E-Magic
(elektronikus aláírás alkalmazás)
v2.0.0
+
XadesMagic
(elektronikus aláírás alkalmazás fejlesztő készlet minősített elektronikus aláíráshoz)
v2.0.0

BIZTONSÁGI ELŐIRÁNYZAT

Verzió:	2.0
Dátum:	2010 november 1
Fájl:	XM_biztonsagi_eloiranyzat_v20.pdf
Minősítés:	nyilvános
Oldalak:	105

Tartalomjegyzék

Változás kezelés

Verzió	Dátum	Leírás	Készítette
0.1	2010 október 15.	1. fejezet	Törteli Viktor
0.2	2010 október 16.	1. fejezet pontosítása	Törteli Viktor
0.3	2010 október 25.	1.-8. fejezet	Törteli Viktor
0.4	2010 október 28.	pontosítások	Törteli Viktor
0.5	2010 október 30.	Az értékelők észrevételei alapján pontosított változat	Törteli Viktor
2.0	2010 november 1.	Az értékeléshez elfogadott változat	Törteli Viktor

1. Bevezetés

Ez a fejezet dokumentum-kezelő és áttekintő információkat tartalmaz.

Az 1.1 alfejezet (ST hivatkozás) egyértelműen azonosítja a biztonsági előirányzatot.

Az 1.2 alfejezet (TOE hivatkozás) egyértelműen azonosítja az értékelés tárgyát.

Az 1.3 alfejezet (Hivatkozások) különböző referenciákat határoz meg.

Az 1.4 alfejezet (TOE áttekintés) összefoglalja a TOE használatát és fő biztonsági tulajdonságait, valamint azonosítja a TOE típusát és a TOE által megkövetelt valamennyi nem TOE hardvert/szoftvert/förmvert.

Az 1.5 alfejezet (TOE leírás) leírja a TOE általa támogatott funkcionalitást, bemutatja az értékelés tárgyát egy aláírás létrehozó rendszeren, illetve egy aláírás ellenőrző modulon belül, valamint meghatározza a TOE fizikai és logikai hatókörét.

1.1 ST hivatkozás

Cím:	E-Magic (elektronikus aláírás alkalmazás) v2.0.0 + XadesMagic (elektronikus aláírás alkalmazás fejlesztő készlet minősített elektronikus aláíráshoz) v2.0.0 - Biztonsági előirányzat
Verzió szám:	2.0
Dátum:	2010. november 1.
Szerző:	SDA stúdió Kft.

1.2 TOE hivatkozás

Az értékelés tárgya (TOE):	E-Magic (elektronikus aláírás alkalmazás) v2.0.0 + XadesMagic (elektronikus aláírás alkalmazás fejlesztő készlet minősített elektronikus aláíráshoz) v2.0.0
A TOE rövid neve:	E-Magic + XadesMagic (esetenként E-Magic vagy XadesMagic)
Verzió szám:	2.0.0 (E-Magic), 2.0.0 (XadesMagic)
Dátum:	2010. november 1.
Szponzor szervezet:	SDA stúdió Kft.
Garanciaszint:	MIBÉTS fokozott (CC EAL3)
Kulcsszavak:	Nyilvános kulcsú infrastruktúra (PKI), elektronikus aláírás

1.3 Hivatkozások

[ALGO] ETSI TS 102 176-1: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms, V2.0.0, July 2007.

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Revision 1, September 2006.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Revision 2, September 2007.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, Revision 2, September 2007.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, Revision 2, September 2007.

[CWA 14169] Secure signature-creation devices "EAL 4+", CEN/WS, March 2004.

[CWA 14170] Security requirements for signature creation applications, CEN/WS, May 2004.

[CWA 14171] General guidelines for electronic signature verification, CEN/WS, May 2004

[FIPS 180-3] FIPS PUB 180-3: Secure Hash Standard, October 2008

[MMM-001] Egységes MELASZ formátum elektronikus aláírásokra v2.0 (MMM-001: 2008, v2.0)

[PKCS#1] RSA Cryptography Standard v2.1, June 2002

[PP-ESCA] Protection Profile - Electronic Signature Creation Application (DCSSI-PP-2008/05)

[PP-ESVM] Protection Profile - Electronic Signature Verification Module (DCSSI-PP-2008/06)

[RFC 2560] RFC 2560 - X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 1999

[RFC 3161] RFC 3161 - X.509 Internet Public Key Infrastructure - Time-Stamp Protocol (TSP), August 2001

[RFC 5280] RFC 5280 - Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, May 2008

1.4 TOE áttekintés

Jelen biztonsági előirányzat egy olyan Windows alkalmazás (E-Magic), illetve az ennek alapját képező szoftver fejlesztőkészlet (XadesMagic) biztonsági szolgáltatásait és az ezekre vonatkozó követelményeket írja le, melyek felhasználásával szabványos formátumú elektronikus aláírások készíthetők, illetve ellenőrizhetők biztonságos módon.

1.4.1 A TOE alap funkcionalitása

Az E-Magic + XadesMagic által támogatott két alap funkcionalitás az alábbi:

- elektronikus aláírások létrehozása,
- elektronikus aláírások ellenőrzése.

Támogatják mind a fokozott biztonságú, mind a minősített elektronikus aláírásokat.

1.4.2 A TOE szabványoknak való megfelelése

Az E-Magic + XadesMagic az alábbi szabványoknak, illetve ajánlásoknak megfelelő működést biztosít:

- [RFC 2560] (OCSP kérés előállítás, valamint OCSP és OCSP válasz ellenőrzés)
- [RFC 3161] (Időbélyeg kérés, valamint az időbélyeg és időbélyeg válasz ellenőrzés)
- [RFC 5280] (Tanúsítványok és CRL-ek ellenőrzése, tanúsítási útvonal felépítése és érvényesítése. A tanúsítványlánc felépítésénél az alábbi kiterjesztéseket támogatja:
  - ExtendedKeyUsage
  - KeyUsage
  - BasicConstraints
  - CRLDistributionPoints
  - SubjectAlternativeName
  - IssuerAlternativeName
- [MMM-001] (elektronikus aláírás formátumok létrehozása és ellenőrzése, az alábbi szabványos formátumokkal:
  - XAdES-EPES,
  - XAdES-T,
  - XAdES-C,
  - XAdES-X,
  - XAdES-X-L,
  - XAdES-A.)

1.4.3 A TOE típusa

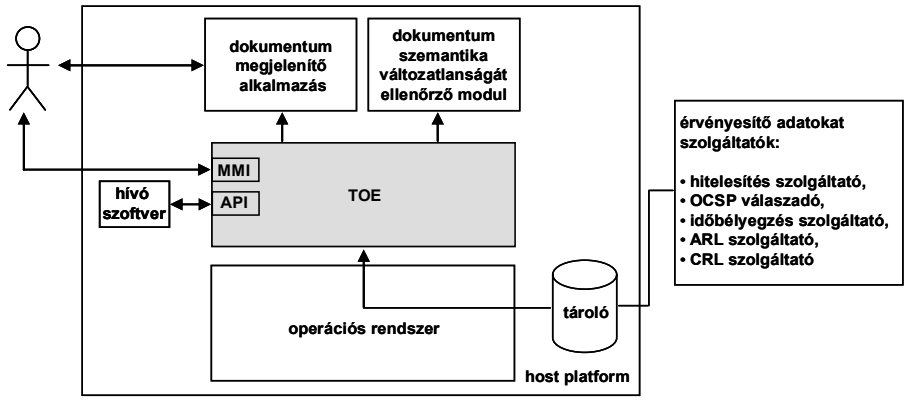
Az E-Magic + XadesMagic egy olyan speciális elektronikus aláírás termék, melynek fő funkciója elektronikus aláírások létrehozása és ellenőrzése.

1.4.4 A TOE által megkövetelt hardver, szoftver és förmver elemek

Az (E-Magic + XadesMagic)-t egy hosztgép platformján integrálják.
Az E-Magic + XadesMagic informatikai környezete az alábbi elemekből áll:

- a hosztgép platform operációs rendszere
- az a szoftver, mely lehetővé teszi az aláírandó/aláírt dokumentum megtekintését, és amely figyelmezteti az aláírót/ellenőrzőt, ha ennek jellegzetességei nem teljesen megfelelők a dokumentum által megkívánt megjelenítés jellegzetességeinek (színek használata, a szükséges betűkészletek megléte, ...),
- (csak aláírás létrehozásnál): minősített elektronikus aláírás esetén SSCD, fokozott biztonságú elektronikus aláírás esetén SCDev (pl. intelligens kártya, USB token),
- (csak aláírás létrehozásnál): az operációs rendszeren telepített azon szoftver komponensek, melyek az SSCD/SCDev-vel való kommunikációt teszik lehetővé (pl. PKCS#11 driver-ek vagy egy kriptográfiai interfészt meghatározó CSP, melyeket az aláíró alkalmazás hív meg, hogy elérje az aláírást előállító modult),
- (csak aláírás ellenőrzésnél): azok a szoftver vagy hardver komponensek, melyek biztosítják az érvényesítő adatokat.

A fenti elemeket az 1. ábra szemlélteti.



1. ábra: A TOE működtetési környezetében

1.5 TOE leírás

Az E-Magic + XadesMagic által támogatott két alap funkcionalitás az alábbi:

- elektronikus aláírások létrehozása,
- elektronikus aláírások ellenőrzése.

Az alábbiak az (E-Magic + XadesMagic)-t elhelyezik egy általános aláírás létrehozó rendszeren, illetve egy általános aláírás ellenőrző modulon belül.

1.5.1 Az E-Magic + XadesMagic, mint egy aláírás létrehozó rendszer

Egy elektronikus aláírás létrehozó rendszer szoftver és/vagy hardver összetevők egy készlete, amely elektronikus aláírásokat hoz létre egy aláírás-létrehozó eszköz (SCDev) segítségével, mely utóbbi az aláíró magánkulcsát használva végrehajtja a kriptográfiai műveleteket.

Egy elektronikus aláírás létrehozó rendszer (összhangban a [CWA 14170]-ben bevezetett modell elnevezéseivel) a következő funkcionális összetevőkből áll:

- az aláíróval kölcsönható összetevő,
- az aláírói dokumentumot megjelenítő összetevő,
- a dokumentumok szemantikai stabilitását ellenőrző összetevő,
- az aláírási tulajdonságokat megjelenítő összetevő,
- az aláírási szabályzatot kezelő/megvalósító összetevő,
- az aláírandó adatot formattáló és lenyomatoló összetevő,
- az aláírás-létrehozó eszköz interfészét irányító összetevő.

1.5.1.1 Az aláíróval kölcsönható összetevő

Az aláíróval kölcsönható összetevő interfészt biztosít az aláírónak, lehetővé téve számára egy vagy több dokumentum aláírását. Ez az interfész vagy egy ember-gép interfész (man-machine interface, MMI), amely közvetlen kölcsönhatásba lépési lehetőséget biztosít az aláírás létrehozó rendszerrel vagy egy programozói interfész (API), mely egy szoftver komponensnek teszi lehetővé ezt a kölcsönhatást.
Minimálisan támogatni kell az aláíró dokumentum kiválasztásának lehetőségét, az aláíráshoz felhasznált tanúsítvány megadásának lehetőségét, az aláírás kiváltására vonatkozó egyértelmű akarat kinyilvánításának lehetőségét és az SCDev számára szükséges hitelesítő adat megadásának lehetőségét.

Az aláírónak lehetőséget kell biztosítani az általa elfogadott elemek áttekintésére, még mielőtt aláírná ezeket ("Azt írod alá, amit látsz" elv.). Ehhez az alábbiakra van szükség:

- Lehetővé kell tenni az aláíró számára, hogy megtekintse az aláírói dokumentumot.
- A papír dokumentumoktól eltérően az elektronikus dokumentumok szemantikája

bizonyos esetekben megváltozhat, a megjelenítő környezettől függő módon. Ezért szükség van az aláírói dokumentum szemantikus stabilitásának (vagyis megváltoztathatatlanságának) ellenőrzésére.
- Lehetővé kell tenni az aláíró számára, hogy megtekintse a dokumentumhoz kapcsolódó aláírandó aláírási tulajdonságokat.

Az E-Magic esetén az aláíróval kölcsönható összetevő egy MMI.
Ez az ember – gép interfész lehetővé teszi az aláró számára az alábbiakat:
- dokumentum kiválasztás,
- az alkalmazandó aláírási szabályzat kiválasztása,
- az alkalmazandó aláírási tulajdonságok kiválasztása,
- az aláíráshoz alkalmazandó tanúsítvány (s ezen keresztül a magánkulcs) kiválasztása
- az aláírással egyetértés kifejezésre juttatása,
- az aláíró magánkulcsának aktivizálása,
- az aláírás létrehozás folyamatának leállítása.

Az aláíró hitelesítési adatainak megadását és SCDev-hez továbbítását megvalósító összetevő a TOE hatókörén kívül esik.

A ***dokumentum kiválasztás*** területén az E-Magic az alábbiakat támogatja:
- **Korábbi ellenjegyzett aláírások** (Az aláírandó dokumentum már tartalmazhat aláírásokat. A későbbiekben a "dokumentum" vagy egy egyszerű dokumentumot jelöl, vagy egy olyan dokumentumot, mely már tartalmaz egy vagy több aláírást. A második eset annak felel meg, hogy az aláíró ellenjegyzett aláírást hoz létre.)
- **Egy vagy több dokumentum aláírása** (Amennyiben az aláírás több dokumentumra vonatkozik, mindegyikre ugyanazok az aláírási tulajdonságok lesznek alkalmazva, vagyis ugyanaz az aláíró tanúsítvány (s ezen keresztül a magánkulcs) azonosító, ugyanaz a szerepkör, ugyanaz az aláírási hely, stb... Ebben az esetben az aláíró nyilvánvaló aláírás kiváltási cselekvése az összes kiválasztott dokumentumra vonatkozik.
- **Dokumentumok kiválasztásból való visszavétele** (Miután egy kiválasztott dokumentumot az aláíró megnéz, visszautasíthatja annak aláírását. Az E-Magic lehetővé teszi számára, hogy egy aláírásra kijelölt dokumentumot kivegyen az aláírásra kijelölt halmazból.

Az alkalmazandó aláírási szabályzat kiválasztása területén az E-Magic az alábbiakat támogatja:
- a TOE a végrehajtható kódban tárolt több aláírási szabályzat használatát támogatja (rögzített szabályzatok),
- az alkalmazandó aláírási szabályzat változtatható részeit az aláíró állíthatja be.

Az alkalmazandó aláírási tulajdonságok kiválasztása területén az E-Magic lehetővé teszi, hogy az aláíró kiválassza a dokumentumhoz kapcsolódó alábbi aláírási tulajdonságokat:
- az aláírás helyére vonatkozó állítás (város, megye, irányítószám, ország),
- az aláíró szerepköre (role).

Az aláíráshoz alkalmazandó tanúsítvány kiválasztása területén az E-Magic az alábbiakat támogatja:
- Az E-Magic lehetővé teszi, hogy az aláíró kijelölje, hogy melyik tanúsítványt (s ezen keresztül melyik magánkulcsot) használja az aláírás létrehozásához.

Az aláírással egyetértés kifejezésre juttatása szempontjából az E-Magic az alábbiakat támogatja:

- Az E-Magic ember – gép interfésze lehetővé teszi, hogy az aláíró kifejezze egyetértését az aláírásra, s ezt minden aláírandó dokumentumra megteheti.
- Mielőtt egy vagy több dokumentumra létrejön az aláírás, az E-Magic ellenőrzi, hogy az aláíró valóban akarja-e ezt az aláírást, cselekvése nem szándéktalan vagy nem véletlen-e. Ennek érdekében az E-Magic-nek egy második, nem nyilvánvaló cselekvésre kell késztetnie az aláírót.
- Az aláírással egyetértés fenti művelete különbözik az aláíró SCDev felé történő hitelesítésétől.

Az ***aláíró magánkulcsának aktivizálása*** szempontjából az E-Magic az alábbiakat támogatja:

- Az aláíró kiválasztott tanúsítványához tartozó magánkulcs aktivizálásának előzetes feltétele az aláírással egyetértés kifejezésre juttatása.

Az ***aláírás létrehozás folyamatának leállítása*** szempontjából az E-Magic az alábbiakat támogatja:

- Az E-Magic lehetővé teszi az aláíró számára, hogy leállítsa egy vagy több dokumentum aláírásának folyamatát bármikor, amíg az E-Magic az aláírandó adatot még nem küldte át az SCDev-nek.

1.5.1.2 Az aláírói dokumentumot megjelenítő összetevő

Az aláírói dokumentumot megjelenítő összetevő lehetővé teszi az aláíró számára az elektronikus dokumentum tartalmának megtekintését, még az elektronikus aláírás létrehozása előtt.

Az E-Magic esetén az aláíró még aláírás előtt megtekintheti az aláírni kívánt dokumentumot: *az „Aláírandó állományok listája”* részben felsorolt állományok között felsorolt dokumentumok közül a kiválasztott sorra kattintással. Ennek hatására az E-Magic végrehajt egy a megnézni kívánt dokumentum formátumának megfelelő megjelenítő alkalmazást.
Ennek érdekében az E-Magic összerendeli egymással a támogatott dokumentum formátumokat és a megjelenítő alkalmazásokat. Ha az aláíró olyan állományt választ ki, aminek kiterjesztése nem szerepel a „kiterjesztés – megjelenítő alkalmazás” összerendelés listában, akkor nem hajtható végre az aláírás. Ha a .txt-n és a .xml-en kívül olyan állományt szeretne aláírni, amelyet előzetesen felvett, akkor saját felelősségre megtörténhet az aláírás, de üzenetben az alkalmazás figyelmeztet, hogy a kiválasztott file kiterjesztése nem támogatott.
Az E-Magic által végrehajtott megjelenítő alkalmazások listáját az aláíró határozza meg.
Az E-Magic alap értelmezetten két kiterjesztést támogat: *.txt* és *.xml*. Ez a lista módosítható (kiegészthető vagy szűkíthető).
A megjelenítő alkalmazások az E-Magic hatókörén kívül állnak.

1.5.1.3 A dokumentumok szemantikai stabilitását ellenőrző összetevő

Az aláírói dokumentum olyan változó mezőket vagy aktív kódokat tartalmazhat, melyek külső paraméterektől függnek, s melyek így a dokumentum megtekintési környezetétől függően eltérők lehetnek.
Bizonyos esetekben így az aláíró egy olyan elektronikus dokumentumot írhat alá, melynek tartalma függ a megtekintés környezetétől.
Ez az aláírást fogadó ellenőrzőt is megtévesztheti. Egy olyan dokumentumot láthat, mely szemantikailag különbözik attól, amit az aláíró látott.
Ezért az aláírandó dokumentum tartalmát ellenőrizni kell annak igazolása érdekében, hogy szemantikája nem függ külső paraméterektől. Ezt az ellenőrzést az általános modellben a dokumentumok szemantikai stabilitását ellenőrző összetevő végzi el.

Az E-Magic az aláírandó dokumentumok szemantikai stabilitásának ellenőrzését végző összetevőt nem tartalmaz. A funkcionalitást azonban támogatja, az alábbi módon:

- Alap értelmezésben az E-Magic csak két stabil kiterjesztést (.txt, .xml) támogat.
- Minden más kiterjesztést automatikusan „nem megváltoztathatatlan” (tehát nem stabil) kategóriába sorol. Ha az aláíró a .txt-n és a .xml-en kívül olyan állományt szeretne aláírni, amelynek kiterjesztését korábban már felvette a támogatottak körébe, akkor az alkalmazás üzenetben figyelmezteti, hogy a kiválasztott file kiterjesztése nem támogatott (nem stabil), s ezután az aláíró eldöntheti, hogy a figyelmeztetés ellenére, saját felelősségére aláír-e.

1.5.1.4 Az aláírási tulajdonságokat megjelenítő összetevő

Az aláírási tulajdonságokat megjelenítő összetevő lehetővé teszi az aláíró számára a kiválasztott aláírási tulajdonságok megtekintését, még az aláírás létrehozása előtt.

Az E-Magic lehetővé teszi az aláíró számára az alábbi kiválasztott aláírási tulajdonságok megtekintését, még az aláírás létrehozása előtt:

- Aláírás típusa
- Aláírás helye
- Aláíró szerepköre
- tartalom-formátum

1.5.1.5 Az aláírási szabályzatot kezelő/megvalósító összetevő

Az aláírási szabályzat az elektronikus aláírások létrehozására és ellenőrzésére vonatkozó szabályok gyűjteménye. Az aláírási szabályzatot kezelő/megvalósító összetevő az aláírás létrehozásakor az aláírási szabályzatnak csak azt a részét alkalmazza, melyek az aláírások elfogadásához szükségesek.
Ezen követelmények egy része az aláíró tanúsítványára vonatkozik:

- az aláíró számára elfogadható tanúsítvány szabályok azonosítóinak listája;
- a magánkulcs használatával kapcsolatos információk (key usage);
- a tanúsítványra elvárt kiterjesztések (QCstatements).

Más attribútumokra vonatkozó követelmények is vannak, például:

- az aláírási szabályzat által engedélyezett kötelezettségvállalás típusok.

A TOE-nak támogatnia kell az alábbi alternatívák egyikét:

- a végrehajtható kódban tárolt egy vagy több aláírási szabályzat használata (rögzített szabályzatok),
- az aláírási szabályzatokat a TOE számára értelmezhető fájlok formájában használja (konfigurálható szabályzatok).

Az E-Magic lehetővé teszi az aláíró számára az alkalmazandó aláírási szabályzat alábbi részeinek beállítását (*a Konfiguráció menü Beállítások felületén keresztül*):

- Aláírás helye (város, megye, ország, irányítószám)
- Szerepkör
- Xades típus (Xades-EPES vagy Xades–T)
- Aláíró algoritmus (RSA-SHA1 vagy RSA-SHA256)
- Lenyomatképző algoritmus (SHA1 vagy SHA256)
- Aláírás fajtája *(*Fokozott vagy Minősített)
- A kivárási idő figyelembe vételének kikapcsolása
- Időbélyeg szolgáltató kiválasztása
- Aláírás előtti időbélyeg használatának beállítása
- CRL és OCSP használata közötti választás (CRL(nincs OCSP) vagy Explicit OCSP szolgáltató vagy Tanúsítványban szereplő OCSP szolgáltató)
- Megtekinthető és aláírható típusok (dokumentum formátum/megjelenítő alkalmazás lista)

Az E-Magic lehetővé teszi az aláíró számára az alkalmazandó aláírási szabályzat alábbi pontosítását is (*a Parancsok menü - Fájl aláíró felület - Aláíró tanúsítvány kiválasztása felületén keresztül*):

- Aláírás típusa (Elektronikus adat aláírása / Közjegyzői (ellenjegyző) aláírás)
- Szerepkör
- Aláírás helye (város, megye, ország, irányítószám)
- Aláírás előtti időbélyegzés hozzáadása (igen/nem)

1.5.1.6 Az aláírandó adatot formattáló és lenyomatoló összetevő

Az aláírandó adatot formattáló és lenyomatoló összetevő formattálja az aláírói dokumentumot és az aláírási tulajdonságokat, majd lenyomatolással (hash képzéssel) elkészíti a "Data To Be Signed Representation (DTBSR)"–nak nevezett információt, mely az SCDev-nek lesz továbbítva az aláírás végrehajtásához.

