER.1.3 megállapítja: A TSF-nek ki kell hagynia a visszavonás ellenőrzését, ha a visszavonási információ nem áll rendelkezésre és a felhasználó nevében végrehajtott folyamat felülbírálja a visszavonás ellenőrzést. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Tanúsítvány feldolgozás során a visszavonási állapot ellenőrzés kihagyásra kerül, ha az AHA folyamat felülbírálta azt.

FDP_DAU_CPV_CER.1.4 megállapítja: A TSF-nek el kell fogadnia a tanúsítványt, ha a visszavonási állapot CRL ellenőrzése vagy OCSP ellenőrzés alapján, meggyőződött arról, hogy a tanúsítvány nincs visszavonva. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Tanúsítvány feldolgozás során a tanúsítvány elfogadásra kerül, ha az a CRL ellenőrzése alapján nincs visszavonva.

FDP_DAU_CPV_CER.1.5 megállapítja: A TSF-nek nyilvános kulcs paraméterei állapotgépet a következő szabályok szerint kell vezérelnie:

a) a paraméter megállapítása a tanúsítvány subjectPublickeyInfo mezőjéből, ha abban szerepel a paraméter, különben
b) az eredeti paraméter állapot megtartása, ha az aktuális tanúsítvány nyilvános kulcsának algoritmusa és a kibocsátó nyilvános kulcsának algoritmusa azonos algoritmus családba tartozik, különben
c) a paramétert be kell állítani „null” értékre.

Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Tanúsítvány feldolgozás során a nyilvános kulcs paraméterei állapotgép szabályai alkalmazásra kerülnek.

FDP_DAU_CPV_CER.2.1 megállapítja: A TSF-nek a közbenső tanúsítványt csak akkor kell elfogadnia, ha a következő ellenőrzések sikeresen megtörténtek:

a) basicConstraints kiterjesztés jelen van, és abban a cA = TRUE
b) pathLenConstraint kényszer teljesül
c) ha kritikus keyUsage kiterjesztés jelen van, akkor abban a keyCertSign bit be van állítva

Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Közbenső tanúsítvány feldolgozás során a közbenső tanúsítvány elfogadásának feltételei ellenőrzésre kerülnek.

FDP_DAU_CPV_OUT.1.1 megállapítja: A TSF-nek tanúsítási útvonal érvényesítési hibát kell visszaadnia, ha az tanúsítási útvonalban bármely tanúsítvány visszautasításra került. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Tanúsítási útvonal kimenetében hiba visszaadása, ha a tanúsítási útvonalban bármely tanúsítvány visszavonásra került.

FDP_DAU_CPV_OUT.1.2 megállapítja: A végtanúsítványból a TSF-nek a következő változókat kell visszaadnia: subject DN, subject public key algorithm identifier, subject public key, kritikus keyUsage kiterjesztés. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Tanúsítási útvonal kimenetében az alany, nyilvános kulcs és további adatok visszaadása a végtanúsítványból.

FDP_DAU_CPV_OUT.1.3 megállapítja: A végtanúsítványból a TSF-nek a következő további változókat kell visszaadnia: tanúsítvány, subject alternative names, tanúsítvány lánc, extendedKeyUsage. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Tanúsítási útvonal kimenetében a végtanúsítvány, az alternatív nevek, tanúsítvány lánc és extendedKeyUsage visszaadása a végtanúsítványból.

FDP_DAU_CPV_OUT.1.4 megállapítja: A TSF-nek az alany nyilvános kulcs paramétereit a tanúsítási útvonal paraméter állapotgép alapján kell visszaadnia. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CPV** Tanúsítási útvonal kimenetében a nyilvános kulcs visszaadása a tanúsítási útvoval állapotgép alapján történik.

8.3.1.3 PKI aláírás készítés csomag biztonsági követelmények kielégítésének indoklása

FDP_ETC_SIG.1.1 megállapítja: A TSF-nek a magánkulcs felhasználásával elektronikus aláírást kell létrehozni. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.SIGSIV** PKI aláírás exportálása során a magánkulcs használatával az aláírás létrehozása.

FDP_ETC_SIG.1.2 megállapítja: A TSF-nek az elektronikus aláírásba a következő aláírást kísérő információkat kell befoglalnia:

1)A1-kombatibilis elektronikus aláírás készítése esetén:

a)kötelezően: hash algoritmus, aláírási algoritmus, aláíró nyilvános kulcs, aláíró DN, aláíró tanúsítványt kibocsátó DN, aláíró tanúsítványának sorozatszáma, aláíró tanúsítványa, aláíró tanúsítványának az érvényesített tanúsítási útvonala, aláírás időpontja

b)opcionálisan: aláírás helye(város), aláírás helye(irányítószám), aláírás helye(megye), aláírás helye(ország), aláíró szerepkör

2)A2 elektronikus aláírás készítése esetén:

a)„Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára (2005. november 22.)” választása esetén:

aa)kötelezően:

- kanonizálási módszer (CanonicalizationMethod), a http://www.w3.org/TR/2001/REC-xml-c14n-20010315 értékkel
- aláírási algoritmus (SignatureMethod) az RSAwithSHA1 értékkel
- aláírt dokumentumok külső vagy belső hivatkozásai (Reference)
- transzformációk (Transforms) az http://www.w3.org/TR/2001/REC-xml-c14n-20010315 vagy http://www.w3.org/2000/09/xmldsig#BASE64 értékkel
- lenyomatképző algoritmus (DigestMethod) az SHA1 értékkel
- az aláíró tanúsítványa (KeyInfo)
- aláírás időpontja (SigningTime)
- hivatkozás az aláíró tanúsítványára (SigningCertificate)
- aláírási szabályzat (SignaturePolicyIdentifier)
- aláírt dokumentumok adatformátum leírásai (DataObjectFormat)

ab)opcionálisan:

- az aláíró nyilvános kulcsa (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)
- aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)
- aláíró szerepkörei (SignerRole)
- kötelezettségvállalás jelzése (CommitmentTypeIndication)
- aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)
- ellenjegyző aláírás (CounterSignature)
- aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)

- hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)
- aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)
- referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)
- archív időbélyeg(ek) (ArchiveTimeStamp)

b)v1.2.2 vagy v1.3.2 szabványos formátum választása esetén:

ba)kötelezően:

- kanonizálási módszer (CanonicalizationMethod) http://www.w3.org/TR/2001/REC-xml-c14n-20010315, http://www.w3.org/TR/2001/REC-xml-c14n-0010315#WithComments, http://www.w3.org/TR/2001/REC-xml-c14n-20010315, http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments, http://www.w3.org/2006/12/xml-c14n11, http://www.w3.org/2006/12/xml-c14n11#WithComments
- aláírási algoritmus (SignatureMethod) RSAwithSHA1, RSAwithSHA256, RSAwithSHA384, RSAwithSHA512 vagy DSAwithSHA1
- aláírt dokumentumok külső vagy belső hivatkozásai (Reference)
- transzformációk (Transforms)
- lenyomatképző algoritmus (DigestMethod)
- az aláíró tanúsítványa (KeyInfo)
- aláírás időpontja (SigningTime)
- hivatkozás az aláíró tanúsítványára (SigningCertificate)

bb)opcionálisan:

- az aláíró nyilvános kulcsa (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)
- aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)
- aláíró szerepkörei (SignerRole)
- aláírási szabályzat (SignaturePolicyIdentifier)
- aláírt dokumentumok adatformátum leírásai (DataObjectFormat
- kötelezettségvállalás jelzése (CommitmentTypeIndication)
- aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)
- ellenjegyző aláírás (CounterSignature)
- aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)
- aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)
- referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)

- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)
- archív időbélyeg(ek) (ArchiveTimeStamp)

c)„Egységes MELASZ formátum elektronikus aláírásokra” v2.0 választása esetén:
ca)kötelezően:

- kanonizálási módszer (CanonicalizationMethod), a http://www.w3.org/TR/2001/REC-xml-c14n-20010315 értékkel
- aláírási algoritmus (SignatureMethod) az RSAwithSHA1 vagy RSAwithSHA256 értékkel
- aláírt dokumentumok külső vagy belső hivatkozásai (Reference)
- transzformációk (Transforms) az http://www.w3.org/TR/2001/REC-xml-c14n-20010315 vagy http://www.w3.org/2000/09/xmldsig#BASE64 értékkel
- lenyomatképző algoritmus (DigestMethod) az SHA1 vagy SHA256 értékkel
- az aláíró tanúsítványa (KeyInfo)
- aláírás időpontja (SigningTime)
- hivatkozás az aláíró tanúsítványára (SigningCertificate)
- aláírási szabályzat (SignaturePolicyIdentifier)
- aláírt dokumentumok adatformátum leírásai (DataObjectFormat)

cb)opcionálisan:

- az aláíró nyilvános kulcsa (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)
- aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)
- aláíró szerepkörei (SignerRole)
- kötelezettségvállalás jelzése (CommitmentTypeIndication)
- aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)
- ellenjegyző aláírás (CounterSignature)
- aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)
- aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)
- referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)
- archív időbélyeg(ek) (ArchiveTimeStamp)

Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.SIGSIV** PKI aláírás exportálása során a magánkulcs használatával az aláírás létrehozása.

8.3.1.4 PKI aláírás ellenőrzés csomag biztonsági követelmények kielégítésének indoklása

FDP_ITC_SIG.1.1 megállapítja: A TSF-nek az alábbi aláírást kísérő információkat kell használnia az aláírás ellenőrzése során:

1)A1-kombatibilis elektronikus aláírás ellenőrzése esetén:

a)kötelezően: hash algoritmus, aláírási algoritmus, aláíró nyilvános kulcs, aláíró DN, aláíró tanúsítványt kibocsátó DN, aláíró tanúsítványának sorozatszáma, aláíró tanúsítványa, aláíró tanúsítványának az érvényesített tanúsítási útvonala, aláírás időpontja

b)opcionálisan: aláírás helye(város), aláírás helye(irányítószám), aláírás helye(megye), aláírás helye(ország), aláíró szerepkör

2)A2 elektronikus aláírás ellenőrzés esetén:

a)„Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára (2005. november 22.)" formátumnak vagy az „Egységes MELASZ formátum elektronikus aláírásokra" v2.0 dokumentumnak megfelelő aláírás ellenőrzése esetén:

aa)kötelezően:

- kanonizálási módszer (CanonicalizationMethod)
- aláírási algoritmus (SignatureMethod)
- aláírt dokumentumok külső vagy belső hivatkozásai (Reference)
- transzformációk (Transforms)
- lenyomatképző algoritmus (DigestMethod)
- az aláíró tanúsítványa (KeyInfo)
- aláírás időpontja (SigningTime)
- hivatkozás az aláíró tanúsítványára (SigningCertificate)
- aláírási szabályzat (SignaturePolicyIdentifier)
- aláírt dokumentumok adatformátum leírásai (DataObjectFormat)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)

ab)opcionálisan:

- az aláíró nyilvános kulcsa (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)
- aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)
- aláíró szerepkörei (SignerRole)
- kötelezettségvállalás jelzése (CommitmentTypeIndication)
- aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)
- ellenjegyző aláírás (CounterSignature)
- aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)
- aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)
- referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)
- archív időbélyeg(ek) (ArchiveTimeStamp)

b)szabványos formátumnak megfelelő aláírás ellenőrzése esetén:
ba)kötelezően:
- kanonizálási módszer (CanonicalizationMethod)
- aláírási algoritmus (SignatureMethod)
- aláírt dokumentumok külső vagy belső hivatkozásai (Reference)
- transzformációk (Transforms)
- lenyomatképző algoritmus (DigestMethod)
- az aláíró tanúsítványa (KeyInfo)
- aláírás időpontja (SigningTime)
- hivatkozás az aláíró tanúsítványára (SigningCertificate)