Az E-Magic az alábbi lenyomatoló algoritmusokat (hash függvényeket) támogatja:

- SHA-1,
- SHA-256

1.5.1.7 Az aláírás-létrehozó eszköz interfészét irányító összetevő

Az aláírás-létrehozó eszköz interfészét irányító összetevő az SCDev-vel való kölcsönhatásra szoftver és/vagy middleware komponenseket használ.
Ez az összetevő az alábbi funkciókat biztosítja:

- megszerzi az SCDev-től az aláíró által használható tanúsítványokat, vagy ezek hivatkozásait;
- kijelöli az SCDev számára az aktivizálandó aláíró kulcsot;
- átküldi az SCDev számára a DTBSR-t;
- minden aláírt dokumentumra fogadja az SCDev-től az elektronikus aláírást, egyúttal átveszi az aláírás létrehozási folyamat sikerességére vagy sikertelenségére vonatkozó állapotot;

Az E-Magic az SCDev-vel való kölcsönhatásra az alábbi szoftver és middleware komponenseket használja:
Fokozott biztonságú elektronikus aláírás esetén:

- eToken Pro 64K v4.2 (middleware: Aladdin eToken PKI Client v5.0.0.65)

Minősített elektronikus aláírás esetén:

- SmartSign CSP for StarCert v1.0.9.15 (Giesecke StarCert v2.2 SSCD esetén)
- Classic Client Toolbox (Gemalto TPC IM CC v3 SSCD esetén)

A fenti middleware-ek a TOE hatókörén kívül áll.

1.5.1.8 A XadesMagic támogatása az aláírás létrehozására

A XadesMagic felhasználója egy program lehet, mely számára API interfészt biztosít.

A XadesMagic függvényei az E-Magic (és más aláírás létrehozó rendszer) alábbi funkcionális összetevőit támogatják:

- az aláírási szabályzatot kezelő/megvalósító összetevő,
- az aláírandó adatot formattáló és lenyomatoló összetevő,
- az aláírás-létrehozó eszköz interfészét irányító összetevő.

1.5.2 Az E-Magic + XadesMagic, mintegy aláírás ellenőrző modul

Egy elektronikus aláírás ellenőrző modul szoftver és/vagy hardver összetevők egy készlete, amely elektronikus aláírások ellenőrzésére alkalmazható.

Az aláírás ellenőrző modult egyaránt meghívhatja egy személy, vagy egy automata rendszer (meghívó alkalmazás).

Az **aláírási szabályzat** az elektronikus aláírások létrehozására és ellenőrzésére vonatkozó szabályok gyűjteménye, melyek segítségével megállapítható az elektronikus aláírások érvényessége. Tartalmazza azokat a szabályokat, melyek meghatározzák az aláíró által biztosítandó aláírási tulajdonságokat, valamint a harmadik felekkel (CA, OCSP szerver, TS szerver,...) kapcsolatos szabályokat. Egy aláírási szabályzat a következő elemeket tartalmazza:

- egy vagy több megbízható pont (trusted point) azonosítása, valamint az aláíró tanúsítványától az egyik ilyen megbízható pontig vezető tanúsítványlánc felépítésére vonatkozó szabályok;
- időhivatkozás módja, melynek segítségével az aláíró aláírásának időpontja behatárolható (pl. időbélyegzés);
- a visszavonási állapot ellenőrzésének módja a tanúsítvány lánc minden tanúsítvány elemére, az időhivatkozást és kivárási időt is figyelembe véve;
- az aláíró tanúsítványában előforduló lehetséges tulajdonságok (attribútumok) (pl. hitelesítési rend azonosító, QCStatements, key usage, stb);
- azon attribútumok, amelyeket az aláíró tanúsítványának hivatkozásán túl alá kell írni a dokumentumhoz csatoltan (pl. aláírási szabályzat hivatkozás, kötelezettségvállalás típus, az aláírás feltételezett dátuma, a dokumentum formátuma, az aláíró feltételezett szerepköre, az aláírás feltételezett helyszíne, stb.);
- az aláíró által biztosítandó érvényesítő adatok köre;
- időhivatkozás módja, melynek segítségével az érvényesítő adatok időpontja behatárolható (pl. időbélyegzés vagy gépóra);
- azon kriptográfiai algoritmusok (aláíró és hash), melyek a dokumentum és érvényesítő adatok digitális aláírásának ellenőrzéséhez használhatók.

Egy aláírás ellenőrző modul működésében két **működési mód** (használati eset) különböztethető meg:

- kezdeti ellenőrzés,
- utólagos ellenőrzés.

A **kezdeti ellenőrzés** az elektronikus aláírás első ellenőrzése, melyet az elektronikus aláírás fogadását követően minél hamarabb végre kell hajtania az ellenőrzőnek.
Az aláírás ellenőrző modult arra használják, hogy az ellenőrző által kiválasztott aláírási szabályzatnak megfelelően ellenőrizzék az elektronikus aláírás érvényességét. Az ehhez szükséges érvényesítő adatok vagy megtalálhatók az elektronikus aláírásban, vagy más módon gyűjtendők össze. Ezen érvényesítő adatok tartalmaznak egy időhivatkozást is, mely igazolja a digitális aláírás létezését egy meghatározott időpontban. A többi érvényesítő adat érvényessége ehhez az időponthoz képest ellenőrizhető.

Az **utólagos ellenőrzés** az elektronikus aláírás olyan ellenőrzése, melyre a kezdeti ellenőrzés során összegyűjtött érvényesítő adatok alapján, az ellenőrző által kiválasztott aláírási szabályzat szerint kerül sor. Ez az ellenőrzés mindaddig végrehajtható, ameddig a digitális aláírást időben elhelyező időhivatkozás (pl. időbélyeg token) még érvényes.

Egy általános aláírás ellenőrző modul az alábbi **funkcionális összetevők**et tartalmazza:

- a felhasználóval kölcsönható összetevő,
- az alkalmazandó aláírási szabályzatot kiválasztó összetevő,
- a dokumentumok szemantikai stabilitását ellenőrző összetevő,
- a dokumentum megjelenítő alkalmazásokat végrehajtó összetevő,
- az érvényesítő adatokat összegyűjtő és feldolgozó összetevő,
- a digitális aláírásokat ellenőrző összetevő,
- az aláírási szabályzatokat adminisztráló összetevő.

1.5.2.1 A felhasználóval kölcsönható összetevő

A felhasználóval kölcsönható összetevő két típusú felhasználót különböztethet meg, az ellenőrzőt és az aláírás ellenőrző modul biztonsági adminisztrátorát. (Ez a biztonsági adminisztrátor szerepkör különbözik a gazdagép platform adminisztrátorától.)
Az aláírás ellenőrző modul interfészt biztosít a felhasználóknak, mely a felhasználó típusától függően lehet ember-gép interfész (MMI), programozói interfész (API), vagy a kettő kombinációja.

Az E-Magic (mint aláírás ellenőrző modul) felhasználója egy személy lehet (nem automata).
Ez a személy az ellenőrző (nincs ellenőrző és adminisztrátor megkülönböztetés).
Az E-Magic MMI interfészt biztosít az ellenőrző számára, az alábbi kölcsönhatásokat lehetővé téve:

- az ellenőrizendő dokumentum kiválasztása,
- az alkalmazandó aláírási szabályzat kiválasztása,
- az aláírási tulajdonságok bemutatása,
- az ellenőrzés állapot kijelzése az ellenőrzési folyamat végén,
- az érvényesítő adatok átadása.

Az E-Magic ***az ellenőrizendő dokumentum kiválasztása*** során lehetőséget biztosít az ellenőrző számára, hogy:

- ellenőrizze a kiválasztott dokumentum elektronikus aláírásának érvényességét a beállított aláírási szabályzatnak megfelelően (*Parancsok menü – Ellenőrző felület - Egy állomány megnyitása ellenőrzésre gomb*)
- ellenőrizze a kiválasztott dokumentum elektronikus aláírásának érvényességét, részben a beállított alárási szabályzatnak megfelelően, részben a kijelölt Xades típus váltás figyelembe vételével (*Parancsok menü – Ellenőrző felület - Xades típusváltás gomb*)

Az E-Magic az ***alkalmazandó aláírási szabályzat kiválasztása*** során lehetőséget biztosít az ellenőrző számára, hogy az alkalmazott aláírási szabályzat különböző szabályait beállítsa, alkalmazását pontosítsa (lásd 1.2.5.7: Az aláírási szabályzatokat adminisztráló összetevő).

Az E-Magic az ***aláírási tulajdonságok bemutatása*** során lehetőséget biztosít az ellenőrző számára az elektronikus aláírásban lévő alábbi aláírási tulajdonságok megtekintésére:

- Aláírás ideje
- Szerepkör
- Aláírás helye
- Tartalom-formátum

Az E-Magic az ***ellenőrzés állapot kijelzése*** tekintetében az ellenőrzési folyamat végén jelzi az ellenőrzés állapotát *(Parancsok menü – Ellenőrző felület - Egy állomány megnyitása ellenőrzésre gomb megnyomására: a folyamat sikeresen befejeződött, illetve az aláírás státuszának megjelenítése az aláírók ablakban: érvényes/érvénytelen/még nem eldönthető)*

Az E-Magic az ***érvényesítő adatok átadása*** tekintetében lehetőséget biztosít az ellenőrző számára, hogy az megkapja az elektronikus aláírás ellenőrzése során használt érvényesítő adatokat, az aláírásba foglalva ezeket.

1.5.2.2 Az alkalmazandó aláírási szabályzatot kiválasztó összetevő

Az alkalmazandó aláírási szabályzatot kiválasztó összetevő a következő módon határozza meg az alkalmazandó aláírási szabályzatot, s ezen keresztül a modul által megvalósított ellenőrzést:

- Amennyiben az ellenőrző közvetlenül kiválasztott egy aláírási szabályzatot, akkor ez lesz alkalmazva még akkor is, ha az elektronikus aláírásban szerepel is egy aláírási szabályzatra történő hivatkozás. Az aláírás ellenőrző modul tájékoztatja az ellenőrzőt, ha az alkalmazott és az elektronikus aláírásban meghivatkozott aláírási szabályzat eltér egymástól.
- Amennyiben az aláírási szabályzatot az aláírás ellenőrző modult hívó alkalmazás nem határozza meg, akkor az elektronikus aláírásban meghivatkozott aláírási szabályzat lesz alkalmazva, amennyiben van ilyen hivatkozás. Ebben az esetben a hivatkozott aláírási szabályzat visszaadódik a hívó alkalmazásnak annak érdekében, hogy az szükség esetén ellenőrizhesse a szabályzat megfelelőségét.
- Amennyiben nincs sem előre kiválasztott, sem az elektronikus aláírásban hivatkozott aláírási szabályzat, akkor ez vagy hibát okoz, vagy egy alapértelmezett aláírási szabályzat kerül alkalmazásra, mely utóbbi esetben ez az alapértelmezett aláírási szabályzat visszaadódik a hívó alkalmazásnak annak érdekében, hogy az szükség esetén ellenőrizhesse a szabályzat megfelelőségét.

Az E-Magic alap értelmezésben az aktuálisan beállított aláírási szabályzat szerint ellenőrzi a kiválasztott elektonikus alárás érvényességét.
Mindig van aktuálisan beállított aláírási szabályzat, mert a Beállítás menüben a különböző lehetőségek közül mindig pontosan egyet lehet (és kell is) beállítani.

1.5.2.3 A dokumentumok szemantikai stabilitását ellenőrző összetevő

A dokumentumok szemantikai stabilitását ellenőrző összetevő azért szükséges, mert az aláírói dokumentum olyan változó mezőket vagy aktív kódokat tartalmazhat, melyek külső paraméterektől függnek, s melyek így a dokumentum megtekintési környezetétől függően eltérők lehetnek. Bizonyos esetekben így az aláíró egy olyan elektronikus dokumentumot írhat alá, melynek tartalma függ a megtekintés környezetétől. Ez az aláírást fogadó ellenőrzőt is megtéveszthetti, hiszen egy olyan dokumentumot láthat, mely szemantikailag különbözik attól, amit az aláíró látott. Ezért az aláírandó dokumentum tartalmát ellenőrizni kell annak igazolása érdekében, hogy szemantikája nem függ külső paraméterektől.

Az E-Magic esetén nincs ilyen összetevő. A támogatott kiterjesztéseket stabilnak tekinti, minden más kiterjesztés automatikusan nem támogatott (nem stabil) figyelmeztetést eredményez.

1.5.2.4 A dokumentum megjelenítő alkalmazásokat végrehajtó összetevő

A dokumentum megjelenítő alkalmazásokat végrehajtó összetevő akkor szükséges, ha az ellenőrzést egy személy végzi, vagy az automata ellenőrző rendszert egy üzemeltető felügyeli. Az ilyen esetekben az ellenőrzés során a dokumentum tartalmi kiértékelése érdekében az ellenőrző/üzemeltető kérésére az aláírás ellenőrző modulnak végre kell hajtania egy a dokumentum formátumának megfelelő megjelenítő alkalmazást.

Az E-Magic esetében az ellenőrzést egy személy végzi, ezért szükség van a dokumentum megjelenítő alkalmazásokat végrehajtó összetevőre.

Az ellenőrző kérésére az E-Magic végrehajtja az ellenőrizendő dokumentum formátumának megfelelő megjelenítő alkalmazást, amennyiben a kiterjesztés szerepel a támogatott kiterjesztések között. Ellenkező esetben az ellenőrző figyelmeztetést kap.
A megjelenítő alkalmazások a TOE hatókörén kívül állnak.

1.5.2.5 Az érvényesítő adatokat összegyűjtő és feldolgozó összetevő

Az érvényesítő adatokat összegyűjtő és feldolgozó összetevő az alkalmazott aláírási szabályzatnak megfelelő módon a következő funkciókat biztosítja:

- az aláírási tulajdonságok megfelelőségének ellenőrzése,
- a digitális aláírás elhelyezése az időben,
- a digitális aláíráshoz használt algoritmus és kulcshossz megfelelőségének megállapítása
- az aláíró tanúsítványának megfelelőség ellenőrzése,
- egy érvényes tanúsítványlánc felépítése,
- a tanúsítványlánc érvényességének ellenőrzése.

Ezek a funkciók iteratív módon valósulnak meg, egészen addig, amíg egy érvényes tanúsítványlánc építhető fel.

Az E-Magic a következő módon gyűjti össze az érvényesítő adatokat:

- letölti a tanúsítványban szereplő helyről a CRL-t,
- letölti a tanúsítványban szereplő helyről az OCSP-t.

Az érvényességi adatok összegyűjtésénél az E-Magic hálózati protokollt (http) használ.
Az E-Magic az érvényesítő adatok feldolgozása során a következő funkciókat biztosítja:

- a digitális aláírás elhelyezése az időben,
- az aláíró tanúsítványának megfelelőség ellenőrzése,
- érvényes tanúsítványlánc felépítése,
- tanúsítványlánc érvényességének ellenőrzése.

A ***digitális aláírás elhelyezése az időben*** funkció azért szükséges, hogy az aláíró tanúsítványának és más érvényesítő adatoknak az érvényessége, s ezen keresztül az elektronikus aláírás érvényessége ellenőrizhető legyen.
A "digitális aláírás elhelyezése az időben” jelentése: „tanúsítani a digitális aláírás (mint adat) meglétét egy megbízható időhivatkozás által biztosított időpontban".
Az aláírási szabályzat meghatározza a digitális aláírás időbeli elhelyezésére használható módszereket.
Az E-Magic eltérően viselkedik a két működési módjában:

- A „kezdeti ellenőrzés” működési módban, ha még nincs idő hivatkozás, összegyűjti ezt az aláírási szabályzatnak megfelelően.
- Az „utólagos ellenőrzés” működési módban az E-Magic felhasználja a kezdeti ellenőrzés során meghatározott idő hivatkozás, ha ez létezik. Ellenőrzi az aláírási szabályzatnak való megfelelőségét. Amennyiben az idő hivatkozás nem felel meg az aláírási szabályzatnak vagy hiányzik, akkor az elektronikus aláírást „érvénytelen” állapotúnak nyilvánítja.

Az E-Magic az ***aláíró tanúsítványának megfelelőség ellenőrzése*** funkción belül az aláíró tanúsítványra (mely közvetlenül, vagy hivatkozásán keresztül közvetve szerepel az aláírási tulajdonságok között) ellenőrzi az aláírási szabályzat követelményeinek teljesülését:

- a tanúsítványhoz tartozó kulcs algoritmusának ellenőrzése (csak az RSA lehet),
- a tanúsítvány kulcs lenyomat algoritmusának ellenőrzése (csak SHA1 és SHA256 lehet),
- a tanúsítvány kulcs hosszának ellenőrzése (csak 1020-nál nagyobb lehet),
- a tanúsítvány lejártának az ellenőrzése

- a tanúsítvány visszavonási címének ellenőrzése (van e CDP kiterjesztés),
- a tanúsítvány kritikus kiterjesztéseinek vizsgálata (csak az aláírási szabályzatban meghatározott kritikus kiterjesztést tartalmazhat),
- minősített eléektronikus aláírás azonosítása (a tanúsítványban szerepel-e a QCStatement kiterjesztés az id-etsi-qcs-QcCompliance OID-vel),
- a kulcshasználat kiterjesztés helyességének ellenőrzése (minősített elektronikus aláírás esetén a NonRepudiation flag értéke igaz, a többi hamis, fokozott biztonságú elektronikus aláírás esetén csak a DigitalSignature flag vagy a NonRepudiation flag értéke lehet igaz, de legalább az egyiküknek igaznak kell lennie)

Az E-Magic az **érvényes tanúsítványlánc felépítése** funkción belül (annak érdekében, hogy meggyőződjön az aláírói tanúsítvány érvényességéről és hitelességéről a digitális aláírás időpontjában) egy érvényes tanúsítványláncot keres az aláíró tanúsítványa és a Windows tanúsítvány tárban lévő egyik megbízható pont között.
Az E-Magic ezt a két működési módjában eltérő módon valósítja meg:

- A „kezdeti ellenőrzés” működési módban az E-Magic mindazon funkciókat megvalósítja, amelyeket az aláírási szabályzat szabályai megkövetelnek, egészen az érvényes tanúsítványlánc felépítéséig.
  A tanúsítványlánc felépítése során az E-Magic importálja az érvényesítő adatokat (a hálózatról), egyben ellenőrzi ezek érvényességét az alkalmazott aláírási szabályzatban meghatározott szabályok szerint.
  Amennyiben az E-Magic megállapítja, hogy nem építhető ki tanúsítványlánc, vagy minden felépített tanúsítványlánc érvénytelen, akkor az elektronikus aláírást „érvénytelen” állapotúnak nyilvánítja.
  Amennyiben az E-Magic megállapítja, hogy nem elérhetők olyan adatok, melyek tanúsítják, hogy a tanúsítványlánc egy eleme nem került visszavonásra, akkor az elektronikus aláírást „még nem eldönthető” állapotúnak nyilvánítja, s a kezdeti ellenőrzés később ismét végrehajtható lesz.
- Az „utólagos ellenőrzés” működési módban az E-Magic rekonstruálja a tanúsítványláncot és érvényességét pusztán a kezdeti ellenőrzés során összegyűjtött adatok alapján ellenőrzi.
  Amennyiben az E-Magic megállapítja, hogy az elérhető adatokból nem lehet tanúsítványláncot felépíteni, vagy az ezekből az elérhető adatokból felépíthető összes tanúsítványlánc érvénytelen, akkor az elektronikus aláírást „érvénytelen” állapotúnak nyilvánítja.
  Amennyiben a tanúsítványlánc egy elemére hiányzik olyan adat, mely tanúsítja annak nem visszavont állapotát, akkor az E-Magic az elektronikus aláírást „érvénytelen” állapotúnak nyilvánítja.

Az E-Magic a ***tanúsítvány érvényességének ellenőrzése*** funkción belül ellenőrzi a tanúsítványláncot alkotó összes tanúsítvány érvényességét, felhasználva ehhez a digitális aláírásban meghatározott idő referenciát, valamint a tanúsítványban megadott érvényességi periódust.
A tanúsítványlánc egy elemének az érvényesség ellenőrzése során az E-Magic a következő ellenőrzéseket végzi:

- az elem sértetlensége és eredet hitelessége, a hozzá tartozó aláírás felhasználásával;
- az aláírásban meghatározott idő hivatkozás időpontjának az elem érvényességi periódusba esése;
- az elem nem visszavontsága az aláírásban meghatározott idő hivatkozás időpontjában.

A fenti műveleteket az E-Magic az alkalmazandó aláírási szabályzatban meghatározott technikai részletekkel összhangban valósítja meg.

1.5.2.6 A digitális aláírásokat ellenőrző összetevő

A digitális aláírásokat ellenőrző összetevő a digitális aláírások ellenőrzéséhez szükséges (hash és aláírás ellenőrző) algoritmusokat támogató kriptográfia összetevő, melyet az ellenőrző folyamat hív meg.

Az E-Magic esetében ez az összetevő az összes alábbi típusú digitális aláírást ellenőrzi:

- a dokumentum digitális aláírása,
- a tanúsítványláncot alkotó tanúsítványok digitális aláírásai,
- a hiteles gyökér tanúsítvány (megbízható pont) digitális aláírása,
- az összegyűjtött érvényesítő adatokhoz (CRL, OCSP válaszok, időbélyeg tokenek,...) tartozó digitális aláírások.

1.5.2.7 Az aláírási szabályzatokat adminisztráló összetevő

Az aláírási szabályzatokat adminisztráló összetevő az általános modellben lehetővé teszi a hitelesített adminisztrátor számára a TOE által támogatott aláírási szabályzatok kezelését.

Az E-Magic lehetővé teszi az ellenőrző számára az alkalmazandó aláírási szabályzat alábbi részeinek beállítását:

- A kivárási idő (melynek alap értelmezett értéke 4 óra) figyelembe vételének kikapcsolása
- Tanúsítványlánc visszavonás ellenőrzési szabály beállítása (teljes aláírói lánc visszavonásának ellenőrzése/csak az aláírói tanúsítvány visszavonásának ellenőrzése)
- Időbélyeghez tartozó tanúsítványlánc visszavonás ellenőrzési szabály beállítása (teljes időbélyeg aláírói lánc visszavonásának ellenőrzése/csak az időbélyeg aláírói tanúsítvány visszavonásának ellenőrzése/nincs időbélyeg visszavonás ellenőrzés)
- OCSP hibakezelési szabály beállítása (hiba esetén CRL használata/hiba esetén folyamat megszakítás)
- OCSP szolgáltató kiválasztása (CRL (nincs OCSP)/explicit szolgáltató/ tanúsítványban szereplő OCSP szolgáltató)
- OCSP ellenőrzési szintjének meghatározása (csak végfelhasználói tanúsítványnál/teljes tanúsítvány láncon)

Az E-Magic lehetővé teszi az ellenőrző számára, hogy a már beállított aláírási szabályzat alkalmazását pontosítsa:

- Xades-T (az ellenőrzés során időbélyeget helyez el az aláíráson)
- Xades-C (az ellenőrzés során begyűjti és csatolja az ellenőrzési adatokat)
- Xades-X-L (az ellenőrzés során a begyűjtött és csatolt ellenőrzési adatokat időbélyeggel védi meg)
- Xades-A (az ellenőrzés során a teljes elektronikus aláírást archív időbélyeggel védi meg)

1.5.2.8 A XadesMagic támogatása az aláírás ellenőrzésére

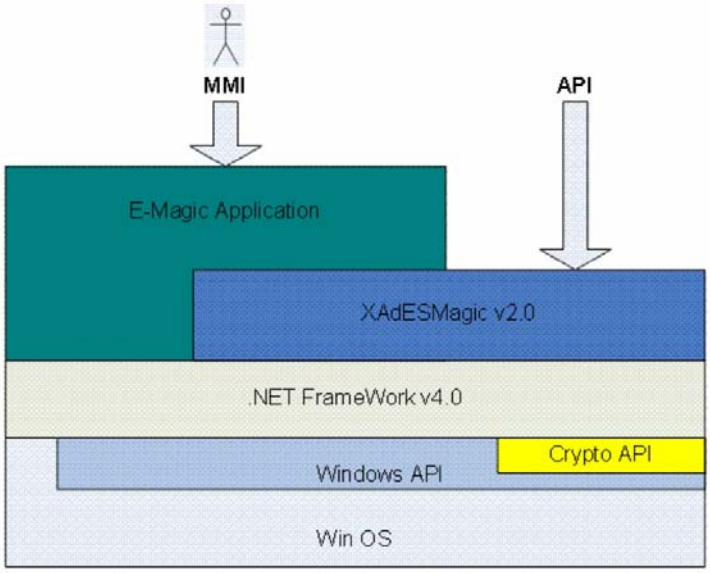
A XadesMagic felhasználója egy program lehet, mely számára API interfészt biztosít.

A XadesMagic függvényei az E-Magic (és más aláírás ellenőrző modulok) alábbi funkcionális összetevőit támogatják:

- az érvényesítő adatokat összegyűjtő és feldolgozó összetevő,
- a digitális aláírásokat ellenőrző összetevő
- az aláírási szabályzatokat adminisztráló összetevő (a különböző Xades formátum típusok kezelése)

1.5.3 Az E-Magic + XadesMagic fizikai határai

Az (E-Magic + XadesMagic)-t alkotó fizikai összetevőket és környezetét szemlélteti a 2. ábra.



2. ábra Az E-Magic + XadesMagic fizikai elemei

Az értékelés tárgyának összetevői:

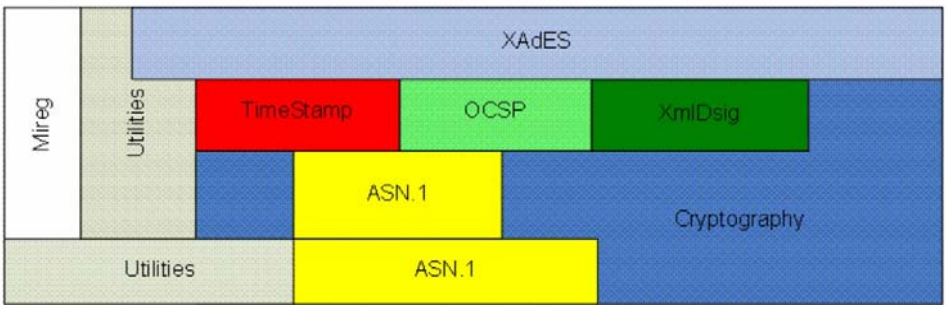
- E-Magic aláíró alkalmazás
- XadesMagic (önállóan is meghívható fejlesztő készlet)
- Felhasználói dokumentáció (E-Magic)
- Fejlesztői dokumentáció (XadesMagic)

Az értékelés tárgya az alábbi informatikai elemekből álló környezetben működőképes:

- Windows operációs rendszerek (XP, Windows7, Vista),
- Windows API (benne CryptoAPI),
- fejlesztő környezet (.NET Framework 4.0).

1.5.4 Az E-Magic + XadesMagic logikai határai

A 3. ábra a (E-Magic + XadesMagic)-t alkotó összetevőket mutatja azok tágabb üzemeltetési környezetébe eső más komponensekkel együtt. A szürke mezők a működtetési környezet által biztosított szolgáltatásokat jelentik, a színes dobozok pedig az E-Magic + XadesMagic logikai határaiba eső funkcionalitást mutatják.



3. ábra Az E-Magic + XadesMagic logikai határai és üzemeltetési környezete

1.5.5 Az E-Magic + XadesMagic értékelt konfigurációja

Értékelt E-Magic verzió: SDA.E-Magic.exe v2.0.0.3

Értékelt XadesMagic verzió: 2.0.0.2, mely az alábbi dll-ekből áll:

- SDA.XadesMagic.dll (v2.0.0.2)
- SDA.Cryptography.dll (v2.0.0.2)
- SDA.Cryptography.Framework.dll (v2.0.0.2)
- SDA.TimestampProtocol.dll (v2.0.0.2)

Az értékelt konfiguráció elemei:

Operációs rendszerek:

- XP SP3,
- Windows7,
- Vista SP2

Fejlesztő környezet: .NET Framework 4.0

Minősített elektronikus aláírás létrehozásához biztonságos aláírás-létrehozó eszközök:

- Gemalto TPC IM CC v3 (middleware: Classic Client Toolbox)
- Giesecke StarCert v2.2 (middleware: SmartSign CSP for StarCert v1.0.9.15)

Fokozott biztonságú elektronikus aláírás létrehozásához aláírás létrehozó eszköz:

- eToken Pro 64K v4.2 (middleware: Aladdin eToken PKI Client v5.0.0.65)

2 Megfelelőségi nyilatkozatok

2.1 CC megfelelőség

2.1.1 CC verzió

Jelen biztonsági előirányzat a *Common Criteria (CC) 3.1 2. javítás* verzió alapján készült (ISO/IEC 15408 IT biztonság értékelési követelményei, 1. rész: Bevezetés és általános modell, 2. rész: Funkcionális biztonsági követelmények, 3. rész: Garanciális biztonsági követelmények), és az alábbi pontokban megadott megfelelőségi állítások érvényesek rá.

Az alkalmazott CC verzió nyelve angol.

2.1.2 ST megfelelőség a CC 2. részéhez képest

Jelen biztonsági előirányzat megfelel a CC 2. részének.

2.1.3 ST megfelelőség a CC 3. részéhez képest

Jelen biztonsági előirányzat megfelel a CC 3. részének, és megfelel az EAL3 garanciaszint követelményeinek.

2.2 PP megfelelőség

Jelen biztonsági előirányzat PP megfelelőségi nyilatkozatot nem tesz, de a [PP-ESCA] és a [PP-ESVM] védelmi profilok figyelembe vételével készült.

2.3 Biztonsági követelmény csomag megfelelőség

Jelen biztonsági előirányzat nem állít biztonsági követelmény csomag megfelelőséget.

3 Biztonsági probléma meghatározás

3.1 Értékek

Ez a rész leírja a TOE által védendő értékeket.

3.1.1 Az aláírás létrehozással kapcsolatos védendő értékek

A TOE aláírás létrehozással kapcsolatos védendő értékei az alábbiak[1]:

- felhasználói adatok:
  - bemenő adatok:
    - aláírói dokumentum (D.Signatory's_Document),
    - **aláírandó adat** (D.Data_To_Be_Signed),
    - **formattált DTBS** (D.DTBS_Formatted),
    - **lenyomat értéke** (D.DTBS_Digest)
    - **DTBS reprezentáns** (D.DTBS_Representation)
  - visszaadott adatok:
    - elektronikus aláírás (D.Electronic_Signature)
- a TOE működését befolyásoló (TSF) adatok:
    - aláírási szabályzat (D.Signature_Policy),
    - szolgáltatások (D.Services),
    - belső adatábrázolás (D.Data_Representations_Association),
    - formátum/megjelenítő tábla (D.DocFormat_Application_Association).

D.Signatory's_Document
Az aláírói dokumentum (SD) az aláírási folyamat során tartalmazhat egyetlen elektronikus dokumentumot, vagy több elektronikus dokumentumot. Az aláírói dokumentum méretének nagyobnak kell lennie nullánál.

Védendő: sértetlenség

D.Data_To_Be_Signed
Az aláírandó adat (DTBS) az az információ, amelyre elektronikus aláírás kell. Az alábbiakat tartalmazza:

- az aláírandó dokumentum,
- az aláíró által közvetlenül, vagy az alkalmazás által közvetve kiválasztott aláírási tulajdonságok.

Az aláírási tulajdonságok között kötelező szerepelnie az alábbinak:

- az aláíró tanúsítványa, vagy az erre a tanúsítványra vonatkozó egyértelmű hivatkozás.

Az aláírási tulajdonságok között szerepelhetnek még az alábbiak:

- az aláírás helyére vonatkozó állítás,
- az aláírás dátumára és időpontjára vonatkozó állítás,
- tartalom-formátum,
- az aláíró munkaköre (szerepköre).

Védendő: sértetlenség

D.DTBS_Formatted
A formattált DTBS az aláírandó adat első formattált képe (envelope).

Védendő: sértetlenség

[1] Félkövér betűtípus jelzi az aláírás létrehozás specifikus védendő értékeket. (A többi védendő érték szerepel az aláírás ellenőrzésnél is.)

D.DTBS_Digest

A DTBS lenyomat a formattált DTBS lenyomata (hash képe).

Védendő: sértetlenség

D.DTBS_Representation
A DTBS reprezentáns a DTBS lenyomatnak az SCDev felé való továbbítás előtti formattálásával keletkezik.

Védendő: sértetlenség

D.Electronic_Signature
Az elektronikus aláírás tartalmazza az alábbiakat:

- DTBS lenyomat;
- az aláírás;
- az aláírás ellenőrzését lehetővé tevő egyéb adatok.

Ezt az értéket létrehozása után egészen az aláírónak való átadásig védenie kell a TOE-nak.

Védendő: sértetlenség

D.Signature_Policy
A TOE az aláírási műveleteket egy aláírási szabályzat szerint hajtja végre.

Védendő: sértetlenség

D.Services
Ez az érték a TOE által biztosított szolgáltatásokat megvalósító végrehajtható kódot jelenti.

Védendő: sértetlenség

D.Data_Representations_Association
A TOE-n belül az adatokat gyakran másképpen ábrázolják, mint ahogyan azokat az aláíró számára megjelenítik, vagy a TOE-nak beadják.
1. Példa: az aláíró kötelezettségvállalásának típusa (pl. „átolvasva és jóváhagyva”) belül egy OID-val ábrázolható, míg az interfészen közvetlenül megjeleníthető az aláró számára.
2. Példa: a dokumentum formátum belül egy OID-val ábrázolható.

Védendő: sértetlenség

D.DocFormat_Application_Association
Ez az érték (táblázat) egy a TOE által kezelt paraméter, mely alapján a TOE az aláíró számára megjelenítendő dokumentum formátumától függően eldöntheti, hogy melyik külső megjelenítő alkalmazást hívja meg.

Védendő: sértetlenség

3.1.2 Az aláírás ellenőrzéssel kapcsolatos védendő értékek

A TOE aláírás ellenőrzéssel kapcsolatos védendő értékei az alábbiak[2]:

- felhasználói adatok:
  - bemenő adatok:
    - az aláíró által aláírt dokumentum (D.Document),
    - elektronikus aláírás (D.Signature),
    - **aláírt (aláírási) tulajdonságok** (D.Signed_Attributes),
    - b**emeneti érvényesítő adatok** (D.Validation_Data_In_input)
  - munka adatok:
    - **ellenőrizendő hash érték** (D.Hash_Data_tobe_Verified)
  - visszaadott adatok:
    - **ellenőrzési állapot** (D.Return_Status),
    - **kimeneti érvényesítő adatok** (D.Validation_Data_In_Output)
- a TOE működését befolyásoló (TSF) adatok:
    - szolgáltatások (D.Services),
    - **ellenőrző motor** (D.Verification_Rules),
    - aláírási szabályzatok (D.Signature_Policies),
    - belső adatábrázolás (D.Data_Representations_Association),
    - formátum/megjelenítő tábla (D.DocFormat_Application_Association).

D. Document
Az aláíró által aláírt dokumentum az az elektronikus dokumentum, melynek aláírását a TOE-nak ellenőriznie kell. A TOE-nak megadható egy független állományban, vagy egy olyan állományban, mely az aláírást is tartalmazza.

Védendő: sértetlenség

D.Signature
Egy aláíró elektronikus aláírása egy dokumentumon.

Védendő: sértetlenség

D.Signed_Attributes
Az aláírt (aláírási) tulajdonságok azok az adatok, melyeket a dokumentummal egyszerre írtak alá. Kiegészítő információkat szolgáltatnak az ellenőrző számára az aláírásra, illetve annak végrehajtási körülményeire vonatkozóan.
Az alábbiakat tartalmazzák:

- az aláíró tanúsítványa, vagy az erre a tanúsítványra vonatkozó egyértelmű hivatkozás.

Az aláírási tulajdonságok között szerepelhetnek még az alábbiak:

- az aláírás helyére vonatkozó állítás,
- az aláírás dátumára és időpontjára vonatkozó állítás,
- a dokumentum tartalom-formátuma,
- az aláíró állított vagy tanúsított munkaköre (szerepköre).

Védendő: sértetlenség

[2] Félkövér betűtípus jelzi az aláírás ellenőrzés specifikus védendő értékeket. (A többi védendő érték szerepel az aláírás létrehozásnál is.)

D.Validation_Data_In_input
A bemeneti érvényesítő adatok az ellenőrzéshez hasznos adatok.
Az alábbiakat tartalmazhatják:

- az aláíró tanúsítványa,
- a hitelesítés-szolgáltató, a CRL publikálók, az OCSP szerverek, az időbélyegző egységek, tanúsítványa,
- tanúsítvány visszavonási lista (CRL),
- OCSP válaszok,
- szolgáltató visszavonási lista (ARL),
- időbélyeg tokenek.

Védendő: sértetlenség

Alkalmazási megjegyzés:
Ezek az adatok különböző módokon szerezhetők be:

- egy távoli szerverről (egy lokális vagy nyílt hálózatban),
- az ellenőrzést végrehajtó gépen lokálisan letárolva,
- az aláíráson belül letárolva (a formátumnak megfelelően).

D.Hash_Data_tobe_Verified

Ez az adat az aláírással kapcsolatos adatok (aláírt dokumentumok és tulajdonságok) TOE által lenyomatolt képe.

Védendő: sértetlenség

D.Return_Status

Az ellenőrzés után a TOE egy ellenőrzési állapottal tér vissza, mely az eredménytől függően:

- érvényes aláírás (“érvényes” állapot): minden szükséges elem megtalálható és helyes,
- érvénytelen aláírás (“érvénytelen” állapot): egy vagy több elem hibás,
- befejezetlen ellenőrzés (“befejezetlen ellenőrzés” állapot): az ellenőrzés során az ellenőrzéshez szükséges adatok nem voltak elérhetőek.

A kezdeti ellenőrzés esetén egy befejezetlen ellenőrzést az ellenőrző vagy érvénytelen aláírásnak tekint, vagy egy későbbi időpontban megismételhető kezdeti ellenőrzés lehetőségének. Az utólagos ellenőrzés esetén egy befejezetlen ellenőrzést az ellenőrző érvénytelen aláírásnak tekint.

Védendő: sértetlenség

D.Validation_Data_In_Output
A kimeneti érvényesítő adatok a TOE által feldolgozott érvényesítő adatok. Ezeket a TOE későbbi felhasználás céljára adja vissza az ellenőrző számára.
Ezek az adatok vagy teljesek, vagy nem. Amennyiben teljesek, felhasználhatók egy utólagos ellenőrzéshez. Ellenkező esetben ismételten felhasználhatók és kiegészíthetők egy új kezdeti ellenőrzéshez.

Védendő: sértetlenség

D.Services
Ez az érték a TOE által biztosított szolgáltatásokat megvalósító végrehajtható kódot jelenti.

Védendő: sértetlenség

D.Verification_Rules
A TOE fő összetevője egy az aláírási szabályzatban meghatározott szabályokat ellenőrző motor. Ennek végrehajtható kódja sértetlenség ellenőrzést igényel.

Védendő: sértetlenség

D.Signature_Policy
Az aláírási szabályzat azokat a szabályokat tartalmazza, melyeket egy aláírás ellenőrzése során alkalmazni kell.
A TOE több aláírási szabályzatot támogat. Az aláírási szabályzatok sértetlenségét meg kell őrizni.

Védendő: sértetlenség

Alkalmazási megjegyzés:
A TOE által elfogadott aláírási szabályzatok formája az alábbi:

- részben a TOE által értelmezhető állományok (beállítások eredményét őrző temporális állomány),
- részben az értelmezéshez szükséges végrehajtható kód formájában.

D.Data_Representations_Association
A TOE-n belül az adatokat gyakran másképpen ábrázolják, mint ahogyan azokat az ellenőrző számára megjelenítik, vagy a TOE-nak beadják.
1. Példa: az aláíró kötelezettségvállalásának típusa (pl. „átolvasva és jóváhagyva”) belül egy OID-val ábrázolható, míg az interfészen közvetlenül megjeleníthető az ellenőrző számára.
2. Példa: a dokumentum formátum belül egy OID-val ábrázolható.

Védendő: sértetlenség

D.DocFormat_Application_Association
Ez az érték (táblázat) egy a TOE által kezelt paraméter, mely alapján a TOE az ellenőrző számára megjelenítendő dokumentum formátumától függően eldöntheti, hogy melyik külső megjelenítő alkalmazást hívja meg.

Védendő: sértetlenség

Alkalmazási megjegyzés:
A dokumentum formátuma:

- az aláírásban szerepel, mint aláírt tulajdonság.

3.2 Szerepkörök /Szubjektumok

S.Signatory
Az aláíró kölcsönhatásba lép az E-Magic-kel, hogy aláírjon egy vagy több dokumentumot a beállított aláírási szabályzatnak megfelelően.
Az aláíró felelős a következő műveletekért is:

- Az E-Magic által használandó aláírási szabályzatok beállítható értékeinek megadása (aláírás helye, szerepkör, lenyomatképző algoritmus, időbélyeg szolgáltató választás, aláírás előtti időbélyeg használatának kérése, CRL és OCSP mód közötti választás, OCSP szolgáltató választás),
- a támogatott dokumentum-formátumok és megjelenítő alkalmazások közötti összerendelések kezelése (az alaplista bővítése, szűkítése).

S.Verifier
Az ellenőrző kölcsönhatásba lép az E-Magic-kel, hogy ellenőrizzen egy vagy több dokumentumot a beállított aláírási szabályzatnak megfelelően.
Az ellenőrző felelős a következő műveletekért is:

- Az E-Magic által használandó aláírási szabályzatok beállítható értékeinek megadása (Xades típus, időbélyeg szolgáltató választás, visszavonási ellenőrzés szabályok beállítása, OCSP szolgáltató választás, OCSP hibakezelés, OCSP ellenőrzési szabályok beállítása),

Alkalmazási megjegyzés:
Az E-Magic csak logikailag különbözteti meg a fenti szerepköröket, egy felhasználó betöltheti az aláíró és az ellenőrző szerepkörét is.

S.Calling_Application
A XadesMagic fejlesztőkészletet hívó alkalmazás.

3.3 Fenyegetések

3.3.1 Az aláírás létrehozással kapcsolatos fenyegetések

Mivel a biztonsági előirányzat a [CWA 14170] mértékadó dokumentumon alapuló követelményeket tartalmaz, ezért nem fenyegetések, hanem szabályok (szabályzatok) formájában képezi le ezeket a követelményeket.
Ezért a biztonsági előirányzat fenyegetéseket formálisan nem tartalmaz, minden biztonsági célt feltételezések és szervezeti biztonsági szabályzatok indokolnak.

3.3.2 Az aláírás ellenőrzéssel kapcsolatos fenyegetések

Mivel a biztonsági előirányzat a [CWA 14171] mértékadó dokumentumon alapuló követelményeket tartalmaz, ezért nem fenyegetések, hanem szabályok (szabályzatok) formájában képezi le ezeket a követelményeket.
Ezért a biztonsági előirányzat fenyegetéseket formálisan nem tartalmaz, minden biztonsági célt feltételezések és szervezeti biztonsági szabályzatok indokolnak.

3.4 Szervezeti biztonsági szabályzatok (OSP)[3]

3.4.1 Az aláírás létrehozással kapcsolatos szabályzatok

A TOE aláírás létrehozással kapcsolatos szabályzatai az alábbiak[4]:

- a létrehozott aláírások érvényességére vonatkozó szabályzatok:
  - P.Signatory_Certificate_Conformity
  - P.Signatory_Certificate_Validity
  - P.Signature_Attributes_Conformity
- a dokumentum szemantika stabilitásának ellenőrzésére vonatkozó szabályzat:
  - P.Document_Stability_Control
- a dokumentum és az aláírási tulajdonságok megjelenítésére vonatkozó szabályzatok:
  - P.Document_Presentation
  - **P.Signature_Attributes_Presentation**
- a szabványoknak való megfelelésre vonatkozó szabályzat:
  - P.Hash_Algorithms
- az aláíróval való kölcsönhatásra vonatkozó szabályzatok:
  - **P.Multiple_Documents_Signature**
  - **P.Signature_Process_Interruption**
  - **P.Explicit_Agreement**
- egyéb szabályzatok:
  - **P. Certificate/Private_Key_Association**
  - **P.Electronic_Signature_Export**
  - P.Administration

P.Signatory_Certificate_Conformity
Az érvénytelen aláírás létrehozás elkerülése érdekében a TOE-nak ellenőriznie kell, hogy az aláíró által kiválasztott tanúsítvány megfelel-e az alkalmazott aláírási szabályzatnak.

P.Signatory_Certificate_Validity
Az érvénytelen aláírás létrehozás elkerülése érdekében a TOE-nak ellenőriznie kell, hogy az aláíró által kiválasztott tanúsítványt érvényességi időszakaszán belül kívánják-e használni, és a rendelkezésre álló visszavonási információk alapján érvényes.