bb)opcionálisan:
- az aláíró nyilvános kulcsa (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványok (KeyInfo)
- az aláírói tanúsítványhoz felépített láncot alkotó tanúsítványokhoz a visszavonási információk (KeyInfo)
- aláírás helye (város, irányítószám, megye, ország) (SignatureProductionPlace)
- aláíró szerepkörei (SignerRole)
- aláírási szabályzat (SignaturePolicyIdentifier)
- aláírt dokumentumok adatformátum leírásai (DataObjectFormat
- kötelezettségvállalás jelzése (CommitmentTypeIndication)
- aláírást megelelőzően készített időbélyeg(ek) (AllDataObjectsTimeStamp vagy IndividualDataObjectsTimeStamp)
- ellenjegyző aláírás (CounterSignature)
- aláírás időpontját hitelesítő időbélyeg(ek) (SignatureTimeStamp)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonal elemeire (CompleteCertificateRefs)
- hivatkozás az aláírói tanúsítványhoz és az időbélyeget aláíró tanúsítványhoz felépetett tanúsítási útvonal elemeihez a visszavonási információkra (CRL vagy OCSP) (CompleteRevocationRefs)
- aláírást és referenciákat magában foglaló időbélyeg(ek) OCSP visszavonási információ esetén (SigAndRefsTimeStamp)
- referenciákat magában foglaló időbélyeg(ek) CRL visszavonási információ esetén (RefsOnlyTimeStamp)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványok (CertificateValues)
- aláírói tanúsítványhoz és az időbélyeg(ek)et aláíró tanúsítványhoz felépített tanúsítási útvonalat alkotó tanúsítványokhoz a visszavonási információk (CRL vagy OCSP) (RevocationValues)
- archív időbélyeg(ek) (ArchiveTimeStamp)

Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:
- **SF.SIGSIV** PKI aláírás importálása során az aláírást kísérő információk használva lesznek.

FDP_DAU_SIG.1.1 megállapítja: A TSF-nek a Tanúsítási útvonal érvényesítése (CPV) - Alap csomagból a következő információkat kell használnia: subject public key algorithm, subject public key, subject public key parameters, amikor az aláírt adaton az elektronikus aláírást ellenőrzi. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:
- **SF.SIGSIV** Aláírás bináris ellenőrzése során az aláírás ellenőrzéséhez az SF.CPV biztonsági funkcióból származó adatok kötelezően használva lesznek.

FDP_DAU_SIG.1.2 megállapítja: A TSF-nek ellenőriznie kell, hogy a Tanúsítási útvonal érvényesítése (CPV) - Alap csomag által visszaadott keyUsage kiterjesztésben a nonRepudiation bit vagy a digitalSignature bit be van állítva. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.SIGSIV** Aláírás bináris ellenőrzése során a kulcshasználat (nonRepudiation) az SF.CPV biztonsági funkció kimenetében ellenőrzésre kerül.

FDP_DAU_SIG.1.3 megállapítja: A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie:

a) Tanúsítási útvonal érvényesítése (CPV) - Alap csomag által visszaadott subject DN egyezik az aláírási információkkal.
b) a tanúsítvány keyUsage kiterjesztésében:
ba) ha aláírási szabályzat nincs érvényben, akkor kizárólag csak a nonRepudiation bit van beállítva
bb) ha aláírási szabályzat van érvényben, akkor annak rendelkezésétől függően az alábbiak valamelyike:
- kizárólag csak a nonRepudiation bit van beállítva
- kizárólag csak a digitalSignature bit van beállítva
- a nonRepudiation bit van beállítva, a többi bit nem számít
- a digitalSignature bit van beállítva, a többi bit nem számít
c) szigorú üzemmódban a minősített elektronikus aláírás esetén az aláíró tanúsítványában a kötelező qcStatements kiterjesztésben az id-etsi-qcs-QcCompliance OID meglétének ellenőrzése

Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.SIGSIV** Aláírás bináris ellenőrzése során az aláíró DN az SF.CPV biztonsági funkció kimenetével egyeztetésre kerül, ha aláírási szabályzat nincs érvényben, akkor a keyUsage kiterjesztésben kizárólag csak a nonRepudiation bit beállítottsága, ha aláírási szabályzat érvényben van, akkor annak előírásai szerint a nonRepudiation és digitalSignature bit vizsgálata, a minősített elektronikus aláíráshoz a kötelező qcStatements kiterjesztésben az id-etsi-qcs-QcCompliance OID megléte ellenőrzésre kerül.

8.3.1.5 PKI titkosítás kulcs átviteli algoritmusokkal csomag biztonsági követelmények kielégítésének indoklása

FDP_ETC_ENC.1.1 megállapítja: A TSF-nek a következő információkat kell a titkosított adattal együtt biztosítania:

a) visszafejtő (címzett) nyilvános kulcsú tanúsítványa
b) titkosítás időpontja
c) fájl név vagy annak megfelelője
d) titkosítatlan tartalomra képzett lenyomat
e) a címzett részére aszimmetrikus titkosítással csomagolt titkos kulcs

Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.ENCDEC** PKI titkosítás exportja során a titkosított adathoz a titkosítást kísérő információk csatolásra kerülnek.

FDP_ETC_ENC.1.2 megállapítja: A TSF-nek a Tanúsítási útvonal érvényesítése (CPV) - Alap csomagból a következő információkat kell használnia a titkosított adat létrehozásakor: subject public key algorithm, subject public key, subject public key paraméterek. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.ENCDEC** PKI titkosítás exportja során a nyilvános kulcs adatok az SF.CPV biztonsági funkció kimenetéből lesznek használva.

FDP_DAU_ENC.1.1 megállapítja: A TSF-nel ellenőriznie kell, hogy a Tanúsítási útvonal érvényesítése (CPV) - Alap csomagból visszaadott keyUsage kiterjesztésben a keyEncipherment bit be van állítva. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.ENCDEC** PKI titkosítás ellenőrzése során a kulcshasználat (keyEncipherment) az SF.CPV biztonsági funkció kimenetében ellenőrzésre kerül.

FDP_DAU_ENC.1.2 A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie:
a) a visszafejtett tartalomra képzett lenyomat megegyezik-e az eredeti lenyomattal.
Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.ENCDEC** PKI titkosítás ellenőrzése során a lenyomat egyeztetésre kerül.