P.Signature_Attributes_Conformity
Az érvénytelen aláírás létrehozás elkerülése érdekében a TOE-nak ellenőriznie kell, hogy:

- az aláíró által kiválasztott aláírási tulajdonságok megfelelnek-e az alkalmazott aláírási szabályzatnak, és
- az aláírási szabályzat által megkövetelt valamennyi aláírási tulajdonság megtalálható-e.

P.Document_Stability_Control
A TOE-nak tájékoztatnia kell az aláírót, ha az aláírandó dokumentum szemantikája nem tekinthető megváltoztathatatlannak (stabilnak). Az aláíró ezt a tájékoztatást figyelmen kívül hagyhatja.

P.Document_Presentation
A TOE-nak lehetővé kell tennie, hogy az aláíró megnézhesse az aláírandó dokumentum egy megbízható megjelenítését. A TOE-nak nem szabad lehetővé tennie a dokumentum aláírását, ha az aláíró nem tudja megtekinteni azt.

[3] A szervezeti biztonsági szabályokra P. -tal kezdődő jelölést használunk (P: Policy)
[4] Félkövér betűtípus jelzi az aláírás létrehozás specifikus szabályzatokat. (A többi szabályzat szerepel az aláírás ellenőrzésnél is.)

P.Signature_Attributes_Presentation
A TOE-nak lehetővé kell tennie az aláíró számára az aláírói tulajdonságok megtekintését.

P.Hash_Algorithms
A TOE által megvalósított lenyomatoló algoritmus(ok)nak ki kell zárniuk azt, hogy két különböző dokumentum ugyanazt a hash értéket eredményezze.
A TOE által megvalósított lenyomatoló algoritmus(ok)nak meg kell felelni(e/ük) az alábbi kriptográfiai szabványnak: [FIPS 180-3].

P.Multiple_Documents_Signature
A TOE-nak lehetővé kell tennie véges számú dokumentum aláírását, ahol a véges szám egy is lehet.
Az aláíró egyetértése ezen dokumentum vagy dokumentumok aláírására azonos aláírási tulajdonságokra fog vonatkozni.

P.Signature_Process_Interruption
Az aláírónak meg kell tudni szakítania az aláírás folyamatát, még az aláíró kulcs aktivizálása előtt.

P.Explicit_Agreement
A TOE-nak az aláírási folyamat végrehajtása előtt az aláírót egy nem nyilvánvaló művelet végrehajtására kell kényszerítenie, az aláírással való egyetértése ellenőrzése céljából.

P. Certificate/Private_Key_Association
A TOE-nak továbbítania kell a szükséges információkat az SCDev felé, melynek alapján az aktivizálhatja a kiválasztott tanúsítványnak megfelelő magánkulcsot.

P.Electronic_Signature_Export
Az aláírási folyamat végén a TOE-nak át kell adnia az aláírónak a dokumentum elektronikus aláírását, mely legalább az alábbiakat tartalmazza:

- a dokumentum aláírása;
- az összes aláírt adatra vonatkozó hash érték;
- az aláíró tanúsítványára (vagy aktuális tanúsítványára) vonatkozó hivatkozás;
- az alkalmazott aláírási szabályzatra vonatkozó hivatkozás.

Alkalmazási megjegyzés:
Az aláírás ellenőrzését megkönnyítő egyéb információk is megadhatók (pl. az aláíró tanúsítványa, időbélyeg tokenek, stb.).

P.Administration
A TOE-nak lehetővé kell tennie az aláíró számára az alábbiakat:

- az aláírási szabályzat [D.Signature_Policy] beállítása,
- a dokumentum formátumok és a megjelenítő alkalmazások közötti megfeleltetés tábla [D.DocFormat_Application_Association] kezelése (hozzáadás/törlés).

3.4.2 Az aláírás ellenőrzéssel kapcsolatos szabályzatok

A TOE aláírás ellenőrzéssel kapcsolatos szabályzatai az alábbiak[5]:

- az aláírási szabályzat alkalmazására vonatkozó szabályzatok:
  - P.Signatory_Certificate_Validity
  - P.Signed_Attributes_Conformity
  - P.Signatory_Certificate_Conformity
  - **P.Signatory_Certificate_Authenticity**
  - **P.Validation_Data_Authenticity/Integrity**
- az aláírási visszaadására vonatkozó szabályzat:
  - **P.Signed_Attributes_Communication**
- a dokumentum megjelenítésére vonatkozó szabályzatok:
  - P.Document_Presentation
  - P.Document_Stability_Control
- a szabványoknak való megfelelésre vonatkozó szabályzatok:
  - P.Hash_Algorithms
  - **P.Signature_Algorithms**
- az érvényesítő adatok exportálására vonatkozó szabályzat:
  - **P.Validation_Data_Export**
- egyéb szabályzat:
  - P.Administration

P.Signatory_Certificate_Validity
A TOE-nak ellenőriznie kell, hogy az aláíró tanúsítványa érvényes volt-e az aláírást időben elhelyező időhivatkozás időpontjában.

P.Signed_Attributes_Conformity
A TOE-nak ellenőriznie kell, hogy

- az aláírt tulajdonságok megfelelnek-e az alkalmazott aláírási szabályzatnak, és
- az aláírási szabályzat által megkövetelt valamennyi aláírási tulajdonság megtalálható-e.

P.Signatory_Certificate_Conformity
A TOE-nak ellenőriznie kell, hogy a tanúsítványlánc valamennyi tanúsítványa (köztük az aláíró tanúsítványa is) megfelel-e az alkalmazott aláírási szabályzatnak.

P.Signatory_Certificate_Authenticity
A TOE-nak ellenőriznie kell, hogy létezik egy érvényes tanúsítási útvonal[6] az aláíró tanúsítványa és egy az aláírási szabályzat által hivatkozott megbízható pont között.

P.Validation_Data_Authenticity/Integrity
A TOE-nak ellenőriznie kell a felhasznált érvényesítő adatok sértetlenségét és eredetének hitelességét.

P.Signed_Attributes_Communication
A TOE-nak lehetővé kell tennie, hogy az ellenőrző megnézhesse az aláírási tulajdonságokat.

P.Document_Presentation
A TOE-nak lehetővé kell tennie, hogy az ellenőrző megnézhesse az aláírt dokumentumot.

5 Félkövér betűtípus jelzi az aláírás ellenőrzés specifikus szabályzatokat. (A többi szabályzat szerepel az aláírás létrehozásnál is.)
6 Egy ilyen tanúsítvány lánc létezése bizonyítja az aláíró tanúsítványának hitelességét a gyökér tanúsítványhoz (megbízható ponthoz) viszonyítva.

P.Document_Stability_Control
A TOE-nak tájékoztatnia kell az ellenőrzőt, ha az aláírt dokumentum szemantikája nem tekinthető megváltoztathatatlannak (stabilnak). Az ellenőrző ezt a tájékoztatást figyelmen kívül hagyhatja.

P.Hash_Algorithms
A TOE által megvalósított lenyomatoló algoritmus(ok)nak ki kell zárni(a/uk) azt, hogy két különböző dokumentum ugyanazt a hash értéket eredményezze.
A TOE által megvalósított lenyomatoló algoritmus(ok)nak meg kell felelni(e/ük) az alábbi kriptográfiai szabványnak: [FIPS 180-3].

P.Signature_Algorithms
A TOE által támogatott kriptográfiai algoritmusoknak és a TOE-ban megvalósított kulcshosszaknak ellenállónak kell lenniük a kulcsok tanúsítványának érvényességi periódusában.
A TOE által megvalósított kriptográfiai algoritmusoknak és kulcshosszaknak meg kell felelniük az alábbi mértékadó dokumentum kriptográfiai követelményeinek: [ALGO]

Alkalmazási megjegyzés:
A használt kulcsoknak meg kell felelniük az [ALGO]-ban megfogalmazott kulcs kezelési követelményeknek is.

P.Validation_Data_Export
A TOE-nak lehetővé kell tennie az ellenőrzés során használt érvényesítő adatok exportálását az ellenőrző számára.

P.Administration
A TOE-nak lehetővé kell tennie az ellenőrző számára az alábbiakat:

- az aláírási szabályzat [D.Signature_Policy] beállítása.

3.5 Feltételezések[7]

Ez a rész a TOE üzemeltetési környezetére tett feltételezéseket írja le.

3.5.1 Az aláírás létrehozással kapcsolatos feltételezések

A TOE aláírás létrehozással kapcsolatosan az üzemeltetési környezetre tett feltételezései az alábbiak[8]:

- a hosztgép platformjára vonatkozó feltételezés:
  - A.Host_Platform,
- az SCDev-re vonatkozó feltételezések:
  - **A.SCDev**,
  - **A.TOE/SCDev_Communications**,
  - **A.Signatory_Authentication_Data_Protection**
- a dokumentum megjelenítésre vonatkozó feltételezések:
  - A.Document_Presentation,
  - **A.Previous_Signatures_Presentation**
- a műveletekre vonatkozó feltételezések:
  - **A.Signatory_Presence**,
  - A.Trusted_Security_Administrator,

A.Host_Platform
Feltételezés, hogy az a hoszt platform, melyre a TOE-t telepítették, vagy közvetlenül az aláíró, vagy egy olyan szervezet felügyelete alatt áll, amelynek az aláíró munkatársa vagy ügyfele.
Feltételezés, hogy a hosztgép operációs rendszere az általa futtatott alkalmazások számára elkülönített futási környezetet biztosít.
Fentieken túl az alábbi intézkedések teljesülnek:

- a hoszt védett a vírustámadásokkal szemben;
- a hoszt platform és nyílt hálózati kapcsolattal rendelkező egyéb IT elemek közötti kommunikáció tűzfallal védett;
- a hoszt platform adminisztrátori funkcióihoz való hozzáférés a platform adminisztrátorokra korlátozott ("hoszt adminisztrátor"). A felhasználói fiók különbözik a hoszt adminisztrátoritól.
- a hoszt platform szoftverének telepítése és frissítése a hoszt adminisztrátor ellenőrzése alatt áll;
- a hoszt platform operációs rendszere nem engedi nem megbízható alkalmazások végrehajtását.

A.SCDev
Az SCDev-re feltételezés, hogy a TOE-tól kapott adatokból képes digitális aláírást létrehozni.
Feltételezés, hogy az SCDev hitelesíti az aláírót, és sikeres hitelesítés esetén lehetővé teszi számára a kiválasztott tanúsítványnak megfelelő magánkulcs aktivizálását (sikertelen hitelesítés esetén pedig nem).
Az SCDev felelős az aláíró adatainak megvédéséért.
Feltételezés, hogy az alábbi adatokat az SCDev biztonságos módon tárolja és használja:

- Az aláírás létrehozásával kapcsolatos értékek:
  - az aláíró magánkulcsa(i) (védendő a bizalmasság és sértetlenség);

[7] A feltételezésekre A. -tal kezdődő jelölést használunk (A: Assumption)
[8] Félkövér betűtípus jelzi az aláírás létrehozás specifikus feltételezéseket. (A többi feltételezés szerepel az aláírás ellenőrzésnél is.)

  - az aláíró tanúsítványa(i) vagy az erre/ezekre vonatkozó egyértelmű hivatkozás (védendő a sértetlenség);
  - a magánkulcs/tanúsítvány megfeleltetése (védendő a sértetlenség);
- Az aláíró hitelesítésével kapcsolatos értékek:
  - az aláíró hitelesítő adata (védendő a bizalmasság és sértetlenség);
  - a hitelesítő adat és a (magánkulcs, tanúsítvány) pár megfeleltetése (védendő a sértetlenség);

A megfeleltetés egy hitelesítő adatra és egy (magánkulcs, tanúsítvány) párra irányulhat. Egy SCDev több (magánkulcs, tanúsítvány) párt is tárolhat. Hozzáférésüket különböző hitelesítő adatok védhetik.

A.TOE/SCDev_Communications
Feltételezés, hogy vagy a TOE és az SCDev közötti interfészt biztosító szoftver és/vagy hardver összetevők képesek kezelni (megnyitni/lezárni) egy biztonságos csatornát, mely garantálja a kommunikáció kizárólagosságát és sértetlenségét, vagy ugyanezt a környezet biztosítja.

Alkalmazási megjegyzés:
A TOE és az SCDev közötti kommunikációt biztosító összetevők az operációs rendszerre telepített számos szoftver és/vagy hardver komponenst tartalmazhatnak (pl. PKCS#11 driver-ek vagy CSP-k (cryptographic service providers), melyek egy olyan kriptográfiai interfészt határoznak meg, amelyeket az aláíró alkalmazás hív meg, hogy elérje az aláírást létrehozó modult.

A.Signatory_Authentication_Data_Protection
Feltételezés, hogy azok a szoftver és hardver összetevők, melyek lehetővé teszik az aláíró hitelesítését az SCDev felé a kiválasztott tanúsítványnak megfelelő magánkulcs aktivizálása érdekében, garantálják a hitelesítő adatok bizalmasságát és sértetlenségét az adatok bevitele és az SCDev felé történő továbbítás során.

A.Document_Presentation
Feltételezés, hogy annak az aláírás létrehozó rendszernek, melyre a TOE-t telepítették, van egy vagy több olyan megjelenítő alkalmazása, mely:

- vagy pontosan megjeleníti az aláírandó dokumentumot,
- vagy figyelmezteti az aláírót a megjelenítő alkalmazás és a dokumentum jellemzői közötti lehetséges inkompatibilitási problémákról.

A.Previous_Signatures_Presentation
Ellenjegyző aláírás esetén feltételezés, hogy az aláírónak módjában áll legalább az előzetesen aláíró(k) személyének megismerésére, legjobb esetben ezen aláírások ellenőrzésére is.

A.Signatory_Presence
Feltételezés, hogy az aláíró jelen van a dokumentumok aláírási szándékának kinyilvánításától kezdve egészen addig, amíg hitelesítő adatainak megadásával aktivizálja aláíró kulcsát.

A.Trusted_Security_Administrator
Feltételezés, hogy a TOE-t adminisztráló aláíró megbízható, a TOE használatára kiképzett, s rendelkezik a feladatai ellátásához szükséges eszközökkel.
Feltételezés, hogy a TOE-t futtató hoszt gép adminisztrátora is megbízható, s rendelkezik a feladatai ellátásához szükséges eszközökkel.

3.5.2 Az aláírás ellenőrzéssel kapcsolatos feltételezések

A TOE aláírás ellenőrzéssel kapcsolatosan az üzemeltetési környezetre tett feltételezései az alábbiak[9]:

- a hosztgép platformjára és fizikai környezetére vonatkozó feltételezés:
  - A.Host_Platform,
- a dokumentum megjelenítésre vonatkozó feltételezés:
  - A.Document_Presentation,
- a műveletekre vonatkozó feltételezések:
  - A.Trusted_Security_Administrator,
  - **A.Validation_Data_Access**

A.Host_Platform

Feltételezés, hogy az a hoszt platform, melyre a TOE-t telepítették, vagy közvetlenül az ellenőrző felügyelete alatt, vagy egy olyan természetes vagy jogi személy felügyelete alatt áll, aki/amely garantálja az ellenőrző fél számára, hogy az alábbi biztonsági intézkedéseket alkalmazzák.

Feltételezés, hogy a hosztgép operációs rendszere az általa futtatott alkalmazások számára elkülönített futási környezetet biztosít.

Fentieken túl az alábbi intézkedések teljesülnek:

- a hoszt védett a vírustámadásokkal szemben;
- a hoszt platform és nyílt hálózati kapcsolattal rendelkező egyéb IT elemek közötti kommunikáció tűzfallal védett;
- a hoszt platform adminisztrátori funkcióihoz való hozzáférés a platform adminisztrátorokra korlátozott ("hoszt adminisztátor"). A felhasználói fiók különbözik a hoszt adminisztrátoritól.
- a hoszt platform szoftverének telepítése és frissítése a hoszt adminisztrátor ellenőrzése alatt áll;
- a hoszt platform operációs rendszere nem engedi nem megbízható alkalmazások végrehajtását;
- a hoszt kellő pontosságú rendszeridőt biztosít.

A.Document_Presentation

Feltételezés, hogy annak a hoszt platformnak, melyre a TOE-t telepítették, van egy vagy több olyan megjelenítő alkalmazása, mely:

- vagy pontosan megjeleníti az aláírandó dokumentumot,
- vagy figyelmezteti az ellenőrzőt a megjelenítő alkalmazás és a dokumentum jellemzői közötti lehetséges inkompatibilitási problémákról.

A.Trusted_Security_Administrator

Feltételezés, hogy a TOE-t adminisztráló ellenőrző megbízható, a TOE használatára kiképzett, s rendelkezik a feladatai ellátásához szükséges eszközökkel.

Feltételezés, hogy a TOE-t futtató hoszt gép adminisztrátora is megbízható, s rendelkezik a feladatai ellátásához szükséges eszközökkel.

A.Validation_Data_Access

A TOE rendelkezik minden olyan érvényesítő adattal (vagy hozzáfér ezekhez), amely egy dokumentum ellenőrzéséhez az alkalmazott aláírási szabályzat szerint szükséges.

[9] Félkövér betűtípus jelzi az aláírás ellenőrzés specifikus feltételezéseket. (A többi feltételezés szerepel az aláírás létrehozásnál is.)

4 Biztonsági célok

4.1 Az értékelés tárgyára vonatkozó biztonsági célok

4.1.1 TOE-ra vonatkozó aláírás létrehozási biztonsági célok

Az aláírás létrehozással kapcsolatos TOE-ra vonatkozó biztonsági célok az alábbiak[10]:

- általános célok:
  - **O.Certificate/Private_Key_Association**
  - O.Administration
- az aláíróval való kölcsönhatásra vonatkozó célok:
  - **O.Signature_Attributes_Presentation**
  - **O.Explicit_Agreement**
  - **O.Signature_Process_Interruption**
  - **O.Documents_To_Be_Signed**
- az aláírási szabályzat alkalmazására vonatkozó célok:
  - **O.Signatory_Certificate_Conformity**
  - **O.Signatory_Certificate_Validity**
  - **O.Signature_Attributes_Conformity**
  - **O.Electronic_Signature_Export**
- a kriptográfiai műveletekre vonatkozó cél:
  - O.Cryptographic_Operations
- a dokumentum szemantikai stabilitásának ellenőrzésére vonatkozó cél:
  - O.Document_Stability_Control
- az aláírandó dokumentumok megjelenítésére vonatkozó cél:
  - **O.Viewer_Application_Execution**

O.Certificate/Private_Key_Association
A TOE-nak továbbítania kell a szükséges információkat az SCDev felé, melynek alapján az aktivizálhatja a kiválasztott tanúsítványnak megfelelő magánkulcsot.

O.Administration
A TOE tegye lehetővé az aláíró számára az alábbiak kezelését:

- aláírási szabályzat [D.Signature_Policy] beállítása
- a dokumentum formátumok és a megjelenítő alkalmazások közötti megfeleltetés tábla [D.DocFormat_Application_Association] kezelése (hozzáadás /törlés)

O.Signature_Attributes_Presentation
A TOE-nak meg kell mutatnia az aláírónak az aláírásra kerülő aláírói tulajdonságok egy pontos reprezentációját.

O.Explicit_Agreement
A TOE-nak lehetőséget kell biztosítania az aláíró számára, hogy közvetlenül (azaz önkéntes és egyértelmű formában) kifejezze egyetértését a dokumentum(ok) kiválasztásában és a kiválasztott dokumentum(ok) aláírási folyamatának megkezdésében.

O.Signature_Process_Interruption
A TOE-nak lehetőséget kell biztosítania az aláíró számára, hogy megszakítsa az aláírás folyamatát, még az aláíró kulcs aktivizálása előtt.

[10] Félkövér betűtípus jelzi az aláírás létrehozás specifikus TOE biztonsági célokat. (A többi TOE biztonsági cél szerepel az aláírás ellenőrzésnél is.)

O.Documents_To_Be_Signed
Miután az aláíró kifejezte az aláírásra vonatkozó egyetértését, a TOE-nak garantálnia kell, hogy az aktuálisan feldolgozott dokumentumok pontosan megfelelnek az aláírásra kiválasztott dokumentumoknak.
Amennyiben az aláíró több dokumentum aláírására vonatkozóan fejezte ki egyetértését, az aláíráshoz minden dokumentumra ugyanazokat az aláírási tulajdonságokat kell használni.

O.Signatory_Certificate_Conformity
A TOE-nak ellenőriznie kell, hogy az aláíró által kiválasztott tanúsítvány megfelel az alkalmazandó aláírási szabályzat elvárásainak.

O.Signatory_Certificate_Validity
A TOE-nak ellenőriznie kell, hogy az aláíró által kiválasztott tanúsítványt annak érvényességi periódusán belül használják, és az elérhető visszavonási információk alapján érvényes.

Alkalmazási megjegyzés:
Az ebből a célból alkalmazott idő hivatkozás a hoszt platform operációs rendszere által biztosított idő.

O.Signature_Attributes_Conformity
A TOE-nak ellenőriznie kell az aláíró által kiválasztott aláírási tulajdonságok meglétét és megfelelőségét az alkalmazandó aláírási szabályzat szerint.

O.Electronic_Signature_Export
Az aláírási folyamat végén a TOE-nak át kell adnia az aláírónak a dokumentum elektronikus aláírását, mely legalább az alábbiakat tartalmazza:

- a dokumentum aláírása;
- az összes aláírt adatra vonatkozó hash érték;
- az aláíró tanúsítványára (vagy aktuális tanúsítványára) vonatkozó hivatkozás;
- az alkalmazott aláírási szabályzatra vonatkozó hivatkozás.

Alkalmazási megjegyzés:
Az aláírás ellenőrzését megkönnyítő egyéb információk is megadhatók (pl. az aláíró tanúsítványa, időbélyeg tokenek, stb.).

O.Cryptographic_Operations
A TOE-nak az alábbi kriptográfiai tulajdonságokkal rendelkező kriptográfiai algoritmusokat kell alkalmaznia:

- A lenyomatoló algoritmusoknak olyannak kell lenniük, hogy két dokumentumhoz ne forduljon elő ugyanazon lenyomat érték.
- A megvalósított kriptográfiai algoritmusoknak és azok kulcshosszainak a megfelelő nyilvános kulcsok tanúsítványaiban szereplő érvényességi idő alatt ellen kell állni a kriptográfiai támadásoknak.
- Az algoritmusoknak meg kell felelniük az alábbi mértékadó dokumentum kriptográfiai követelményeinek: [ALGO].

O.Document_Stability_Control
Minden aláírandó dokumentumra a TOE állapítsa meg a dokumentum szemantikájának megváltoztathatóságát (invariáns/stabil szemantika, variáns/nem stabil szemantika, ellenőrzési hiba). Amennyiben a dokumentum szemantikája nem stabil, a TOE tájékoztassa az aláírót a stabilitás hiányáról, aki ezt figyelmen kívül hagyhatja.