8.3.1.6 PKI visszafejtés kulcs átviteli algoritmusokkal csomag biztonsági követelmények kielégítésének indoklása

FDP_ITC_ENC.1.1 megállapítja: A TSF-nek a titkosított adatról a következő információkat kell használnia:
a) visszafejtő (címzett) nyilvános kulcsú tanúsítványa
b) titkosítás időpontja
c) fájl név vagy annak megfelelője
d) titkosítatlan tartalomra képzett lenyomat
e) a címzett részére aszimmetrikus titkosítással csomagolt titkos kulcs
Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.ENCDEC** PKI titkosítás importja során a titkosítást kísérő információk lesznek használva.

FDP_ITC_ENC.1.2 megállapítja*:* A TSF-nek el kell végeznie a visszafejtést. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.ENCDEC** PKI titkosítás importja során a visszafejtés elvégészésre kerül.

8.3.1.7 Tanúsítvány visszavonási lista (CRL) érvényesítés csomag biztonsági követelmények kielégítésének indoklása

FDP_DAU_CRL.1.1 megállapítja: A TSF-nek a CRL-t a következő forrásokból kell beszereznie:a felhasználó nevében végrehajtott folyamat által szolgáltatott tároló. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CRL** Alap CRL ellenőrzés során a CRL beszerzése az AHA folyamat által szolgáltatott tárolóból történik, vagy a kérdéses tanúsítvány CRLDistributionPoints kiterjesztése által mutatott címről.

FDP_DAU_CRL.1.2 megállapítja: A TSF-nek meg kell szereznie a CRL kibocsátójáról a következő adatokat: megbízható nyilvános kulcs, algoritmus, és a nyilvános kulcs paraméterei.
Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CRL** Alap CRL ellenőrzés során a a CRL kibocsátó nyilvános kulcsának adatai megszerzésre kerülnek.

FDP_DAU_CRL.1.3 megállapítja: A TSF-nek meg kell szereznie a CRL kibocsátójáról a következő adatokat: megbízható nyilvános kulcs, algoritmus, és a nyilvános kulcs paraméterei. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CRL** Alap CRL ellenőrzés során a CRL aláírása a megbízható nyilvános kulccsal ellenőrzésre kerül.

FDP_DAU_CRL.1.4 megállapítja: A TSF-nek ellenőriznie kell, hogy a CRL-t kibocsátó tanúsítványában a kritikus keyUsage kiterjesztés jelen legyen és abban a cRLSign bit be legyen állítva. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CRL** Alap CRL ellenőrzés során a CRL-t kibocsátó tanúsítványában a kulcshasználat (cRLSign) ellenőrzésre kerül.

FDP_DAU_CRL.1.5 megállapítja: A TSF-nek a CRL-ben a kibocsátó mezőt egyeztetnie kell a CRL feltételezett kibocsátójával. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CRL** Alap CRL ellenőrzés során CRL kibocsátó mezője egyeztetésre kerül a feltételezett kibocsátóval.

FDP_DAU_CRL.1.6 megállapítja: A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha thisUpdate mező értékére nézve a következő szabályzat érvényesül:
current-time <= thisUpdate + x, ahol az x a felhasználó nevében végrehajtott folyamat által megadott érték. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CRL** Alap CRL ellenőrzés során a CRL aktuálisnak kerül elfogadásra, a CRLAfterThisUpdateLimit ellenőrzés teljesülésekor.

FDP_DAU_CRL.1.7 megállapítja: A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha nextUpdate mező értékére nézve a következő szabályzat érvényesül:
current-time <= nextUpdate + x, ahol az x a felhasználó nevében végrehajtott folyamat által megadott érték. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CRL** Alap CRL ellenőrzés során a CRL aktuálisnak kerül elfogadásra, a CRLAfterNextUpdateLimit ellenőrzés teljesülésekor.

FDP_DAU_CRL.1.8 megállapítja: A TSF-nek a CRL-t el kell fogadnia, mint aktuális, ha a felhasználó nevében végrehajtott folyamat felülbírálja a frissesség ellenőrzését. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CRL** Alap CRL ellenőrzés során a CRL aktuálisnak kerül elfogadásra, ha az AHA folyamat felülbírálja a frissesség ellenőrzését.

FDP_DAU_CRL.1.9 megállapítja: A TSF-nek vissza kell utasítania a CRL-t, ha az olyan kritikus kiterjesztést tartalmaz, amelyet a TSF nem dolgoz fel. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CRL** Alap CRL ellenőrzés során a fel nem dolgozott kritikus kiterjesztést tartalmazó CRL visszautasításra kerül.

FDP_DAU_CRL.1.10 megállapítja: A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie:

a) a CRL formátuma X.509.

Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.CRL** Alap CRL ellenőrzés során az X.509 formátum ellenőrzésre kerül.

8.3.1.8 Időbélyeg kliens csomag biztonsági követelmények kielégítésének indoklása

FDP_DAU_TSP.1.1 megállapítja: A TSF-nek a PKIX RFC 3161-nek megfelelő formában kell összeállítania az időbélyeg kérést. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.TSP** Az időbélyegek kérése az RFC 3161-nek megfelelően történik.

FDP_DAU_TSP.1.2 megállapítja: Az időbélyeg kérésnek a következő adatokat kell tartalmaznia:

a) kötelezően: verzió, messageImprint, nonce, certReq true értékkel,
b) opcionálisan: reqPolicy, extensions.

Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.TSP** Az időbélyeg kötelezően tartalmazza a verzió, messageImprint, nonce true értékkel, opcionálisan tartalmazza a reqPolicy, extensions adatokat.

FDP_DAU_TSP.1.3 megállapítja: A TSF-nek ellenőriznie kell, hogy a kapott időbélyeg válasz formátuma az PKIX RFC 3161-nek megfelelő. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.TSP** Az időbélyegek ellenőrzése az RFC 3161-nek megfelelően történik.