Alkalmazási megjegyzés:
A TOE a fenti célt a következőképpen teljesíti: A TOE a .txt és a .xml kiterjesztésű állományokat automatikusan stabilnak tekinti. Minden ettől eltérő kiterjesztést automatikusan megváltoztathatónak tekint, s erről tájékoztatja az aláírót.

O.Viewer_Application_Execution
A TOE legyen képes egy olyan külső alkalmazás végrehajtására, mely lehetővé teszi az aláírandó dokumentum megtekintését az aláíró számára.
A végrehajtandó megjelenítő alkalmazás azonosítása érdekeben a TOE kezelje a TOE által megengedett dokumentum formátumok és a megjelenítő alkalmazások közötti megfeleltetést.
A TOE ne engedje meg egy dokumentum aláírását, ha nem képes meghatározni, hogy melyik megjelenítő alkalmazást kell végrehajtania.

4.1.2 TOE-ra vonatkozó aláírás ellenőrzési biztonsági célok

Az aláírás ellenőrzéssel kapcsolatos TOE-ra vonatkozó biztonsági célok az alábbiak[11]:

- általános cél:
  - O.Administration
- az ellenőrzési szabályokra vonatkozó célok:
  - **O.Time_Reference**
  - **O.Certification_Path**
  - **O.Certificates_Conformity**
  - **O.Certificates_Validity**
  - **O.Validation_Data_Conformity**
  - **O.Signed_Attributes_Conformity**
- az aláírt adatok megjelenítésére vonatkozó cél:
  - **O.Presentation_Application_Execution**
  - **O.Signed_Attributes_Communication**
  - **O.Validation_Data_Export**
- a dokumentum szemantikai stabilitásának ellenőrzésére vonatkozó cél:
  - O.Document_Stability_Control
- a kriptográfiai műveletekre vonatkozó cél:
  - O.Cryptographic_Operations

O. Administration
A TOE tegye lehetővé az ellenőrző számára az alábbiak kezelését:

- aláírási szabályzat [D.Signature_Policy] beállítása.

O.Time_Reference
A TOE az alkalmazott aláírási szabályzatnak megfelelően szerezzen be egy megbízható idő hivatkozást, mely bizonyíthatóvá teszi a digitális aláírás létezését egy meghatározott időpontban.

Alkalmazási megjegyzés:
A megbízható idő hivatkozás egy idő hivatkozás bármely olyan megszerzését jelenti, amely a TOE felhasználása szempontjából biztonságosnak tekinthető. Megbízható idő hivatkozás lehet például:

- egy időbélyeg token, melyet egy az aláírási szabályzatnak megfelelő megbízható időbélyegzés-szolgáltató írt alá,
- egy időjelzés, melyet egy az aláírási szabályzatnak megfelelő megbízható szereplő biztosított.

[11] Félkövér betűtípus jelzi az aláírás létrehozás specifikus TOE biztonsági célokat. (A többi TOE biztonsági cél szerepel az aláírás létrehozásnál is.)

O.Certification_Path
A TOE-nak ellenőriznie kell, hogy érvényes tanúsítási útvonal építhető fel az alábbiak között:

- az aláíró tanúsítványa (melyre való hivatkozás szerepel az aláírási tulajdonságok között) és
- egy az aláírási szabályzatban meghatározott megbízható pont.

O.Certificates_Conformity
A TOE-nak ellenőriznie kell, hogy a tanúsítási útvonal minden tanúsítványa (ideértve az aláíró tanúsítványát is) megfelel az alkalmazott aláírási szabályzat követelményeinek.

O.Certificates_Validity
Az RFC 5280 6.1 alfejezetének és az alkalmazandó aláírási szabályzatnak megfelelően a tanúsítási útvonal minden tanúsítványára (ideértve az aláíró tanúsítványát is) a TOE-nak ellenőriznie kell az alábbiakat:

- a tanúsítvány eredetének hitelessége és a tanúsítvány sértetlensége;
- a tanúsítvány érvényes volt a digitális aláírás létrehozásakor;
- a tanúsítvány nem volt visszavont állapotú a digitális aláírás létrehozásakor.

O.Validation_Data_Conformity
A TOE-nak ellenőriznie kell, hogy az aláírások ellenőrzéséhez használt érvényesítő adatok megfelelnek-e az alkalmazott aláírási szabályzatnak, különös tekintettel arra, hogy azokat a küldőjük aláírta, biztosítván ezzel a sértetlenségét és az eredet hitelességét.

Alkalmazási megjegyzés:
Az érvényesítő adatok aláírása egyszerre teszi lehetővé ezen adatok sértetlenségének és eredet hitelességének garantálását (az alkalmazandó aláírási szabályzatnak megfelelően.

O.Signed_Attributes_Conformity
A TOE-nak ellenőriznie kell az aláírási tulajdonságok meglétét és az alkalmazott aláírási szabályzatnak való megfelelőségét.

O.Presentation_Application_Execution
A TOE legyen képes olyan külső alkalmazások végrehajtására, melyek lehetővé teszik az ellenőrző számára az ellenőrizendő aláíráshoz tartozó dokumentum megtekintését.

O.Signed_Attributes_Communication
A TOE-nak képesnek kell tennie, hogy továbbítsa az aláírási tulajdonságokat az ellenőrző számára.

Alkalmazási megjegyzés:
Ez a cél egyaránt alkalmazandó azokra az esetekre, amikor a felhasználó egy személy, illetve amikor agy meghívó alkalmazás (a továbbításra használt eszköz az első esetben egy MMI (man-machine interface), míg a másik esetben egy API (application programming interface).

O.Validation_Data_Export
A TOE tegye lehetővé az ellenőrzés során használt érvényesítő adatok exportálását az ellenőrző számára.

O.Document_Stability_Control
Minden aláírt dokumentumra a TOE állapítsa meg a dokumentum szemantikájának megváltoztathatóságát (invariáns/stabil szemantika, variáns/nem stabil szemantika, ellenőrzési hiba). Amennyiben a dokumentum szemantikája nem stabil, a TOE tájékoztassa az ellenőrzőt a stabilitás hiányáról, aki ezt figyelmen kívül hagyhatja.

Alkalmazási megjegyzés:
A TOE a fenti célt a következőképpen teljesíti: A TOE a .txt és a .xml kiterjesztésű állományokat automatikusan stabilnak tekinti. Minden ettől eltérő kiterjesztést automatikusan megváltoztathatónak tekint, s erről tájékoztatja az ellenőrzőt.

O.Cryptographic_Operations
A TOE-nak az alábbi kriptográfiai tulajdonságokkal rendelkező kriptográfiai algoritmusokat kell alkalmaznia:

- A lenyomatoló algoritmusoknak olyannak kell lenniük, hogy két dokumentumhoz ne forduljon elő ugyanazon lenyomat érték.
- A megvalósított kriptográfiai algoritmusoknak és azok kulcshosszainak a megfelelő nyilvános kulcsok tanúsítványaiban szereplő érvényességi idő alatt ellen kell állni a kriptográfiai támadásoknak.
- Az algoritmusoknak meg kell felelniük az alábbi mértékadó dokumentum kriptográfiai követelményeinek: [ALGO].

Alkalmazási megjegyzés:
A használt kulcsoknak meg kell felelniük az [ALGO]-ban megfogalmazott kulcs kezelési követelményeknek is.

4.2 Az üzemeltetési környezetre vonatkozó biztonsági célok

4.2.1 Üzemeltetési környezetre vonatkozó aláírás létrehozási biztonsági célok

Az aláírás létrehozással kapcsolatos üzemeltetési környezetre vonatkozó biztonsági célok az alábbiak[12]:

- a hosztgép platformjára vonatkozó biztonsági cél:
  - OE.Host_Platform
- az SCDev-re és környezetére vonatkozó biztonsági célok:
  - **OE.SCDev**
  - **OE.TOE/SCDev_Communications**
  - **OE.Signatory_Authentication_Data_Protection**
- az aláíró jelenlétére vonatkozó biztonsági célok:
  - **OE.Signatory_Presence**
- a dokumentum megjelenítésre vonatkozó biztonsági célok:
  - OE.Document_Presentation
- egyéb biztonsági célok:
  - OE .Trusted_Security_Administrator

OE.Host_Platform

Az a hoszt platform, melyre a TOE-t telepítették, vagy közvetlenül az aláíró, vagy egy olyan szervezet felügyelete alatt álljon, amely garantálja az aláíró számára, hogy az alábbi biztonsági intézkedéseket ténylegesen alkalmazzák.

A hoszt platform operációs rendszere elkülönített futási környezetet biztosítson az általa futtatott alkalmazások számára.

Fentieken túl az alábbi biztonsági intézkedéseket kell megvalósítani:

- a hoszt védett legyen a vírustámadásokkal szemben;
- a hoszt platform és nyílt hálózati kapcsolattal rendelkező egyéb IT elemek közötti kommunikáció tűzfallal védett legyen;
- a hoszt platform szoftverének telepítése és frissítése a hoszt adminisztrátor ellenőrzése alatt álljon;
- a hoszt platform operációs rendszere ne engedje meg nem megbízható alkalmazások végrehajtását;
- a hoszt kellő pontosságú rendszeridőt biztosít.

OE.SCDev

Az SCDev-nek képesnek kell lennie a TOE-tól kapott adatokból digitális aláírást létrehozni.

Az SCDev-nek hitelesítenie kell az aláírót, lehetővé téve számára a kiválasztott tanúsítványnak megfelelő magánkulcs aktivizálását.

Az SCDev felelős az aláíró adatainak megvédéséért. Az SCDev-nek az alábbi adatokat biztonságos módon kell tárolnia és használnia:

- az aláírás létrehozásával kapcsolatos adatok:
  - az aláíró magánkulcsa (bizalmasság és sértetlenség)
  - az aktuális tanúsítványok, vagy az aláíró tanúsítványára való hivatkozás (sértetlenség)
  - a magánykulcs és a tanúsítvány összetartozása (sértetlenség)
- az aláíró hitelességével kapcsolatos adatok:
  - az aláíró hitelesítő adata (bizalmasság és sértetlenség)
  - a hitelesítő adatok és a magánkulcs/tanúsítvány pár összetartozása (sértetlenség)

[12] Félkövér betűtípus jelzi az aláírás létrehozás specifikus környezeti biztonsági célokat. (A többi környezeti biztonsági cél szerepel az aláírás ellenőrzésnél is.)

OE.TOE/SCDev_Communications
A TOE és az SCDev közötti interfészt biztosító szoftver és/vagy hardver összetevőknek kezelniük (megnyitni/lezárni) kell tudniuk egy biztonságos csatornát, mely garantálja a kommunikáció kizárólagosságát és sértetlenségét.

OE.Signatory_Authentication_Data_Protection
Azoknak a szoftver és hardver összetevőknek, melyek lehetővé teszik az aláíró hitelesítését az SCDev felé a kiválasztott tanúsítványnak megfelelő magánkulcs aktivizálása érdekében, garantálniuk kell a hitelesítő adatok bizalmasságát és sértetlenségét az adatok bevitele és az SCDev felé történő továbbítás során.

OE.Signatory_Presence
Az aláírónak jelen kell lennie a dokumentumok aláírási szándékának kinyilvánításától kezdve egészen addig, amíg hitelesítő adatainak megadásával aktivizálja aláíró kulcsát.

Alkalmazási megjegyzés:
Amennyiben valamilyen ok miatt az aláíró nem tud jelen lenni, akkor újra kell kezdenie a folyamatot az elejétől kezdve: az aláírandó dokumentumok kiválasztása, aláírási tulajdonságok kiválasztása, stb.

OE.Document_Presentation
Annak a hosztnak, melyre a TOE-t telepítették legyen egy vagy több olyan megjelenítő alkalmazása, mely:

- vagy pontosan megjeleníti az aláírandó dokumentumot,
- vagy figyelmezteti az ellenőrzőt a megjelenítő alkalmazás és a dokumentum jellemzői közötti lehetséges inkompatibilitási problémákról.

Amennyiben az aláírandó dokumentum már maga is tartalmaz aláírásokat, a TOE környezete az aláíró számára tegye lehetővé legalább az előzetesen aláírók személyének megismerését, legjobb esetben ezen aláírások ellenőrzését is.

OE .Trusted_Security_Administrator
Az aláíró legyen megbízható, a TOE használatára kiképzett, s rendelkezzen a feladatai ellátásához szükséges eszközökkel.
A hoszt gép adminisztrátora legyen megbízható, s rendelkezzen a feladatai ellátásához szükséges eszközökkel.

4.2.2 Üzemeltetési környezetre vonatkozó aláírás ellenőrzési biztonsági célok

Az aláírás ellenőrzésével kapcsolatos üzemeltetési környezetre vonatkozó biztonsági célok az alábbiak[13]:

- a hosztgép platformjára vonatkozó biztonsági cél:
  - OE.Host_Platform
- a dokumentum megjelenítésre vonatkozó biztonsági célok:
  - OE.Document_Presentation
- egyéb biztonsági célok:
  - OE .Trusted_Security_Administrator
  - **OE.Validation_Data_Provision**

[13] Félkövér betűtípus jelzi az aláírás ellenőrzés specifikus környezeti biztonsági célokat. (A többi környezeti biztonsági cél szerepel az aláírás létrehozásnál is.)

OE.Host_Platform
Az a hoszt platform, melyre a TOE-t telepítették, vagy közvetlenül az ellenőrző, vagy egy olyan szervezet felügyelete alatt álljon, amely garantálja az ellenőrző számára, hogy az alábbi biztonsági intézkedéseket ténylegesen alkalmazzák.
A hoszt platform operációs rendszere elkülönített futási környezetet biztosítson az általa futtatott alkalmazások számára.
Fentieken túl az alábbi biztonsági intézkedéseket kell megvalósítani:

- a hoszt védett legyen a vírustámadásokkal szemben;
- a hoszt platform és nyílt hálózati kapcsolattal rendelkező egyéb IT elemek közötti kommunikáció tűzfallal védett legyen;
- a hoszt platform szoftverének telepítése és frissítése a hoszt adminisztrátor ellenőrzése alatt álljon;
- a hoszt platform operációs rendszere ne engedje meg nem megbízható alkalmazások végrehajtását.
- a hoszt kellő pontosságú rendszeridőt biztosít.

OE.Document_Presentation
Annak a hosztnak, melyre a TOE-t telepítették legyen egy vagy több olyan megjelenítő alkalmazása, mely:

- vagy pontosan megjeleníti az aláírt dokumentumot,
- vagy figyelmezteti az ellenőrzőt a megjelenítő alkalmazás és a dokumentum jellemzői közötti lehetséges inkompatibilitási problémákról.

OE.Validation_Data_Provision
A TOE környezete biztosítsa az aláírás ellenőrzéséhez szükséges érvényesítő adatokat.

OE.Trusted_Security_Administrator
Az ellenőrző legyen megbízható, a TOE használatára kiképzett, s rendelkezzen a feladatai ellátásához szükséges eszközökkel.
A hoszt gép adminisztrátora legyen megbízható, s rendelkezzen a feladatai ellátásához szükséges eszközökkel.

4.3 A biztonsági célok indoklása

Ez a fejezet a biztonsági szabályzatok, a feltételezések, valamint a TOE és környezeti biztonsági célok vonatkozásában áttekinti, hogy minden szabályzatot lefed-e TOE biztonsági cél, és minden feltételezéshez szerepel-e környezet által teljesítendő biztonsági cél.

4.3.1 A TOE-ra vonatkozó aláírás létrehozási biztonsági célok indoklása

4.3.1.1 A biztonsági szabályzatok lefedése a biztonsági célokkal

P.Signatory_Certificate_Conformity: Ezt a szabályzatot a vele megegyező szövegezésű alábbi biztonsági cél teljes mértékben lefedi: ***O.Signatory_Certificate_Conformity***.

P.Signatory_Certificate_Validity: Ezt a szabályzatot a vele megegyező szövegezésű alábbi biztonsági cél teljes mértékben lefedi: ***O.Signatory_Certificate_Validity***.

P.Signature_Attributes_Conformity: Ezt a szabályzatot a vele megegyező szövegezésű alábbi biztonsági cél teljes mértékben lefedi: **O.*Signatory_Attributes_Conformity***.

P.Document_Stability_Control: Ezt a szabályzatot az alábbi biztonsági cél fedi le:

- ***O.Document_Stability_Control***, mely a TOE-ra megköveteli, hogy a TOE képes legyen megállapítani az aláírandó dokumentum szemantikájának stabilitását.

P.Document_Presentation: E szabályzatot az alábbi biztonsági célok fedik le:

- ***O.Viewer_Application_Execution*** és ***OE.Document_Presentation***, melyek megkövetelik, hogy
  - egyrészt a TOE legyen képes egy olyan külső alkalmazás végrehajtására, mely lehetővé teszi az aláírandó dokumentum megtekintését az aláíró számára,
  - másrészt a TOE akadályozza meg azoknak a dokumentumoknak az aláírását, melyekre nem lehet egy megjelenítő alkalmazást végrehajtani.

P.Signature_Attributes_Presentation: Ezt a szabályzatot a vele megegyező szövegezésű alábbi biztonsági cél teljes mértékben lefedi: ***O.Signature_Attributes_Presentation***.

P.Hash_Algorithms: Ezt a szabályzatot a vele megegyező szövegezésű alábbi biztonsági cél teljes mértékben lefedi: ***O.Cryptographic_Operations***.

P.Multiple_Documents_Signature: Ezt a szabályzatot az alábbi biztonsági cél fedi le:

- ***O.Documents_To_Be_Signed***, mely megköveteli, hogy:
  - a TOE garantálja, hogy az aláírt dokumentumok pontosan megfelelnek az aláírásra kiválasztott dokumentumoknak (nincs hozzáadás, törlés vagy helyettesítés a dokumentumok listájában);
  - minden aláírt dokumentumra ugyanazok az aláírási tulajdonságok kerülnek felhasználásra, ha az aláíró több dokumentum aláírására vonatkozóan fejezte ki egyetértését.

P.Signature_Process_Interruption: Ezt a szabályzatot a vele megegyező szövegezésű alábbi biztonsági cél teljes mértékben lefedi: ***O.Signature_Process_Interruption***.

P.Explicit_Agreement: Ezt a szabályzatot a vele megegyező szövegezésű alábbi biztonsági cél teljes mértékben lefedi: ***O.Explicit_Agreement***.

P.Certificate/Private_Key_Association: Ezt a szabályzatot a vele megegyező szövegezésű alábbi biztonsági cél teljes mértékben lefedi: ***O.Certificate/Private_Key_Association*.**

P.Electronic_Signature_Export: Ezt a szabályzatot a vele megegyező szövegezésű alábbi biztonsági cél teljes mértékben lefedi: **O.Electronic_Signature_Export**.

P.Administration: Ezt a szabályzatot az alábbi biztonsági célok fedik le:

- ***O.Administration***, mely a szabályzatban használtakhoz hasonló megfogalmazást tartalmaz.
- ***OE.Trusted_Security_Administrator***, mely biztosítja, hogy az aláíró nem egy támadó.

4.3.1.2 A feltételezések lefedése a környezetre vonatkozó biztonsági célokkal

A.Host_Platform: Ezt a szabályzatot a vele megegyező szövegezésű alábbi biztonsági cél teljes mértékben lefedi: ***OE.Host_Platform***.

A.SCDev: Ezt a szabályzatot a vele megegyező szövegezésű alábbi biztonsági cél teljes mértékben lefedi: ***OE.SCDev***.

A.TOE/SCDev_Communications: Ezt a szabályzatot a vele megegyező szövegezésű alábbi biztonsági cél teljes mértékben lefedi: ***OE.TOE/SCDev_*Communications**.

A.Signatory_Authentication_Data_Protection: Ezt a szabályzatot a vele megegyező szövegezésű alábbi biztonsági cél teljes mértékben lefedi: ***OE.Signatory_Authentication_Data_Protection***.

A.Document_Presentation: Ezt a szabályzatot a vele megegyező szövegezésű alábbi biztonsági cél teljes mértékben lefedi: ***OE.Document_Presentation***.

A.Previous_Signatures_Presentation: Ezt a szabályzatot a vele megegyező szövegezésű alábbi biztonsági cél teljes mértékben lefedi: ***OE.Previous_Signatures_Presentation*.**

A.Signatory_Presence: Ezt a szabályzatot a vele megegyező szövegezésű alábbi biztonsági cél teljes mértékben lefedi: ***OE.Signatory_Presence***.

A.Trusted_Security_Administrator: Ezt a szabályzatot a vele megegyező szövegezésű alábbi biztonsági cél teljes mértékben lefedi: ***OE.Trusted_Security_Administrator*.**

4.3.1.3 Megfeleltetés a biztonsági szabályzatok és a biztonsági célok között

Biztonsági szabályzatok (OSP)	Biztonsági célok
P.Signatory_Certificate_Conformity	O.Signatory_Certificate_Conformity
P.Signatory_Certificate_Validity	O.Signatory_Certificate_Validity
P.Signature_Attributes_Conformity	O.Signature_Attributes_Conformity
P.Document_Stability_Control	O.Document_Stability_Control
P.Document_Presentation	O.Viewer Application Execution OE.Document_Presentation
P.Signature_Attributes_Presentation	O.Signature_Attributes_Presentation
P.Hash_Algorithms	O.Cryptographic_Operations
P.Multiple_Documents_Signature	O.Documents_To_Be_Signed
P.Signature_Process_Interruption	O.Signature_Process_Interruption
P.Explicit_Agreement	O.Explicit_Agreement
P.Certificate/Private_Key_Association	O.Certificate/Private_Key_Association
P.Electronic_Signature_Export	O.Electronic_Signature_Export
P.Administration	O.Administration OE.Trusted_Security_Administration

4.1. táblázat: Az OSP-k lefedettsége a biztonsági célokkal

Feltételezések	Az üzemeltetési környezetre vonatkozó biztonsági célok
A.Host_Platform	OE.Host_Platform
A.SCDev	OE.SCDev
A.TOE/SCDev_Communications	OE.TOE/SCDev_Communications
A.Siqnatory_Authentication_Data_ Protection	OE.Siqnatory_Authentication_Data_ Protection
A.Document_Presentation	OE.Document_Presentation
A.Previous_Signatures_Presentation	OE.Document_Presentation
A.Signatory_Presence	OE.Signatory_Presence
A.Trusted_Security_Administrator	OE.Trusted_Security_Administrator

4.2. táblázat: A feltételezések lefedettsége
az üzemeltetési környezetre vonatkozó biztonsági célokkal

TOE biztonsági célok	Biztonsági szabályzatok (OSP)
O.Certificate/Private_Key_Association	P.Certificate/Private_Key_Association
O.Signature_Attributes_Presentation	P.Signature_Attributes_Presentation
O.Explicit_Agreement	P.Explicit_Agreement
O.Signature_Process_Interruption	P.Signature_Process_Interruption
O.Documents_To_Be_Signed	P.Multiple_Documents_Signature
O.Signatory_Certificate_Conformity	P.Signatory_Certificate_Conformity
O.Signatory_Certificate_Validity	P.Signatory_Certificate_Validity
O.Signature_Attributes_Conformity	P.Signature_Attributes_Conformity
O.Electronic_Signature_Export	P.Electronic_Signature_Export
O.Administration	P.Administration
O.Cryptographic_Operations	P.Hash_Algorithms
O.Document_Stability_Control	P.Document_Stability_Control
O.Viewer Application Execution	P.Document_Presentation

4.3. táblázat: A TOE biztonsági célok lefedettsége az OSP-kel

Az üzemeltetési környezetre vonatkozó biztonsági célok	Biztonsági szabályzatok (OSP) és Feltételezések
OE.Host_Platform	A.Host_Platform
OE.SCDev	A.SCDev
OE.TOE/SCDev_Communication	A.TOE/SCDev_Communications
OE.Signatory_Authentication_Data_ Protection	A.Siqnatory_Authentication_Data_ Protection
OE.Signatory_Presence	A.Signatory_Presence
OE.Document_Presentation	P.Document_Presentation A.Document_Presentation A.Previous_Signatures_Presentation
OE.Trusted_Security_Administration	P.Administration A.Trusted_Security_Administrator

4.4. táblázat: Az üzemeltetési környezetre vonatkozó biztonsági célok lefedettsége a biztonsági szabályzatokkal és a feltételezésekkel

4.3.2 A TOE-ra vonatkozó aláírás ellenőrzési biztonsági célok indoklása

4.3.2.1 A biztonsági szabályzatok lefedése a biztonsági célokkal

P.Signatory_Certificate_Validity: Ezt a szabályzatot az alábbi biztonsági célok fedik le:

- ***O.Time_Reference***, mely megköveteli az aláírás időbeli elhelyezését,
- ***O.Certificates_Validity***, mely megköveteli, hogy a TOE ellenőrizze az aláíráshoz használt aláírói tanúsítvány érvényességét az aláírás időpontjában.

P.Signed_Attributes_Conformity: Ezt a szabályzatot a vele megegyező szövegezésű ***O.Signed_Attributes_Conformity*** biztonsági cél teljes mértékben lefedi.

P.Signatory_Certificate_Conformity: Ezt a szabályzatot a vele megegyező szövegezésű ***O.Signatory_Certificate_Conformity*** biztonsági cél teljes mértékben lefedi.

P.Signatory_Certificate_Authenticity: Ezt a szabályzatot az alábbi biztonsági cél fedi le:

- ***O.Certification_Path***, mely megköveteli, hogy a TOE ellenőrizze egy érvényes tanúsítási útvonal létezését, hitelesítve ezzel az aláíráshoz használt aláírói tanúsítványt.

P.Validation_Data_Authenticity/Integrity: Ezt a szabályzatot az alábbi biztonsági cél fedi le:

- ***O.Validation_Data_Conformity***, mely megköveteli, hogy az érvényesítő adatokat küldője aláírja.

P.Signed_Attributes_Communication: Ezt a szabályzatot az alábbi biztonsági cél fedi le:

- ***O.Signed_Attributes_Communication***, mely megköveteli, hogy a TOE jelenítse meg az aláírási tulajdonságokat az ellenőrzőnek.

P.Document_Presentation: Ezt a szabályzatot az alábbi biztonsági célok fedik le:

- ***OE.Document_Presentation***, mely megköveteli, hogy a TOE környezete biztosítson egy alkalmazást, mely lehetővé teszi az ellenőrző számára az aláírt dokumentum megtekintését.
- ***O.Presentation_Application_Execution***, mely megköveteli, hogy egyrészt a TOE legyen képes a környezete által biztosított megjelenítő alkalmazás végrehajtására az ellenőrző kérésére, másrészt ezt a funkcionalitást ki lehessen kapcsolni a telepítés során.

P.Document_Stability_Control: Ezt a szabályzatot az alábbi biztonsági cél fedi le:

- ***O.Document_Stability_Control***, mely a TOE-ra megköveteli, hogy legyen képes megállapítani az aláírt dokumentum szemantikájának stabilitását, s az eredményről tájékoztatni az ellenőrzőt.

P.Hash_Algorithms: Ezt a szabályzatot a vele megegyező szövegezésű részt tartalmazó ***O.Cryptographic_Operations*** biztonsági cél közvetlenül lefedi.

P.Signature_Algorithms: Ezt a szabályzatot a vele megegyező szövegezésű részt tartalmazó ***O.Cryptographic_Operations*** biztonsági cél közvetlenül lefedi.

P.Validation_Data_Export: Ezt a szabályzatot a vele megegyező szövegezésű ***O.Validation_Data_Export*** biztonsági cél teljes mértékben lefedi.

P.Administration: Ezt a szabályzatot az alábbi biztonsági célok fedik le:

- ***O.Administration***, mely a szabályzatban használtakhoz hasonló megfogalmazást tartalmaz.
- ***OE.Trusted_Security_Administrator***, mely biztosítja, hogy az ellenőrző nem egy támadó.

4.3.2.2 A feltételezések lefedése a környezetre vonatkozó biztonsági célokkal

A.Host_Platform: Ezt a feltételezést a vele megegyező szövegezésű ***OE.Host_Platform*** biztonsági cél teljes mértékben lefedi.

A.Document_Presentation: Ezt a feltételezést a vele megegyező szövegezésű ***OE.Document_Presentation*** biztonsági cél teljes mértékben lefedi.

A.Validation_Data_Access: Ezt a feltételezést teljes mértékben lefedi az ***OE.Validation_Data_Provision*** biztonsági cél, mely megköveteli, hogy a TOE környezete biztosítsa az aláírás ellenőrzéséhez szükséges érvényesítő adatokat.

A.Trusted_Security_Administrator: Ezt a feltételezést a vele megegyező szövegezésű ***OE.Trusted_Security_Administrator*** biztonsági cél teljes mértékben lefedi.

4.3.2.3 Megfeleltetés a szervezeti biztonsági szabályzatok és a biztonsági célok között

Szervezeti biztonsági szabályzatok (OSP)	Biztonsági célok
P.Signatory_Certificate_Validity	O.Time_Reference, O.Certificate_Validity
P.Signed_Attributes_Conformity	O.Signed_Attributes_Conformity
P.Signatory_Certificate_Conformity	O.Certificate_Conformity
P.Signatory_Certificate_Authenticity	O.Certificate_Path
P.Validation_Data_Authenticity/Integrity	O.Validation_Data_Conformity
P.Signed_Attributes_Communication	O.Signed_Attributes_Communication
P.Document_Presentation	OE.Document_Presentation O.Presentation_Application_Execution
P.Document_Stability_Control	O.Document_Stability_Control
P.Hash_Algorithms	O.Cryptographic_Operations
P.Signature_Algorithms	O.Cryptographic_Operations
P.Validation_Data_Export	O.Validation_Data_Export
P.Administration	O.Administration OE.Trusted_Security_Administration

4.5. táblázat: Az OSP-k lefedettsége a biztonsági célokkal

Feltételezések	Az üzemeltetési környezetre vonatkozó biztonsági célok
A.Host_Platform	OE.Host_Platform
A.Document_Presentation	OE.Document_Presentation
A.Validation_Data_Access	OE.Validation_Data_Provision
A.Trusted_Security_Administrator	OE.Trusted_Security_Administrator

4.6. táblázat: A feltételezések lefedettsége a környezetre vonatkozó biztonsági célokkal

TOE biztonsági célok	Szervezeti biztonsági szabályzatok (OSP)
O.Administration	P.Administration
O.Time Reference	P.Signatory_Certificate_Validity
O.Certification_Path	P.Signatory_Certificate_Authenticity
O.Certificate_Conformity	P.Signatory_Certificate_Conformity
O.Certificate_Validity	P.Signatory_Certificate_Validity
O.Validation_Data_Conformity	P.Validation_Data_Authenticity/Integrity
O.Signed_Attributes_Conformity	P.Signed_Attributes_Conformity
O.Presentation_Application_Execution	P.Document_Presentation
O.Signed_Attributes_Communication	P.Signed_Attributes_Communication
O.Validation_Data_Export	P.Validation_Data_Export
O.Document_Stability_Control	P.Document_Stability_Control
O.Cryptographic_Operations	P.Hash_Algorithms, P.Signature _Algorithms

4.7. táblázat: A TOE biztonsági célok lefedettsége a biztonsági szabályzatokkal

Az üzemeltetési környezetre vonatkozó biztonsági célok	Szervezeti biztonsági szabályzatok (OSP) és feltételezések
OE.Host_Platform	A.Host_Platform
OE.Document_Presentation	P.Document_Presentation, A.Document_Presentation
OE.Validation_Data_Provision	A.Validation_Data_Access
OE.Trusted_Security_Administration	P.Administration A.Trusted_Security_Administrator

4.8. táblázat: A környezetre vonatkozó biztonsági célok lefedettsége a biztonsági szabályzatokkal és a feltételezésekkel

5 A kiterjesztett biztonsági követelmények definiálása

5.1 Kiterjesztett funkcionális biztonsági követelmények

Jelen biztonsági előirányzat nem tartalmaz kiterjesztett funkcionális biztonsági követelményeket.

5.2 Kiterjesztett garanciális biztonsági követelmények

Jelen biztonsági előirányzat nem tartalmaz kiterjesztett garanciális biztonsági követelményeket.

6 Biztonsági követelmények

6.1 Funkcionális biztonsági követelmények

A funkcionális biztonsági követelményekben az alábbi két szakkifejezés szerepel egy finomítás jelzésére:

- *Szerkesztői finomítás*: (a [CC1]-ben meghatározott szakkifejezés): olyan finomítás, melynél egy követelmény elemben egy kisebb módosítást (pl. az angol nyelvtan szabályainak megfelelő szórend sorrend cserét) hajtottak végre. Ez a módosítás nem változtathatja meg a követelmény értelmét.
- *Finomítás*: olyan finomítás, mely egy követelmény elemben vagy egy összetevő minden követelmény elemében pontosítás hozzáadását vagy az elfogadható megvalósítások korlátozását teszi lehetővé.

6.1.1 Az aláírás létrehozására vonatkozó funkcionális biztonsági követelmények

A 6.1 táblázat felsorolja a funkcionális biztonsági követelményekben szereplő szubjektumokat, objektumokat, műveleteket és ezek biztonsági tulajdonságait.

Szubjektum	objektum/ információ	Művelet	biztonsági tulajdonság
aláíró	aláírandó dokumentum	a dokumentum importálása	**aláíró:** - aláírási szabályzat - az aláíró közvetlen egyetértése az aláírásra (nem stabil dokumentum esetén) **aláírandó dokumentum:** - dokumentum azonosító - a dokumentum stabilitás állapota
aláíró	az aláíró tanúsítványa	az aláíró tanúsítványának importálása	**az aláíró:** - az alkalmazott aláírási szabályzat **az aláíró tanúsítványa:** - a kulcshasználat állapota (key usage) - QCStatement - tanúsítvány azonosító
aláíró, SCDev	a formattált DTBS elektronikus aláírás	a formattált DTBS SCDev-hez továbbítása	**az aláíró:** - az alkalmazott aláírási szabályzat - az aláíró tanúsítványa - az aláíró közvetlen egyetértése az aláírásra (nem stabil dokumentum esetén) **a formattált DTBS:** - a formattált DTBS **az elektronikus aláírás:** - állított szerepkör - az aláírás állított dátuma és időpontja - az aláírás állított helye
aláíró, SCDev	elektronikus aláírás	az elektronikus aláírás aláíróhoz exportálása	**az SCDev:** - az aláírás létrehozási folyamat állapota **az elektronikus aláírás:** - az előállított elektronikus aláírás - az aláírt dokumentum hash értéke - az aláíró tanúsítványára való hivatkozás

6.1. táblázat: a funkcionális biztonsági követelményekben szereplő szubjektumok, objektumok, műveleteket és ezek biztonsági tulajdonságai

6.1.1.1 Dokumentum stabilitás ellenőrzése

Az alábbi követelmények az aláírt dokumentumok szemantikai stabilitásának ellenőrzésére vonatkoznak.

FDP_IFC.1/Dokumentum elfogadás: Részleges információ áramlás ellenőrzés

FDP_IFC.1. 1/ Dokumentum elfogadás

A TSF-nek érvényt kell szereznie a **dokumentum elfogadás** információ áramlás ellenőrzés szabályzatnak az alábbiakon:

- szubjektum: **az aláíró**
- információ: **az aláírandó dokumentum**
- művelet: **a dokumentum importálása**

FDP_IFF.1/Dokumentum elfogadás: Egyszerű biztonsági attribútumok

FDP_IFF.1.1/Dokumentum elfogadás

A TSF-nek érvényt kell szereznie a **dokumentum elfogadás** információ áramlás ellenőrzés szabályzatnak a szubjektumok és információk alábbi biztonsági tulajdonságain alapulva:

- szubjektum: **az aláíró (aláírási szabályzat, az aláíró közvetlen egyetértése az aláírásra nem stabil dokumentum esetén)**
- információ: **az aláírandó dokumentum (dokumentum azonosító, a dokumentum stabilitás állapota)**.

FDP_IFF.1.2/Dokumentum elfogadás

A TSF-nek a következő szabályok betartása esetén engedélyeznie kell egy ellenőrzött szubjektumok és információk közötti, ellenőrzött műveleten keresztül megvalósuló információ áramlást:

A dokumentum importálása

- **vagy a dokumentum stabilitás állapota: "stabil",**
- **vagy a dokumentum stabilitás állapota: "nem stabil" vagy "nem ellenőrizhető", de az aláírási szabályzat megengedi ennek az ellenőrzésnek a megkerülését, és az aláíró közvetlenül egyetértett az ellenőrzés megkerülésével.**

FDP_IFF.1.3/Dokumentum elfogadás

A TSF-nek érvényt kell szereznie az alábbiaknak: **nincs további információ áramlás ellenőrzés szabályzat.**

FDP_IFF.1.4/Dokumentum elfogadás

A TSF-nek közvetlenül engedélyeznie kell az információ áramlást az alábbi szabályokon alapulva:

- **sikeres ellenőrzések, vagy**
- **megkerült ellenőrzések.**

FDP_IFF.1.5/Dokumentum elfogadás

A TSF-nek közvetlenül vissza kell utasítania az információ áramlást az alábbi szabályokon alapulva:

- **sikertelen ellenőrzések, és**
- **az ellenőrzéseket nem lehet megkerülni.**

Alkalmazási megjegyzés:

Az E-Magic a fenti követelményt az alábbi módon teljesíti:

- Automatikusan stabilnak tekinti a .txt és .xml állományokat,
- Automatikusan nem stabilnak tekinti az összes olyan egyéb kiterjesztésű állományt, amely kiterjesztése szerepel a „kiterjesztés – megjelenítő alkalmazás” összerendelés listában. Ezekre az ellenőrzés megkerülhető, de az aláíró közvetlen egyetértését kéri az aláírási folyamat folytatására.
- Automatikusan nem stabilnak tekinti az összes olyan kiterjesztésű állományt, amely kiterjesztése nem szerepel a „kiterjesztés – megjelenítő alkalmazás” összerendelés listában. Ezekre az ellenőrzés nem megkerülhető, az aláírás folyamat megszakad..

FDP_ITC.1/Dokumentum elfogadás: Felhasználói adatok importálása biztonsági tulajdonságok nélkül

FDP_ITC.1. 1/Dokumentum elfogadás

A TSF-nek érvényre kell juttatnia a **dokumentum elfogadás** információ áramlás ellenőrzési szabályt az SFP-k által felügyelt felhasználói adatok TOE-n kívülről történő importálása során.

FDP_ITC.1.2/Dokumentum elfogadás

A TSF-nek figyelmen kívül kell hagynia az importált felhasználói adatokhoz kapcsolódó biztonsági tulajdonságokat a TOE-n kívülről történő importálás során.

FDP_ITC.1.3/Dokumentum elfogadás

A TSF-nek érvényre kell juttatnia az alábbi szabályokat amikor az SFP ellenőrzése alatt a TOE-n kívülről felhasználói adatot importál:

- **meg kell állapítani a dokumentum szemantikáját („stabil”, „nem stabil”),**
- **az aláírót tájékoztatni kell arról, ha a dokumentum szemantikája nem stabil.**

FMT_MSA.3/Dokumentum elfogadás: Statikus tulajdonságok kezdeti értékadása

FMT_MSA.3.1/Dokumentum elfogadás

A TSF-nek érvényre kell juttatnia a **dokumentum elfogadás** információ áramlás ellenőrzési szabályt azzal, hogy **korlátozó** alapértékeket ad az SFP-t megvalósító biztonsági tulajdonságoknak.

FMT_MSA.3.2/Dokumentum elfogadás [Szerkesztői finomítás]

A TSF-nek **senki** számára sem szabad lehetővé tennie az alapértékek alternatív kezdeti értékekkel való felülírását egy objektum vagy információ létrehozásakor.

FMT_MSA.1/Kiválasztott dokumentumok: Biztonsági tulajdonságok kezelése

FMT_MSA.1.1/Kiválasztott dokumentumok

A TSF-nek érvényt kell szereznie a **dokumentum elfogadás** információ áramlás ellenőrzés szabályzatnak azzal, hogy az **aláíróra** korlátozza az alábbi biztonsági tulajdonság **kiválasztását**: **az aláírandó dokumentumok azonosítói.**

FMT_SMF.1/Egy dokumentum lista kiválasztása: Menedzsment funkciók megadása

FMT_SMF.1.1/Egy dokumentum lista kiválasztása

A TSF-nek képesnek kell lennie a következő biztonsági menedzsment funkció végrehajtására:

- **az aláírandó dokumentumok listájának kiválasztása.**

Finomítás:

A TSF-nek addig kell lehetőséget biztosítania az aláírandó dokumentumok listájának kiválasztására, amíg az aláíró kinyilvánítja aláírási szándékát.

Alkalmazási megjegyzés:

Az aláírandó dokumentumok listája nem változtatható meg az aláíró aláírási szándékának kinyilvánítását követően. Ugyanakkor az aláíró bármikor megszakíthatja az aláírás folyamatát (lásd FDP_ROL.2/ Az aláírási folyamat megszakítása).

FMT_MSA.1/Dokumentum szemantika stabilitás állapota: Biztonsági tulajdonságok kezelése

FMT_MSA.1.1/A dokumentum stabilitás állapota [Szerkesztői finomítás]

A TSF-nek érvényt kell szereznie a **dokumentum elfogadás** információ áramlás ellenőrzés szabályzatnak azzal, hogy **senki** számára nem teszi lehetővé az alábbi biztonsági tulajdonság **módosítását**: **a dokumentum stabilitás állapota.**

FMT_SMF.1/A dokumentum stabilitás állapot megszerzése: Menedzsment funkciók megadása

FMT_SMF.1.1/A dokumentum stabilitás állapot megszerzése

A TSF-nek képesnek kell lennie a következő biztonsági menedzsment funkció végrehajtására:

- **a dokumentum kiterjesztés, valamint a dokumentum formátum /megjelenítő összerendelés tábla vizsgálatával a dokumentum szemantika stabilitási állapotának megállapítása (stabil vagy nem stabil).**

FMT_MSA.1/Az aláíró egyetértése nem stabil dokumentum aláírására: Biztonsági tulajdonságok kezelése

FMT_MSA.1.1/Az aláíró egyetértése nem stabil dokumentum aláírására

A TSF-nek érvényt kell szereznie a **dokumentum elfogadás** információ áramlás ellenőrzés szabályzatnak azzal, hogy az **aláíróra** korlátozza az alábbi biztonsági tulajdonság **módosítását**: **aláíró egyetértése egy nem stabil dokumentum aláírására**.

FMT_SMF.1/Az aláíró egyetértése nem stabil dokumentum aláírására: Menedzsment funkciók megadása

FMT_SMF.1.1/Az aláíró egyetértése nem stabil dokumentum aláírására

A TSF-nek képesnek kell lennie a következő biztonsági menedzsment funkció végrehajtására:

- **az aláíró közvelen egyetértésének megszerzése egy nem stabil szemantikájú dokumentum aláírására.**

6.1.1.2 Az aláíróval való kölcsönhatás

FDP_ROL.2/Az aláírási folyamat megszakítása: Emelt szintű visszagörgetés

FDP_ROL.2.1/Az aláírási folyamat megszakítása

A TSF-nek érvényt kell szereznie az **aláírás létrehozás** információ áramlás ellenőrzés szabályzatnak azáltal, hogy megengedi **az elektronikus alárásra és tulajdonságaira irányuló összes művelet visszagörgetését**.

FDP_ROL.2.2/Az aláírási folyamat megszakítása [Szerkesztői finomítás]

A TSF-nek meg kell engednie a műveletek visszapörgetését [**a formattált DTBS-nek az SCDev felé való továbbítása előtt]**.

6.1.1.3 Ellenőrzési szabályok

FMT_MSA.1/Aláírási tulajdonságok: Biztonsági tulajdonságok kezelése

FMT_MSA.1.1/Aláírási tulajdonságok

A TSF-nek érvényt kell szereznie az **aláírás létrehozás** információ áramlás ellenőrzés szabályzatnak azáltal, hogy az **aláíróra** korlátozza az alábbi biztonsági tulajdonság **kiválasztását**: **aláírási tulajdonságok**.

FMT_SMF.1/Az aláírási tulajdonságok módosítása: Menedzsment funkciók megadása

FMT_SMF.1.1/Az aláírási tulajdonságok módosítása

A TSF-nek képesnek kell lennie a következő biztonsági menedzsment funkció végrehajtására:

- **az aláíró számára engedélyezni az alkalmazott aláírási szabályzat által megkövetelt aláírási tulajdonságok értékének módosítását.**

Finomítás:

A TSF-nek addig kell az aláírási tulajdonságok módosítását lehetővé tennie, amíg az aláíró egyetértését nem adja az aláírásra.

FDP_IFC.1/Az aláíró tanúsítványának importálása: Részleges információ áramlás ellenőrzés

FDP_IFC.1.1/Az aláíró tanúsítványának importálása

A TSF-nek érvényt kell szereznie az **aláíró tanúsítványa** információ áramlás ellenőrzés szabályzatnak az alábbiakon:

- szubjektum: **az aláíró**
- információ: **az aláíró tanúsítványa**
- művelet: **az aláíró tanúsítványának importálása**

FDP_IFF.1/Az aláíró tanúsítványának importálása: Egyszerű biztonsági attribútumok

FDP_IFF.1.1/Az aláíró tanúsítványának importálása

A TSF-nek érvényt kell szereznie az **aláíró tanúsítványa** információ áramlás ellenőrzés szabályzatnak a szubjektumok és információk alábbi biztonsági tulajdonságain alapulva:

- szubjektum: **az aláíró (az alkalmazott aláírási szabályzat)**
- információ: **az aláíró tanúsítványa (key usage, minősített elektronikus aláírás esetén: QCStatement)**.