FDP_DAU_TSP.1.4 megállapítja: A TSF-nek az időbélyeg válaszban a következő alap ellenőrzéseket kell elvégeznie:

a) ha a státusz nem granted vagy grantedWithMods, akkor nem szerepelhet a válaszban TimeStampToken
b) ha a státusz nem granted vagy grantedWithMods, akkor a válaszban szerepelnie kell PKIFailureInfo hiba információnak
c) ha a státusz granted vagy grantedWithMods, akkor a válaszban szerepelnie kell TimeStampToken objektumnak
d) ha a státusz granted vagy grantedWithMods, akkor a válaszban kapott TimeStampToken tartalom típusa pkcs7_signedData kell, hogy legyen
e) ha a státusz granted vagy grantedWithMods, akkor a válaszban kapott SignedData tartalom típusa id_ct_TSPInfo kell, hogy legyen

Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.TSP** Az időbélyeg válaszban a tartalmi és formai követelmények ellenőrzésre kerülnek.

FDP_DAU_TSP.1.5 megállapítja: A TSF-nek az időbélyeget aláíró tanúsítványt az időbélyeg válaszból kell megismernie. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.TSP** Az időbélyeget aláíró tanúsítvány megismerése az időbélyeg válaszból történik.

FDP_DAU_TSP.1.6 megállapítja: A TSF-nek a TSA megbízhatóságának megállapítására tanúsítási útvonal érvényesség ellenőrzést kell végrehajtania a Tanúsítási útvonal érvényesítése (CPV) - Alap csomag felhasználásával. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.TSP** Az időbélyeget szolgáltató TSA megbízhatóságának a megállapítása a a Tanúsítási útvonal érvényesítése (CPV) – Alap csomaggal történik.

FDP_DAU_TSP.1.7 megállapítja: A TSF-nek ellenőriznie kell az időbélyeg válasz aláírását a Tanúsítási útvonal érvényesítése (CPV) - Alap csomag kimenetéből származó nyilvános kulccsal. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.TSP** Az időbélyegen az aláírás a Tanúsítási útvonal érvényesítése (CPV) – Alap csomag kimenetéből származó nyilvános kulccsal kerül ellenőrzésre.

FDP_DAU_TSP.1.8 megállapítja: A TSF-nek ellenőriznie kell, hogy ha az időbélyeget aláíró tanúsítvány tartalmazza az extendedKeyUsage kiterjesztést, akkor a kiterjesztés tartalmazza-e a PKIX OID-t időbélyeg aláírásra (id_kp_timeStamping). Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.TSP** Az időbélyeget aláíró tanúsítvány extendedKeyUsage kiterjesztése ellenőrzésre kerül, ha azt tartalmazza, akkor abban a kulcshasználat céljának időbélyeg aláírásnak kell lennie.

FDP_DAU_TSP.1.9 megállapítja: A TSF-nek az időbélyeg válaszban a további ellenőrzéseket kell elvégeznie:

a) messageImprint azonosságát az időbélyeg kérés messageImprint értékkel
b) nonce azonosságát az időbélyeg kérés nonce értékkel
c) ha a kérés tartalmazott TSAPolicyId-t, akkor az azonos-e a válaszban kapott TSAPolicyId értékkel

Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.TSP** A kapott időbélyet válaszban a messageImprint, nonce TSAPolicyID azonossága a küldött időbélyeg válasszal ellenőrzésre kerül.

FDP_DAU_TSP.1.10 megállapítja: A TSF-nek el kell utasítania az időbélyeg választ, ha a válasz olyan kritikus kiterjesztést tartalmaz, amelyet a TSF nem képes feldolgozni. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.TSP** Az olyan időbélyeg válasz, amely fel nem dolgozott kritikus kiterjesztést tartalmaz, visszautasításra kerül.

FDP_DAU_TSP.1.11 megállapítja: A TSF-nek az időbélyeg kérést abban az időpontban kell intéznie, amelyet a felhasználó nevében végrehajtott folyamat beállított. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.TSP** Az időbélyeg kérése a felhasználó nevében végrehajtott folyamat által meghatározott időpontban történik.

FDP_DAU_TSP.1.12 megállapítja: A TSF-nek, amennyiben az aláírás formátuma XAdES v1.3.2 vagy „Egységes MELASZ formátum elektronikus aláírásokra” v2.0, az aláírásban az időbélyeg válaszból (TimeStampResp) kiemelt időbélyeg tokot (TimeStampToken) kell elhelyeznie. A TSF-nek, az ellenőrzés alatt álló aláírásban, amennyiben annak formátuma XAdES v1.3.2-nek vagy „Egységes MELASZ formátum elektronikus aláírásokra”v2.0-nak megfelelő, időbélyeg válasz helyett időbélyeg tokot kell elvárnia. Amennyiben az időbélyeg tok formátuma az RFC 3161-nek megfelelő, a TSF-nek fel kell tételeznie, hogy az időbélyeg tok egy olyan időbélyeg válaszból származik, amelyben a státusz granted. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.TSP** XAdES v1.3.2 aláírás formátum esetén az időbélyegből az időbélyeg tok, a többi aláírás formátum esetén az időbélyeg válasz kerül az aláírásban elhelyezésre. Az ellenőrzés alatt álló aláírásban az időbélyeg elvárt tartalma XAdES v1.3.2 aláírás formátum esetén időbélyeg tok, a többi aláírás formátum esetén időbélyeg válasz. Amennyiben az időbélyeg tok formátuma az RFC 3161-nek megfelelő, feltételezésre kerül, hogy az egy olyan időbélyeg válaszból származik, amelyben a státusz granted.

8.3.1.9 Valós idejű tanúsítvány állapot protokoll (OCSP) kliens csomag biztonsági követelmények kielégítésének indoklása

FDP_DAU_OCS.1.1 megállapítja: A TSF-nek a PKIX RFC 2560-nek megfelelő formában kell összeállítania az OCSP kérést. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.OCSP** Az OCSP kérése az RFC 2560-nak megfelelően történik.

FDP_DAU_OCS.1.2 megállapítja: Az OCSP kérésnek tartalmaznia kell a következő kiterjesztéseket: nonce. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.OCSP** Az OCSP kérés tartalmazza a nonce kiterjesztést.

FDP_DAU_OCS.1.3 megállapítja: A TSF-nek az OCSP választ aláíró tanúsítványt az OCSP válaszból kell megismernie. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.OCSP** Az OCSP válaszadó nyilvános kulcsa a tanúsítvány aláíró CA vagy az OCSP válaszadó tanúsítványból kerül megállapításra.

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

- **SF.OCSP** Az OCSP válaszadó megbízhatósága a Tanúsítási útvonal érvényesítése (CPV) – Alap csomaggal kerül megállapításra.

FDP_DAU_OCS.1.5 megállapítja: A TSF-nek ellenőriznie kell az OCSP válaszon levő aláírást a Tanúsítási útvonal érvényesítése (CPV) – Alap csomag kimenetéből származó nyilvános kulccsal. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.OCSP** Az OCSP válaszon az aláírás az OCSP válaszadó megbízható nyilvános kulcsának, algoritmusának és a nyilvános kulcs paramétereknek a segítségével ellenőrzésre kerül.

FDP_DAU_OCS.1.6 megállapítja: A TSF-nek ellenőriznie kell, hogy ha az OCSP válaszadó tanúsítványa tartalmazza az extendedKeyUsage kiterjesztést, akkor a kiterjesztés tartalmazza-e az id-kp-OCSPSigning OID-t vagy az anyExtendedKeyUsage OID-t.. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.OCSP** Az OCSP válaszadó tanúsítványának extendedKeyUsage kiterjesztése megvizsgálásra kerül, hogy vagy tartalmazza az OCSP aláíró kulcshasználat jelzését vagy az anyExtendedKeyUsage jelzést.

FDP_DAU_OCS.1.7 megállapítja: A TSF-nek össze kell hasonlítania az OCSP válaszból a responderID-t az OCSP válaszadó tanúsítványában található megfelelő információval. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.OCSP** Az OCSP válaszból a responderID összehasonlításra kerül az OCSP válaszadó tanúsítványában található megfelelő információval.

FDP_DAU_OCS.1.8 megállapítja: A TSF-nek az OCSP kérésben található certID-t össze kell hasonlítania az OCSP válasz singleResponse-ban található certID-vel. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.OCSP** Az OCSP kérésből származó certID összehasonlításra kerül az OCSP válasz singleResponse-ból származó certID-vel.

FDP_DAU_OCS.1.9 megállapítja: A TSF-nek aktuálisnak kell elfogadnia az OCSP választ minden bejegyzés tekintetében, ha az alábbi szabályzat érvényesül:
current-time <= producedAt + x, ahol x a felhasználó nevében végrehajtott folyamat által megadott érték. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.OCSP** Az OCSP válasz aktuálisnak kerül elfogadásra az OCSPAfterProducedAtLimit ellenőrzés teljesülésekor.

FDP_DAU_OCS.1.10 megállapítja: A TSF-nek aktuálisnak kell elfogadnia az OCSP választ minden bejegyzés tekintetében, minden esetben, ha az alábbi szabályzat érvényesül:
current-time <= thisUpdate a bejegyzésből + x, ahol x a felhasználó nevében végrehajtott folyamat által megadott érték. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.OCSP** Az OCSP válasz aktuálisnak kerül elfogadásra az OCSPAfterThisUpdateLimit ellenőrzés teljesülésekor.

FDP_DAU_OCS.1.11 megállapítja: A TSF-nek aktuálisnak kell elfogadnia az OCSP választ minden bejegyzés tekintetében, minden esetben, ha az alábbi szabályzat érvényesül:
current-time <= nextUpdate a bejegyzésből + x, ahol x a felhasználó nevében végrehajtott folyamat által megadott érték. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.OCSP** Az OCSP válasz aktuálisnak kerül elfogadásra az OCSPAfterNextUpdateLimit ellenőrzés teljesülésekor.

FDP_DAU_OCS.1.12 megállapítja: A TSF-nek az OCSP választ aktuálisnak kell elfogadni, ha a felhasználó nevében végrehajtott folyamat felülbírálja a frissesség ellenőrzését. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.OCSP** Az OCSP válasz aktuálisnak kerül elfogadásra, ha az AHA folyamat felülbírálja a frissesség ellenőrzését.

FDP_DAU_OCS.1.13 megállapítja: A TSF-nek vissza kell utasítania az OCSP választ, ha az olyan kritikus kiterjesztést tartalmaz, amelyet a TSF nem dolgoz fel. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.OCSP** Az OCSP válasz visszautasításra kerül, ha az fel nem dolgozott kritikus kiterjesztést tartalmaz.

FDP_DAU_OCS.1.14 megállapítja: A TSF-nek a következő kiegészítő ellenőrzéseket kell elvégeznie: nonce a kérésből = nonce a válaszból. Ez a biztonsági követelmény találkozik a következő biztonsági funkcióval:

- **SF.OCSP** Az OCSP válaszból a nonce egyeztetésre kerül az OCSP kérésben szereplő nonce értékével.

8.3.2 A TOE biztonsági funkciói szükségességének indoklása

Az alábbi táblázat bemutatja, hogy a TOE minden biztonsági funkciója szükséges valamely biztonsági funkcionális követelmény teljesítéséhez.