FDP_IFF.1.2/Az aláíró tanúsítványának importálása

A TSF-nek a következő szabályok betartása esetén engedélyeznie kell egy ellenőrzött szubjektumok és információk közötti, ellenőrzött műveleten keresztül megvalósuló információ áramlást:

Az aláíró tanúsítványának importálása:

Fokozott biztonságú aláírás esetén:

- **az aláíró kiválasztott tanúsítványában a "key usage" kiterjesztés azt mutatja, hogy ez a tanúsítvány digitális aláírás és/vagy letagadhatatlansági célokból használható.**

Minősített elektonikus aláírás esetén:

- **az aláíró kiválasztott tanúsítványában a "key usage" kiterjesztés azt mutatja, hogy ez a tanúsítvány letagadhatatlansági célból használható,**
- **a tanúsítvány egy minősített tanúsítvány (QCStatement kiterjesztés szerepel a tanúsítványban),**

FDP_IFF.1.3/Az aláíró tanúsítványának importálása

A TSF-nek érvényt kell szereznie az **aláírási szabályzat által közvetlenül meghatározott egyéb szabályoknak**.

FDP_IFF.1.4/Az aláíró tanúsítványának importálása

A TSF-nek közvetlenül engedélyeznie kell az információ áramlást az alábbi szabályokon alapulva:

- **az ellenőrzések sikeresek voltak.**

FDP_IFF.1.5/Az aláíró tanúsítványának importálása

A TSF-nek közvetlenül vissza kell utasítania az információ áramlást az alábbi szabályokon alapulva:

- **az ellenőrzések sikertelenek voltak.**

FMT_MSA.3/Az aláíró tanúsítványának importálása: Statikus tulajdonságok kezdeti értékadása

FMT_MSA.3.1/Az aláíró tanúsítványának importálása

A TSF-nek érvényt kell szereznie az **aláíró tanúsítványa** információ áramlás ellenőrzés szabálynak, **korlátozó** alapértékek biztosításával az SFP-t érvényre juttató biztonsági tulajdonságokra.

FMT_MSA.3.2/Az aláíró tanúsítványának importálása [Szerkesztői finomítás]

A TSF-nek **senki** számára nem szabad lehetővé tennie, hogy alternatív kezdeti értékeket adhasson meg az alapértelmezett értékek helyett egy objektum vagy információ létrehozásakor.

FMT_MSA.1 Az aláíró tanúsítványa: Biztonsági tulajdonságok kezelése

FMT_MSA.1.1/Az aláíró tanúsítványa

A TSF-nek érvényt kell szereznie az **aláíró tanúsítványa** információ áramlás ellenőrzés szabályzatnak azáltal, hogy az **aláíróra** korlátozza az alábbi biztonsági tulajdonság **kiválasztását**: **tanúsítvány azonosító**.

FDP_ITC.2/Az aláíró tanúsítványa: Felhasználói adatok importálása biztonsági tulajdonságokkal

FDP_ITC.2.1/Az aláíró tanúsítványa

A TSF-nek érvényt kell szereznie az **aláíró tanúsítványa** információ áramlás ellenőrzés szabályzatnak, amikor felhasználói adatokat importál a TOE-n kívülről az SFP ellenőrzése alatt.

FDP_ITC.2.2/Az aláíró tanúsítványa

A TSF-nek használnia kell az importált felhasználói adatokhoz kapcsolódó biztonsági tulajdonságokat.

FDP_ITC.2.3/Az aláíró tanúsítványa

A TSF-nek garantálnia kell, hogy az alkalmazott protokoll egyértelmű összerendelést biztosít a fogadott felhasználói adatok és a biztonsági tulajdonságok között.

FDP_ITC.2.4/Az aláíró tanúsítványa

A TSF-nek garantálnia kell, hogy az importált felhasználói adatok biztonsági tulajdonságait a felhasználói adat forrás szándékának megfelelően értelmezik.

FDP_ITC.2.5/Az aláíró tanúsítványa

A TSF-nek érvényt kell szereznie a következő szabályoknak, amikor a TOE-n kívülről, az SFP ellenőrzése alatt felhasználói adatokat importál: **nincs további importálás ellenőrzési szabály.**

FPT_TDC.1/Az aláíró tanúsítványa: TSF-ek közötti alapszintű TSF adat konzisztencia

FPT_TDC.1.1/Az aláíró tanúsítványa

A TSF-nek képesnek kell lennie a TSF és más megbízható IT termékek között megosztott **tanúsítványok** konzisztens értelmezésére.

FPT_TDC.1.2/Az aláíró tanúsítványa

A TSF-nek a következő értelmezési szabályokat kell alkalmaznia amikor egy másik megbízható IT terméktől kapott TSF adatot értelmez:

Fokozott biztonságú elektronikus aláírások esetén:

- **az aláíró tanúsítványát kibocsájtó hitelesítés-szolgáltató értelmezése**
- **az aláírói tanúsítvány érvényességi időtartamának értelmezése**
- **a kulcshasználat (Key usage) kiterjesztés értelmezése**
- **az aláírói tanúsítványba foglalt megkülönböztető név (DN) értelmezése**

Minősített elektronikus aláírások esetén:

- **az aláíró tanúsítványát kibocsájtó hitelesítés-szolgáltató értelmezése**
- **az aláírói tanúsítvány érvényességi időtartamának értelmezése**
- **a kulcshasználat (Key usage) kiterjesztés értelmezése**
- **az aláírói tanúsítványba foglalt megkülönböztető név (DN) értelmezése**
- **a minősített aláírást jelző kiterjesztés (QCStatement) értelmezése.**

FMT_SMF.1/Az aláíró tanúsítványának kiválasztása: Menedzsment funkciók megadása

FMT_SMF.1.1/Az aláíró tanúsítványának kiválasztása

A TSF-nek képesnek kell lennie a következő biztonsági menedzsment funkciók végrehajtására:

- **lehetővé tenni az aláíró számára egy tanúsítványt kiválasztani az alkalmazandó aláírási szabályzathoz alkalmas tanúsítványok közül.**

6.1.1.4 Az aláírási szabályzat alkalmazása és az aláírás létrehozása

FDP_IFC.1/Aláírás létrehozás: Részleges információ áramlás ellenőrzés

FDP_IFC.1.1/Aláírás létrehozás

A TSF-nek érvényt kell szereznie az **aláírás létrehozás** információ áramlás ellenőrzés szabályzatnak az alábbiakon:

- szubjektumok:
  - **az aláíró,**
  - **az SCDev (minősített elektronikus aláírás esetén SSCD)**
- információk:
  - **a formattált DTBS,**
  - **(a létrejövő) elektronikus aláírás**
- műveletek
  - **a formattált DTBS továbbítása az SSCD/SCDev-nek,**
  - **elektronikus aláírás létrehozás.**

FDP_IFF.1/Aláírás létrehozás: Egyszerű biztonsági attribútumok

FDP_IFF.1.1/Aláírás létrehozás

A TSF-nek érvényt kell szereznie az **aláírás létrehozás** információ áramlás ellenőrzés szabályzatnak a szubjektumok és információk alábbi biztonsági tulajdonságain alapulva:

- szubjektumok:
  - **az aláíró (alkalmazott aláírási szabályzat, az aláíró tanúsítványa, az aláíró közvetlen egyetértése egy megjelenített, nem stabil dokumentum aláírására),**

  - **az SCDev (minősített elektonikus aláírás esetén SSCD)**
- információk:
  - **a formattált DTBS (a DTBS formátuma),**
  - **az elektronikus aláírás (állított szerepkör, az aláírás állított dátuma és időpontja, az aláírás állított helye).**

FDP_IFF.1.2/Aláírás létrehozás

A TSF-nek a következő szabályok betartása esetén engedélyeznie kell egy ellenőrzött szubjektumok és információk közötti, ellenőrzött műveleten keresztül megvalósuló információ áramlást:

A formattált DTBS továbbítása:

- **az aláíró tájékoztatása az aláírási tulajdonságokról még az aláírás létrehozása előtt**
- **a dokumentum formátumának megfelelő megjelenítő elindítása a dokumentum formátum/megjelenítő összerendelés tábla alapján**
- **az aláíró kiválasztott tanúsítványának megfelelő aláíró kulcs aktivizálása.**

FDP_IFF.1.3/Aláírás létrehozás

A TSF-nek érvényt kell szereznie az alábbi szabályoknak: **nincs**.

FDP_IFF.1.4/Aláírás létrehozás

A TSF-nek közvetlenül engedélyeznie kell az információ áramlást az alábbi szabályokon alapulva: **nincs**

FDP_IFF.1.5/Aláírás létrehozás

A TSF-nek közvetlenül vissza kell utasítania az információ áramlást az alábbi szabályokon alapulva: **nincs**

FMT_MSA.3/Aláírás létrehozás: Statikus tulajdonságok kezdeti értékadása

FMT_MSA.3.1/Aláírás létrehozás

A TSF-nek érvényt kell szereznie az **aláírás létrehozás** információ áramlás ellenőrzés szabálynak, **korlátozó** alapértékek biztosításával az SFP-t érvényre juttató biztonsági tulajdonságokra.

FMT_MSA.3.2/Aláírás létrehozás [Szerkesztői finomítás]

A TSF-nek **senki** számára nem szabad lehetővé tennie, hogy alternatív kezdeti értékeket adhasson meg az alapértelmezett értékek helyett egy objektum vagy információ létrehozásakor.

FDP_ITC.1/Az aláíró közvetlen egyetértése: Felhasználói adatok importálása biztonsági tulajdonságok nélkül

FDP_ITC.1.1/Az aláíró közvetlen egyetértése

A TSF-nek érvényt kell szereznie az **aláírás létrehozás** információ áramlás ellenőrzés szabályzatnak, amikor felhasználói adatokat importál a TOE-n kívülről az SFP ellenőrzése alatt.

FDP_ITC.1.2/Az aláíró közvetlen egyetértése

A TSF-nek figyelmen kívül kell hagynia a TOE-n kívülről importált felhasználói adatokhoz kapcsolódó biztonsági tulajdonságokat.

FDP_ITC.1.3/Az aláíró közvetlen egyetértése

A TSF-nek érvényt kell szereznie a következő szabályoknak, amikor az SFP által ellenőrzött felhasználói adatokat importál a TOE-n kívülről: **az aláírónak közvetlenül engedélyeznie kell az aláírást**

6.1.1.5 Elektronikus aláírás exportálása

FDP_IFC.1/Elektronikus aláírás exportálása: Részleges információ áramlás ellenőrzés

FDP_IFC.1.1/Elektronikus aláírás exportálása

A TSF-nek érvényt kell szereznie az **elektronikus aláírás exportálása** információ áramlás ellenőrzés szabályzatnak az alábbiakon:

- szubjektumok:
  - **az aláíró,**
  - **az SCDev**
- információ: **az elektronikus aláírás**
- művelet: **az elektronikus aláírás exportálása az aláíróhoz**

FDP_IFF.1/Elektronikus aláírás exportálása: Egyszerű biztonsági tulajdonságok

FDP_IFF.1.1/Elektronikus aláírás exportálása

A TSF-nek érvényt kell szereznie az **elektronikus aláírás exportálása** információ áramlás ellenőrzés szabályzatnak a szubjektumok és információk alábbi biztonsági tulajdonságain alapulva:

- szubjektumok:
  - **az aláíró**
  - **az SCDev (az aláírás létrehozás folyamatának állapota)**
- információ:
  - **az elektronikus aláírás (a létrehozott elektronikus aláírás, az aláírt dokumentum hash értéke, az aláíró tanúsítványa, az aláírás dátuma és időpontja, az aláírt dokumentum tartalom-formátuma, beállított „szerepkör” aláírási tulajdonság, beállított „aláírás helye” aláírási tulajdonság).**

FDP_IFF.1.2/Elektronikus aláírás exportálása

A TSF-nek a következő szabályok betartása esetén engedélyeznie kell egy ellenőrzött szubjektumok és információk közötti, ellenőrzött műveleten keresztül megvalósuló információ áramlást:

Az elektronikus aláírás exportálása az aláírónak, amennyiben az (SCDev által végrehajtott) aláírás létrehozás sikeres volt.

FDP_IFF.1.3/Elektronikus aláírás exportálása

A TSF-nek érvényt kell szereznie az alábbi egyéb szabálynak: **az aláírásnak a beállított „XAdES formátum”-ra történő formattálása.**

FDP_IFF.1.4/Elektronikus aláírás exportálása

A TSF-nek közvetlenül engedélyeznie kell az információ áramlást az alábbi szabályon alapulva: **nincs**

FDP_IFF.1.5/Elektronikus aláírás exportálása

A TSF-nek közvetlenül vissza kell utasítania az információ áramlást az alábbi szabályokon alapulva:

- **az aláírás létrehozás sikertelen volt.**

FDP_ETC.2/Elektronikus aláírás exportálása: A felhasználói adatok exportálása biztonsági tulajdonságokkal

FDP_ETC.2.1/Elektronikus aláírás exportálása

A TSF-nek érvényt kell szereznie az **elektronikus aláírás exportálása** információ áramlás ellenőrzés szabályzatnak, amikor az SFP-k által ellenőrzött felhasználói adatokat exportál a TOE-n kívülre.

FDP_ETC.2.2/Elektronikus aláírás exportálása

A TSF-nek a felhasználói adatokat az ezekhez kapcsolódó biztonsági tulajdonságokkal együtt kell exportálnia.

FDP_ETC.2.3/Elektronikus aláírás exportálása

A TSF-nek garantálnia kell, hogy a TOE-n kívülre exportálás esetén a biztonsági tulajdonságok egyértelműen összekapcsolódjanak az exportált felhasználói adatokkal.

FDP_ETC.2.4/Elektronikus aláírás exportálása

A TSF-nek érvényt kell szereznie a következő szabályoknak, amikor felhasználói adatokat exportál a TOE-n kívülre: **nincs.**

FMT_MSA.3/Elektronikus aláírás exportálása: Statikus tulajdonságok kezdeti értékadása

FMT_MSA.3.1/Elektronikus aláírás exportálása

A TSF-nek érvényt kell szereznie az **elektronikus aláírás exportálása** információ áramlás ellenőrzés szabálynak, **korlátozó** alapértékek biztosításával az SFP-t érvényre juttató biztonsági tulajdonságokra.

FMT_MSA.3.2/Elektronikus aláírás exportálása [Szerkesztői finomítás]

A TSF-nek **senki** számára nem szabad lehetővé tennie, hogy alternatív kezdeti értékeket adhasson meg az alapértelmezett értékek helyett egy objektum vagy információ létrehozásakor.

FMT_MSA.1/Az SCDev aláírás létrehozás állapota: Biztonsági tulajdonságok kezelése

FMT_MSA.1.1/Az SCDev aláírás létrehozás állapota

A TSF-nek érvényt kell szereznie az **elektronikus aláírás importálás** információ áramlás ellenőrzés szabályzatnak azáltal, hogy **senkire** korlátozza az alábbi biztonsági tulajdonság **módosítását**: **az SCDev aláírás létrehozás állapota**

FMT_SMF.1/Az SCDev aláírás létrehozás állapotának lekérdezése: Menedzsment funkciók megadása

FMT_SMF.1.1/Az SCDev aláírás létrehozás állapotának lekérdezése

A TSF-nek képesnek kell lennie a következő biztonsági menedzsment funkció végrehajtására:

- **az SCDev aláírás létrehozás állapotának lekérdezése (megkülönböztetve az aláírás létrehozás sikeres befejeződését és a sikertelen lezárását).**

6.1.1.6 Kriptográfiai műveletek

FCS_COP.1/Hash függvény: Kriptográfiai művelet

FCS_COP.1.1/Hash függvény

A TSF-nek végre kell hajtania a **hash képzést** az alábbiak alapján:

- kriptográfiai algoritmusok: **SHA1, SHA256**
- kulcsméretek: **nem alkalmazható**
- szabványok: **[FIPS PUB 180-3].**

Finomítás:

A kulcsméret fogalma nem alkalmazható a hash függvények esetében.

6.1.1.7 Biztonsági szerepkörök

FMT_SMR.1 Biztonsági szerepkörök

FMT_SMR.1.1

A TSF-nek kezelnie kell az alábbi szerepköröket:

- **aláíró (E-Magic)**
- **ellenőrző (E-Magic)**
- **hívó alkalmazás (XadesMagic).**

FMT SMR.1.2

A TSF-nek össze kell kapcsolnia a felhasználókat a szerepkörökkel.

6.1.1.8 A TOE adminisztrálása

FMT_MTD.1/Dokumentum formátum/megjelenítő összerendelés tábla: TSF adatok kezelése

FMT_MTD.1.1/Dokumentum formátum/megjelenítő összerendelés tábla:

A TSF-nek az **aláíróra** kell korlátoznia a **dokumentum formátum/ megjelenítő összerendelés tábla módosítását**.

FMT_SMF.1/Dokumentum formátum/megjelenítő összerendelés tábla: Menedzsment funkciók megadása

FMT_SMF.1.1/Dokumentum formátum/megjelenítő összerendelő tábla

A TSF-nek képesnek kell lennie a következő biztonsági menedzsment funkció végrehajtására:

Az aláíró számára lehetővé tenni a dokumentum formátum/ megjelenítő összerendelő tábla alábbi kezelését:

- **az alapértelmezett 2 összerendelés (.txt/saját megjelenítő, .xml/C:\Program Files\Internet Explorer\iexplore.exe) mellé új formátum/megjelenítő pár hozzáadása,**
- **meglévő formátum/megjelenítő pár törlése.**

FMT_MTD.1/ Az aláírási szabályzatok kezelése: TSF adatok kezelése

FMT_MTD.1. 1/ Az aláírási szabályzatok kezelése

A TSF-nek az **aláíróra** kell korlátoznia az **aláírási szabályzat alábbi beállításait:**

- **aláírás helye (város, megye, ország, irányítószám)**
- **szerepkör**
- **Xades típus (Xades-EPES vagy Xades–T)**
- **aláíró algoritmus (RSA-SHA1 vagy RSA-SHA256)**
- **lenyomatképző algoritmus (SHA1 vagy SHA256)**
- **aláírás fajtája (Fokozott vagy Minősített)**
- **időbélyeg szolgáltató kiválasztása**
- **aláírás előtti időbélyeg használatának beállítása**
- **megtekinthető és aláírható típusok (dokumentum formátum/ megjelenítő alkalmazás lista)**
- **aláírás típusa (Elektronikus adat aláírása vagy Közjegyzői aláírás)**

FMT_SMF.1/Az aláírási szabályzatok kezelése: Menedzsment funkciók megadása

FMT_SMF.1.1/Az aláírási szabályzatok kezelése

A TSF-nek képesnek kell lennie a következő biztonsági menedzsment funkció végrehajtására:

- **aláírás helyének beállítása**
- **szerepkör meghatározása**
- **Xades típus kiválasztása**
- **aláíró algoritmus kiválasztása**
- **lenyomatképző algoritmus kiválasztása**
- **aláírás fajta kiválasztása**
- **időbélyeg szolgáltató kiválasztása**
- **aláírás előtti időbélyeg használatának beállítása**
- **megtekinthető és aláírható típusok meghatározása**
- **aláírás típus kiválasztása**

6.1.2 Az aláírás ellenőrzésére vonatkozó funkcionális biztonsági követelmények

A 6.2 táblázat felsorolja a funkcionális biztonsági követelményekben szereplő szubjektumokat, objektumokat, műveleteket és ezek biztonsági tulajdonságait.

Szubjek-tum	objektum/ információ	művelet	biztonsági tulajdonság
ellenőrző	aláírt dokumentum	a dokumentum importálása	**ellenőrző:** - aláírási szabályzat **aláírt dokumentum:** - a dokumentum stabilitás állapota
ellenőrző	elektronikus aláírás	az elektronikus aláírás aláíróhoz exportálása	**ellenőrző:** - az alkalmazott aláírási szabályzat **az elektronikus aláírás:** - állított szerepkör - az aláírás feltételezett dátuma és időpontja - az aláírás feltételezett helye **aláírt dokumentum:** - dokumentum-formátum
ellenőrző	az aláírásra alkalmazott idő hivatkozás	az idő hivatkozás importálása	**ellenőrző:** - az alkalmazott aláírási szabályzat **az aláíró aláírásához alkalmazott elektronikus aláírás:** - az időbélyeg tokenek ellenőrzéséhez alkalmazandó megbízható pont (gyökér tanúsítvány) - az időbélyeg-szolgáltató tanúsítványa - a tanúsítvány és a gyökér tanúsítvány között lévő egyéb szükséges tanúsítványok
ellenőrző	a tanúsítvány-lánchoz tartozó tanúsítványok, a tanúsítvány-lánc ellenőrzéséhez szükséges visszavonási adatok	a tanúsítványok és a visszavonási adatok importálása	**ellenőrző:** - az alkalmazott aláírási szabályzat **a tanúsítvány-lánchoz tartozó tanúsítványok:** - kulcshasználat (key usage) - QCStatement (minősített aláírás esetén) - elektronikus aláírás állapot (érvényes/érvénytelen) - a tanúsítvány érvényességi periódusa - idő hivatkozás
ellenőrző	ellenőrzési állapot (érvényes)	az ellenőrzési állapot átadása az ellenőrzőnek	**ellenőrzési állapot:** - az aláíró nyilvános kulcsa - a dokumentum lenyomata - a dokumentum elektronikus aláírása

6.2. táblázat: a funkcionális biztonsági követelményekben szereplő szubjektumok, objektumok, műveleteket és ezek biztonsági tulajdonságai

6.1.2.1 Ellenőrzés a dokumentum importálása során

FDP_IFC.1/Dokumentum elfogadás: Részleges információ áramlás ellenőrzés

FDP_IFC.1.1/Dokumentum elfogadás

A TSF-nek érvényt kell szereznie a **dokumentum elfogadás** információ áramlás ellenőrzés szabályzatnak az alábbiakon:

- szubjektum: **az ellenőrző**
- információ: **az aláírt dokumentum**
- művelet: **a dokumentum importálása**

FDP_IFF.1/Dokumentum elfogadás: Egyszerű biztonsági attribútumok

FDP_IFF.1.1/Dokumentum elfogadás

A TSF-nek érvényt kell szereznie a **dokumentum elfogadás** információ áramlás ellenőrzés szabályzatnak a szubjektumok és információk alábbi biztonsági tulajdonságain alapulva:

- szubjektum: **az ellenőrző (aláírási szabályzat)**
- információ: **az aláírt dokumentum (a dokumentum stabilitás állapota)**

FDP_IFF.1.2/Dokumentum elfogadás

A TSF-nek a következő szabályok betartása esetén engedélyeznie kell egy ellenőrzött szubjektumok és információk közötti, ellenőrzött műveleten keresztül megvalósuló információ áramlást:

A dokumentum importálása

- **vagy a dokumentum stabilitás állapota: "stabil",**
- **vagy a dokumentum stabilitás állapota: "nem stabil" vagy "nem ellenőrizhető", de az aláírási szabályzat megengedi ennek az ellenőrzésnek a megkerülését, és az aláíró közvetlenül egyetértett az ellenőrzés megkerülésével.**

Az ellenőrzőt csak abban az esetben kell tájékoztatni, ha a dokumentum szemantikája nem stabil.