59. táblázat: A TOE biztonsági funkcióinak szükségessége

Biztonsági funkció	Funkcionális követelmény
SF.BASE	FIA_ATD.1.1
	FIA_UAU.1.1
	FIA_UID.1.1
	FMT_SMF.1.1
	FPT_SEP.1.2
SF.INIT	FPT_SEP.1.1
SF.IAA	FDP_ACC.1.1
	FDP_ACF.1.1
	FDP_ACF.1.2
	FDP_ACF.1.3
	FDP_ACF.1.4
	FIA_AFL.1.1
	FIA_AFL.1.2
	FIA_UAU.1.2
	FIA_UAU.7.1
	FIA_UID.1.2
	FMT_MSA.1.1
	FMT_MTD.1.1
	FMT_SMR.2.1
	FMT_SMR.2.2
	FMT_SMR.2.3
	FPT_RVM.1.1
SF.MAN	FMT_MSA.3.1
	FMT_MSA.3.2
SF.CPV	FDP_CPD.1.1
	FDP_CPD.1.2
	FDP_CPD.1.3
	FDP_CPD.1.4
	FDP_DAU_CPV_INI.1.1
	FDP_DAU_CPV_INI.1.2
	FDP_DAU_CPV_INI.1.3
	FDP_DAU_CPV_INI.1.4
	FDP_DAU_CPV_CER.1.1
	FDP_DAU_CPV_CER.1.2
	FDP_DAU_CPV_CER.1.3
	FDP_DAU_CPV_CER.1.4
	FDP_DAU_CPV_CER.1.5
	FDP_DAU_CPV_CER.2.1
	FDP_DAU_CPV_OUT.1.1
	FDP_DAU_CPV_OUT.1.2
	FDP_DAU_CPV_OUT.1.3
	FDP_DAU_CPV_OUT.1.4
SF.SIGSIV	FDP_ETC_SIG.1.1
	FDP_ETC_SIG.1.2

	FDP_ITC_SIG.1.1
	FDP_DAU_SIG.1.1
	FDP_DAU_SIG.1.2
	FDP_DAU_SIG.1.3
SF.ENCDEC	FDP_ETC_ENC.1.1
	FDP_ETC_ENC.1.2
	FDP_DAU_ENC.1.1
	FDP_DAU_ENC.1.2
	FDP_ITC_ENC.1.1
	FDP_ITC_ENC.1.2
SF.CRL	FDP_DAU_CRL.1.1
	FDP_DAU_CRL.1.2
	FDP_DAU_CRL.1.4
	FDP_DAU_CRL.1.3
	FDP_DAU_CRL.1.5
	FDP_DAU_CRL.1.6
	FDP_DAU_CRL.1.7
	FDP_DAU_CRL.1.8
	FDP_DAU_CRL.1.90
	FDP_DAU_CRL.1.10
SF.TSP	FDP_DAU_TSP.1.1
	FDP_DAU_TSP.1.2
	FDP_DAU_TSP.1.3
	FDP_DAU_TSP.1.4
	FDP_DAU_TSP.1.5
	FDP_DAU_TSP.1.6
	FDP_DAU_TSP.1.7
	FDP_DAU_TSP.1.8
	FDP_DAU_TSP.1.9
	FDP_DAU_TSP.1.10
	FDP_DAU_TSP.1.11
	FDP_DAU_TSP.1.12
SF.OCSP	FDP_DAU_OCS.1.1
	FDP_DAU_OCS.1.2
	FDP_DAU_OCS.1.3
	FDP_DAU_OCS.1.4
	FDP_DAU_OCS.1.5
	FDP_DAU_OCS.1.6
	FDP_DAU_OCS.1.7
	FDP_DAU_OCS.1.8
	FDP_DAU_OCS.1.9
	FDP_DAU_OCS.1.10
	FDP_DAU_OCS.1.11
	FDP_DAU_OCS.1.12
	FDP_DAU_OCS.1.13
	FDP_DAU_OCS.1.14

A leképezések magyarázatai korábban meghatározásra kerültek, ezért itt nem kerülnek megismétlésre.

8.4 A követelmények függőségének indoklása

Alap/csomag	#	Követelmények	Függőség
Alap funkcionális követelmények	1	FDP_ACC.1	FDP_ACF.1
	2	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3
	3	FIA_AFL.1	FIA_UAU.1
	4	FIA_ATD.1	Nincs
	5	FIA_UAU.1	FIA_UID.1
	6	FIA_UAU.7	FIA_UID.1
	7	FIA_UID.1	Nincs
	8	FMT_MSA.1	FMT_SMF.1 FMT_SMR.1 FDP_ACC.1
	9	FMT_MSA.3	FMT_SMR.1 FMT_MSA.1
	10	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1
	11	FMT_SMF.1	Nincs
	12	FMT_SMR.2	FIA_UID.1
	13	FPT_RVM.1	Nincs
	14	FPT_SEP.1	Nincs
Informatikai környezet funkcionáli követelményei	1	FCS_CRM_FPS.1	Nincs
	2	FDP_ITC_PKI_INF.1	Nincs
	3	FPT_SMT.1	Nincs
Tanúsítási útvonal érvényesítése (CPV) - Alap	1	FDP_CPD.1	Nincs
	2	FDP_DAU_CPV_INI.1	FCS_COP.1 (Megjegyzés2) FPT_STM.1 (Megjegyzés1)
	3	FDP_DAU_CPV_CER.1	FCS_COP.1(Megjegyzés2) FPT_STM.1 (Megjegyzés1)
	4	FDP_DAU_CPV_CER.2	FDP_DAU_CPV_CER.1
	5	FDP_DAU_CPV_OUT.1	Nincs
PKI aláírás készítés	1	FDP_ETC_SIG.1	FCS_COP.1 (Megjegyzés2)
PKI aláírás ellenőrzés	1	FDP_ITC_SIG.1	Nincs
	2	FDP_DAU_SIG.1	FCS_COP.1 (Megjegyzés2) FDP_DAU_CPV_OUT.1 (Megjegyzés3)
PKI titkosítás kulcs átviteli algoritmusokkal	1	FDP_ETC_ENC.1	FCS_COP.1 (Megjegyzés2) FDP_DAU_CPV_OUT.1 (Megjegyzés3)
	2	FDP_DAU_ENC.1	FDP_DAU_CPV_OUT.1 (Megjegyzés3)
PKI visszafejtés kulcs átviteli algoritmusokkal	1	FDP_ITC_ENC.1	FCS_COP.1 (Megjegyzés2)
Tanúsítvány visszavonási lista érvényesítés	1	FDP_DAU_CRL.1	FCS_COP.1 (Megjegyzés2) FPT_STM.1 (Megjegyzés1)
Időbélyeg kliens	1	FDP_DAU_TSP.1	FCS_COP.1 (Megjegyzés2)
OCSP kliens	1	FDP_DAU_OCS.1	FCS_COP.1 (Megjegyzés2) FPT_STM.1 (Megjegyzés1)

Megjegyzés1: Az FTP_STM.1 függőséget kielégíti az informatikai környezet FPT_STM.1 biztonsági követelménye.

Megjegyzés2: Az FCS_COP.1 függőség nincs hozzáadva a csomaghoz, mivel a kriptográfiai modul, - amiről fel van tételezve, hogy az informatikai környezetnek a része – fogja végezni a kriptográfiai műveleteket.

Megjegyzés3: Az FDP_DAU_CPV_OUT.1 függőség kielégül a Tanúsítási útvonal érvényesítése (CPV) – Alap csomag tartalmazásával.

8.5 PP nyilatkozatok indoklása

A TOE konform az alábbi PKE PP csomagokkal:

Cím: PKE PP (Public Key-Enabled Application Family of Protection Profiles)
with <
Certification Path Validation (CPV) – Basic,
PKI Signature Generation,
PKI Signature Verification,
PKI Encryption using Key Transfer Algorithms,
PKI Decryption using Key Transfer Algorithms,
Certificate Revocation List (CRL) Validation,
Online Certificate Status Protocol Client >
at EAL <3> with augmentation
Verzió: 2.5
Dátum: 2002.10.31

Az alábbi pontosításokkal:

- A PKE PP az 5.3.1 fejezetben lehetőséget nyújt arra, hogy a Tanúsítási útvonal érvényesítése (CPV) –Alap csomag függjön a Tanúsítvány visszavonási lista (CRL) érvényesítés csomagtól. A TOE ezt a csomagfüggést tartalmazza.
- A PKE PP nem különbözteti meg a minősített és fokozott biztonságú elektronikus aláírási fogalmakat, eltérően a magyar (európai) jogi szabályozástól. A PKE PP kriptográfiai modulokra vonatkozó követelménye, és a magyar tanúsított BALE követelménye, egy az egyben nem feleltethetőek meg egymásnak az eltérő minősítési szempontrendszerek miatt, annak ellenére, hogy gyakorlati szempontból szigorúság és cél alapján azonosnak tekinthetőek.

  Ezért jelen ST a CC szerinti finomítás (refinement) műveletett hajtott végre a PKE PP AE.Crypto_Module feltételezésén, és definiálta a AE.Crypto_Module_Normal és AE.Crypto_Module_Rigid feltételezéseket.

  AE.Crypto_Module_Normal feltételezés azt jelenti, hogy a tanúsított FIPS 140-1 sorozat 1. szint helyett csak ennek a követelménynek való megfelelőséget (compliant) tételez fel miden olyan esetben, amikor a magyar jogi szabályozás másról nem rendelkezik

  Az AE.Crypto_Module_Rigid feltételezés azt jelenti, hogy a FIPS 140-1 sorozat 1. szint megfelelőségű (compliant) kriptográfiai szolgáltatató mellett a magyar tanúsított BALE által nyújtott kriptográfiai szolgáltatást is feltételezi.

  Az előzőekből következően az OE.Crypto biztonsági célkitűzés is finomításra került OE.Crypto_Normal és OE.Crypto_Rigid célkitűzésekre.

  OE.Crypto_Normal biztonsági célkitűzés azt jelenti, hogy legalább FIPS 140-1. sorozat 1.szint megfelelő (compliant) kriptográfiai szolgáltatót használatát feltételezi.

- Az OE.Crypto_Rigid biztonsági célkitűzés azt jelenti, hogy a tanúsított BALE kriptográfiai szolgáltatását kell használni minden olyan esetben, amelyet a magyar törvények előírnak, egyéb esetekben pedig a célkitűzésnek megfelelő kriptográfiai szolgáltatót.

- A PKE PP az informatikai környezetre vonatkozó funkcionális követelményként határozza meg a TSF védelmére FPT_STM.1 biztonsági funkciót, amelynek definíciója; Az IT környezetnek a TSF használatához megbízható időbélyeget kell szolgáltatnia.

  Másrészt a CC 2. rész alapján a FPT_STM.1 biztonsági funkció definíciója; A TSF-nek saját használatra gondoskodnia kell megbízható időbélyegről.

  Ugyanakkor a TOE a megbízható időpontott bizalmi harmadik féltől (TSA) szerzi be időbélyeg kérelemhez és ellenőrzéshez. Annak a zavarnak az elkerülésére, hogy az időbélyeg az informatikai környezetből, vagy bizalmi harmadik féltől származik-e, a PKE PP informatikai környezetére vonatkozó FPT_STM.1 követelmény definíciójában következetesen „megbízható időbélyegről”, „megbízható időpontra” lett módosítva a CC 2. rész alkalmazási megjegyzése (J13) alapján, amely lehetőséget biztosít az PP/ST szerzők számára a „megbízható időbélyeg” fogalom tisztázására.

A fenntiekből következően a PKE PP-nek nem része a bizalmi harmadik féltől (TSA) időbélyeg kérelem és ellenőrzés, ezért jelen ST-be bevezetésre került Időbélyeg kliens csomag nem alapul tanúsított védelmi profilon. Az Időbélyeg kliens csomag Időbélyeget kér és ellenőriz az RFC 3161-nek megfelelően. A csomag függőségben áll a PKE PP Tanúsítási útvonal érvényesítése (CPV) – Alap csomagtól annak biztosítására, hogy ellenőrízhető legyen a bizalmi harmadik fél (TSA) hitelessége, az időbélyeget aláíró tanúsítványa alapján.

Az Időbélyeg kliens csomagban a funkcionális követelmények állításai az FDP_DAU.1 alapszintű adathitelesítés követelményeinek finomításával (refinement) lettek meghatározva a PKIX RFC 3161 meghatározottak szerint. Erre lehetőséget ad a CC 1. része.

Fogalmak, rövidítések, hivatkozott dokumentumok

Jelen dokumentumban használt fogalmak, rövidítések és hivatkozott dokumentumok leírását az A2-Polysys_AX_Appendix dokumentum tartalmazza.

Táblázatok jegyzéke

Ábrák jegyzéke