FDP_IFF.1.3/Dokumentum elfogadás

A TSF-nek érvényt kell szereznie az alábbiaknak: **nincs**

FDP_IFF.1.4/Dokumentum elfogadás

A TSF-nek közvetlenül engedélyeznie kell az információ áramlást az alábbi szabályokon alapulva:

- **sikeres ellenőrzések, vagy**
- **megkerült ellenőrzések.**

FDP_IFF.1.5/Dokumentum elfogadás

A TSF-nek közvetlenül vissza kell utasítania az információ áramlást az alábbi szabályokon alapulva:

- **sikertelen ellenőrzések, és**
- **az ellenőrzéseket nem lehet megkerülni.**

Alkalmazási megjegyzés:

A TOE-nak biztosítania kell az alábbiakat:

- egy külső modul végrehajtása, mely ellenőrzi, hogy az aláírandó dokumentum szemantikája stabil,
- az aláíró figyelmeztetése, ha a dokumentum szemantikája nem stabil.

FDP_ITC.1/Dokumentum elfogadás: Felhasználói adatok importálása biztonsági tulajdonságok nélkül

FDP_ITC.1.1/Dokumentum elfogadás

A TSF-nek érvényre kell juttatnia a **dokumentum elfogadás** információ áramlás ellenőrzési szabályt az SFP-k által felügyelt felhasználói adatok TOE-n kívülről történő importálása során.

FDP_ITC.1.2/Dokumentum elfogadás

A TSF-nek figyelmen kívül kell hagynia az importált felhasználói adatokhoz kapcsolódó biztonsági tulajdonságokat a TOE-n kívülről történő importálás során.

FDP_ITC.1.3/Dokumentum elfogadás

A TSF-nek érvényre kell juttatnia az alábbi szabályt amikor az SFP ellenőrzése alatt a TOE-n kívülről felhasználói adatot importál:

- **meg kell állapítani a dokumentum szemantikáját („stabil”, „nem stabil”).**

Finomítás:
Az E-Magic automatikusan stabilnak tekinti a .txt és .xml kiterjesztésű dokumentumokat, az egyéb dokumentumokat pedig automatikusan nem stabilnak.

FMT_MSA.3/Dokumentum elfogadás: Statikus tulajdonságok kezdeti értékadása

FMT_MSA.3.1/Dokumentum elfogadás

A TSF-nek érvényre kell juttatnia a **dokumentum elfogadás** információ áramlás ellenőrzési szabályt azzal, hogy **korlátozó** alapértékeket ad az SFP-t megvalósító biztonsági tulajdonságoknak.

FMT_MSA.3.2/Dokumentum elfogadás [Szerkesztői finomítás]

A TSF-nek **senki** számára sem szabad lehetővé tennie az alapértékek alternatív kezdeti értékekkel való felülírását egy objektum vagy információ létrehozásakor.

Finomítás:
Az E-Magic alapértelmezett elvárása egy nem stabil dokumentumra az ellenőrző figyelmeztetése.

FMT_MSA.1/Dokumentum szemantika stabil állapota: Biztonsági tulajdonságok kezelése

FMT_MSA.1.1/A dokumentum stabilitás állapota [Szerkesztői finomítás]

A TSF-nek érvényt kell szereznie a **dokumentum elfogadás** információ áramlás ellenőrzés szabályzatnak azzal, hogy **senki** számára nem teszi lehetővé a **dokumentum stabilitás állapota** biztonsági tulajdonság **módosítását.**

FMT_SMF.1/A dokumentum stabilitás állapot meghatározása: Menedzsment funkciók megadása

FMT_SMF.1.1/A dokumentum stabilitás állapot meghatározása

A TSF-nek képesnek kell lennie a következő biztonsági menedzsment funkció végrehajtására:

- **a dokumentum szemantika stabilitási állapotának meghatározása (stabil vagy nem stabil).**

6.1.2.2 Aláírási szabályzatok

FMT_SMF.1/Az alkalmazandó aláírási szabályzat kiválasztása: Menedzsment funkciók megadása

FMT_SMF.1.1/Az alkalmazandó aláírási szabályzat kiválasztása

A TSF-nek képesnek kell lennie a következő biztonsági menedzsment funkció végrehajtására:

- **az alkalmazott aláírási szabályzat kiválasztása.**

FMT_MTD.1/Az alkalmazandó aláírási szabályzat kiválasztása: TSF adatok kezelése

FMT_MTD.1.1/Az alkalmazandó aláírási szabályzat kiválasztása

A TSF-nek az **ellenőrzőre** kell korlátoznia az **alkalmazandó aláírási szabályzat kiválasztását**.

6.1.2.3 Az aláírás ellenőrzése

A következő követelmények a dokumentum aláírásának ellenőrzési folyamatára vonatkoznak.

6.1.2.3.1 Az elektronikus aláírás és aláírási tulajdonságok importálása

A következő követelmények az elektronikus aláírás és az aláírási tulajdonságok importálására vonatkoznak.

FDP_IFC.1/Elektronikus aláírás: Részleges információ áramlás ellenőrzés

FDP_IFC.1.1/Elektronikus aláírás

A TSF-nek érvényt kell szereznie az **elektronikus aláírás** információ áramlás ellenőrzés szabályzatnak az alábbiakon:

- szubjektum: **az ellenőrző**
- információ: **az elektronikus aláírás (az elektronikus aláírás és a kapcsolódó aláírási tulajdonságok, az aláírt dokumentum)**
- művelet: **az elektronikus aláírás importálása (annak elfogadása, hogy az aláírási tulajdonságok megfelelnek az aláírási szabályzatnak)**

FDP_IFF.1/Elektronikus aláírás: Egyszerű biztonsági attribútumok

FDP_IFF.1.1/Elektronikus aláírás

A TSF-nek érvényt kell szereznie az **elektronikus aláírás** információ áramlás ellenőrzés szabályzatnak a szubjektumok és információk alábbi biztonsági tulajdonságain alapulva:

- szubjektum: **az ellenőrző (alkalmazott aláírási szabályzat)**
- információk:
    - **az elektronikus aláírás (az elektronikus aláírás, az aláíró tanúsítványa, az aláírás létrehozás állított dátuma és időpontja, állított szerepkör, az aláírás állított helye),**
    - **aláírt dokumentum (dokumentum-formátum, az aláírt dokumentum hash értéke).**

FDP_IFF.1.2/Elektronikus aláírás

A TSF-nek a következő szabályok betartása esetén engedélyeznie kell egy ellenőrzött szubjektumok és információk közötti, ellenőrzött műveleten keresztül megvalósuló információ áramlást:

Aláírás importálás

- **meg kell hívni a dokumentum formátumának megfelelő megjelenítőt, a dokumentum formátum/megjelenítő összerendelés tábla alapján.**

FDP_IFF.1.3/Elektronikus aláírás

A TSF-nek érvényt kell szereznie **az aláírás SFP-ben közvetlenül meghatározott további szabályoknak**.

FDP_IFF.1.4/Elektronikus aláírás

A TSF-nek közvetlenül engedélyeznie kell az információ áramlást az alábbi szabályokon alapulva:

- **az aláírási tulajdonságok megfelelnek az aláírás SFP-nek,**

- **és az aláírt dokumentum stabil.**

FDP_IFF.1.5/Elektronikus aláírás

A TSF-nek közvetlenül vissza kell utasítania az információ áramlást az alábbi szabályokon alapulva:

- **az aláírási tulajdonságok nem felelnek meg az aláírás SFP-nek, vagy az aláírt dokumentum nem stabil**.

FMT_MSA.3/Elektronikus aláírás: Statikus tulajdonságok kezdeti értékadása

FMT_MSA.3.1/Elektronikus aláírás

A TSF-nek érvényt kell szereznie az **elektronikus aláírás** információ áramlás ellenőrzés szabálynak, **korlátozó** alapértékek biztosításával az SFP-t érvényre juttató biztonsági tulajdonságokra.

FMT_MSA.3.2/Elektronikus aláírás [Szerkesztői finomítás]

A TSF-nek senki számára nem szabad lehetővé tennie, hogy alternatív kezdeti értékeket adhasson meg az alapértelmezett értékek helyett egy objektum vagy információ létrehozásakor.

FMT_MSA.1/Elektronikus aláírás: Biztonsági tulajdonságok kezelése

FMT_MSA.1.1/Elektronikus aláírás

A TSF-nek érvényt kell szereznie az **elektronikus aláírás** információ áramlás ellenőrzés szabályzatnak azáltal, hogy **senkire** korlátozza az alábbi biztonsági tulajdonságok **módosítását**: **az aláírás és annak aláírási tulajdonságai**

FDP_ITC.2/Elektronikus aláírás: Felhasználói adatok importálása biztonsági tulajdonságokkal

FDP_ITC.2.1/Elektronikus aláírás

A TSF-nek érvényt kell szereznie az **elektronikus aláírás** információ áramlás ellenőrzés szabályzatnak, amikor felhasználói adatokat importál a TOE-n kívülről az SFP ellenőrzése alatt.

FDP_ITC.2.2/Elektronikus aláírás

A TSF-nek használnia kell az importált felhasználói adatokhoz kapcsolódó biztonsági tulajdonságokat.

FDP_ITC.2.3/Elektronikus aláírás

A TSF-nek garantálnia kell, hogy az alkalmazott protokoll egyértelmű összerendelést biztosít a fogadott felhasználói adatok és a biztonsági tulajdonságok között.

FDP_ITC.2.4/Elektronikus aláírás

A TSF-nek garantálnia kell, hogy az importált felhasználói adatok biztonsági tulajdonságait a felhasználói adat forrás szándékának megfelelően értelmezik.

FDP_ITC.2.5/Elektronikus aláírás

A TSF-nek érvényt kell szereznie a következő szabályoknak, amikor a TOE-n kívülről, az SFP ellenőrzése alatt felhasználói adatokat importál:

- a dokumentum szemantika stabilitásának ellenőrzése az aláírt dokumentum elektronikus aláírásba foglalt dokumentum-formátuma alapján,
- az ellenőrzés eredményének továbbítása az ellenőrzőnek.

6.1.2.3.2 Egy érvényes idő hivatkozás importálása

FDP_IFC.1/Idő hivatkozás: Részleges információ áramlás ellenőrzés

FDP_IFC.1.1/Idő hivatkozás

A TSF-nek érvényt kell szereznie az **idő hivatkozás elfogadás** információ áramlás ellenőrzés szabályzatnak az alábbiakon:

- szubjektum: **az ellenőrző**
- információ: **az aláíráshoz alkalmazott idő hivatkozás**
- művelet: **az idő hivatkozás importálása**

FDP_IFF.1/Idő hivatkozás: Egyszerű biztonsági attribútumok

FDP_IFF.1.1/Idő hivatkozás

A TSF-nek érvényt kell szereznie az **idő hivatkozás elfogadás** információ áramlás ellenőrzés szabályzatnak a szubjektumok és információk alábbi biztonsági tulajdonságain alapulva:

- szubjektum: **az ellenőrző (az alkalmazott aláírási szabályzat)**
- információ: **az aláíró elektronikus aláírására alkalmazott idő hivatkozás (az időbélyeg tokenek ellenőrzéséhez alkalmazandó megbízható pont (gyökér tanúsítvány), az időbélyeg-szolgáltató tanúsítványa, a tanúsítvány és a gyökér tanúsítvány között lévő egyéb szükséges tanúsítványok.**

FDP_IFF.1.2/Idő hivatkozás

A TSF-nek a következő szabályok betartása esetén engedélyeznie kell egy ellenőrzött szubjektumok és információk közötti, ellenőrzött műveleten keresztül megvalósuló információ áramlást:

idő hivatkozás elfogadás

- az időbélyeg-szolgáltató tanúsítványában a kulcs használat (key usage) kiterjesztés értéke csak időbélyegzési célt jelöl,
- tanúsítványlánc építhető fel az időbélyeg-szolgáltató tanúsítványa és egy időbélyeg tokenek ellenőrzéséhez alkalmazandó megbízható pont között,
- a fent említett tanúsítványláncra az FDP_IFF.1/Tanúsítványlánc követelményben szereplő összes szabály teljesül az idő hivatkozásban szereplő dátumra és időpontra vonatkozóan.

FDP_IFF.1.3/Idő hivatkozás

A TSF-nek érvényt kell szereznie az alábbiaknak: **nincs.**

FDP_IFF.1.4/Idő hivatkozás

A TSF-nek közvetlenül engedélyeznie kell az információ áramlást az alábbi szabályokon alapulva:

- **sikeres ellenőrzések.**

FDP_IFF.1.5/Idő hivatkozás

A TSF-nek közvetlenül vissza kell utasítania az információ áramlást az alábbi szabályokon alapulva:

- **sikertelen ellenőrzések.**

FMT_MSA.3/Idő hivatkozás: Statikus tulajdonságok kezdeti értékadása

FMT_MSA.3.1/Idő hivatkozás

A TSF-nek érvényt kell szereznie az **idő hivatkozás elfogadás** információ áramlás ellenőrzés szabálynak, **korlátozó** alapértékek biztosításával az SFP-t érvényre juttató biztonsági tulajdonságokra.

FMT_MSA.3.2/Idő hivatkozás [Szerkesztői finomítás]

A TSF-nek **senki** számára sem szabad lehetővé tennie az alapértékek alternatív kezdeti értékekkel való felülírását egy objektum vagy információ létrehozásakor.

FMT_MSA.1/Idő hivatkozás: Biztonsági tulajdonságok kezelése

FMT_MSA.1.1/Idő hivatkozás

A TSF-nek érvényt kell szereznie az **idő hivatkozás elfogadás** információ áramlás ellenőrzés szabályzatnak azáltal, hogy **senkire** korlátozza az alábbi biztonsági tulajdonság **módosítását**: **idő hivatkozás.**

FDP_ITC.2/Idő hivatkozás: Felhasználói adatok importálása biztonsági tulajdonságokkal

FDP_ITC.2.1/Idő hivatkozás

A TSF-nek érvényt kell szereznie az **idő hivatkozás elfogadás** információ áramlás ellenőrzés szabályzatnak, amikor felhasználói adatokat importál a TOE-n kívülről az SFP ellenőrzése alatt.

FDP_ITC.2.2/Idő hivatkozás

A TSF-nek használnia kell az importált felhasználói adatokhoz kapcsolódó biztonsági tulajdonságokat.

FDP_ITC.2.3/Idő hivatkozás

A TSF-nek garantálnia kell, hogy az alkalmazott protokoll egyértelmű összerendelést biztosít a fogadott felhasználói adatok és a biztonsági tulajdonságok között.

FDP_ITC.2.4/Idő hivatkozás

A TSF-nek garantálnia kell, hogy az importált felhasználói adatok biztonsági tulajdonságait a felhasználói adat forrás szándékának megfelelően értelmezik.

FDP_ITC.2.5/Idő hivatkozás

A TSF-nek érvényt kell szereznie a következő szabályoknak, amikor a TOE-n kívülről, az SFP ellenőrzése alatt felhasználói adatokat importál: **nincs**.

6.1.2.3.3 Egy érvényes tanúsítványlánc importálása

A következő követelmények a tanúsítványláncot alkotó tanúsítványok azon ellenőrzési szabályaira vonatkoznak, melyek lehetővé teszik eldönteni, hogy a tanúsítványlánc érvényes vagy nem.

Tanúsítványok

FMT_MSA.1/Tanúsítványok: Biztonsági tulajdonságok kezelése

FMT_MSA.1.1/Tanúsítványok

A TSF-nek érvényt kell szereznie a **tanúsítványlánc elfogadás** információ áramlás ellenőrzés szabályzatnak azáltal, hogy **senkire** korlátozza az alábbi biztonsági tulajdonságok **módosítását**: **az importált tanúsítványok**

A tanúsítványok érvényesítő adatai

FMT_MSA.1/Tanúsítvány érvényesítő adatok: Biztonsági tulajdonságok kezelése

FMT_MSA.1.1/Tanúsítvány érvényesítő adatok

A TSF-nek érvényt kell szereznie a **tanúsítványlánc elfogadás** információ áramlás ellenőrzés szabályzatnak azáltal, hogy **senkire** korlátozza az alábbi biztonsági tulajdonságok **módosítását**: **a tanúsítványok visszavonási adatai.**

Egyebek

FDP_IFC.1/Tanúsítványlánc: Részleges információ áramlás ellenőrzés

FDP_IFC.1.1/Tanúsítványlánc

A TSF-nek érvényt kell szereznie a **tanúsítványlánc elfogadás** információ áramlás ellenőrzés szabályzatnak az alábbiakon: szubjektum: **az ellenőrző** információ:

- a tanúsítványlánchoz tartozó tanúsítványok
- a tanúsítványlánc ellenőrzéséhez szükséges visszavonási adatok

- művelet: **az információ importálása (ami a lánc aláírási szabályzat szerinti érvényes tanúsítványláncként való elfogadását jelenti).**

Alkalmazási megjegyzés:
A tanúsítványok és az ezekhez kapcsolódó érvényesítő adatok exportálása azt jelenti, hogy a láncot elfogadták az aláírási szabályzat szerinti érvényes tanúsítványláncként.

FDP_IFF.1/Tanúsítványlánc: Egyszerű biztonsági attribútumok

FDP_IFF.1.1/Tanúsítványlánc

A TSF-nek érvényt kell szereznie a **tanúsítványlánc elfogadás** információ áramlás ellenőrzés szabályzatnak a szubjektumok és információk alábbi biztonsági tulajdonságain alapulva:

- szubjektum: **az ellenőrző (alkalmazott aláírási szabályzat)**
- információ: **tanúsítványlánc érvényesítő adatok, köztük:**
  - **a tanúsítványlánchoz tartozó tanúsítványok (tanúsítvány kiterjesztések: key usage, QCStatement, az elektronikus aláírás állapota, érvényességi periódus, idő hivatkozás),**
  - **a tanúsítványlánc összes tanúsítványára vonatkozó visszavonási adatok).**

FDP_IFF.1.2/Tanúsítványlánc

A TSF-nek a következő szabályok betartása esetén engedélyeznie kell egy ellenőrzött szubjektumok és információk közötti, ellenőrzött műveleten keresztül megvalósuló információ áramlást:

A tanúsítványlánc összetevők és érvényesítő adataik importálása:

- **a tanúsítványlánc összeköti az aláíró tanúsítványát egy az alkalmazott aláírási szabályzat által meghatározott gyökér tanúsítvánnyal.**

A következő szabályoknak teljesülniük kell az importált idő hivatkozásban szereplő dátumra/időpontra.

Tanúsítványlánc:

- **a tanúsítványlánc minden tanúsítványának elektronikus aláírása helyes;**
- **a tanúsítványlánc minden tanúsítványára a tanúsítványba foglalt érvényességi periódus tartalmazza az idő hivatkozásban szereplő dátumot;**
- **minden visszavonási adatra vonatkozó elektronikus aláírás helyes;**
- **a tanúsítványlánc minden tanúsítványára teljesül, hogy a tanúsítvány nincs visszavonva az idő hivatkozásban szereplő időpontban;**
- **a tanúsítványlánc minden tanúsítványára - a végfelhasználói tanúsítvány kivételével - teljesül, hogy a kulcs használat (key usage) kiterjesztés CA tanúsítványt jelez;**

A következő szabályoknak teljesülniük kell az aláíró tanúsítványára:

- **az aláíró tanúsítványában a kulcs használat kiterjesztés jelzi, hogy a tanúsítvány letagadhatatlanság céllal használható (Alkalmazási**

megjegyzés: a keyUsage 1-esre van állítva);

- **minősített elektronikus aláírás esetén a tanúsítvány minősített tanúsítvány (QCStatement kiterjesztés szerepel benne);**

FDP_IFF.1.3/Tanúsítványlánc

A TSF-nek érvényt kell szereznie az alábbiaknak: **nincs.**

FDP_IFF.1.4/Tanúsítványlánc

A TSF-nek közvetlenül engedélyeznie kell az információ áramlást az alábbi szabályokon alapulva:

- **sikeres ellenőrzések.**

FDP_IFF.1.5/Tanúsítványlánc

A TSF-nek közvetlenül vissza kell utasítania az információ áramlást az alábbi szabályokon alapulva:

- **sikertelen ellenőrzések.**

FMT_MSA.3/Tanúsítványlánc: Statikus tulajdonságok kezdeti értékadása

FMT_MSA.3.1/Tanúsítványlánc

A TSF-nek érvényre kell juttatnia a **tanúsítványlánc elfogadás** információ áramlás ellenőrzési szabályt azzal, hogy **korlátozó** alapértékeket ad az SFP-t megvalósító biztonsági tulajdonságoknak.

FMT_MSA.3.2/Tanúsítványlánc [Szerkesztői finomítás]

A TSF-nek **senki** számára sem szabad lehetővé tennie az alapértékek alternatív kezdeti értékekkel való felülírását egy objektum vagy információ létrehozásakor.

FDP_ITC.2/Tanúsítványlánc: Felhasználói adatok importálása biztonsági tulajdonságokkal

FDP_ITC.2.1/Tanúsítványlánc

A TSF-nek érvényt kell szereznie a **tanúsítványlánc elfogadás** információ áramlás ellenőrzés szabályzatnak, amikor felhasználói adatokat importál a TOE-n kívülről az SFP ellenőrzése alatt.

FDP_ITC.2.2/Tanúsítványlánc

A TSF-nek használnia kell az importált felhasználói adatokhoz kapcsolódó biztonsági tulajdonságokat.

FDP_ITC.2.3/Tanúsítványlánc

A TSF-nek garantálnia kell, hogy az alkalmazott protokoll egyértelmű összerendelést biztosít a fogadott felhasználói adatok és a biztonsági tulajdonságok között.

FDP_ITC.2.4/Tanúsítványlánc

A TSF-nek garantálnia kell, hogy az importált felhasználói adatok biztonsági tulajdonságait a felhasználói adat forrás szándékának megfelelően értelmezik.

FDP_ITC.2.5/Tanúsítványlánc

A TSF-nek érvényt kell szereznie a következő szabályoknak, amikor a TOE-n kívülről, az SFP ellenőrzése alatt felhasználói adatokat importál:

- az idő hivatkozás az alkalmazott aláírási szabályzat szerint érvényes (lásd FDP_IFC.1/ Idő hivatkozás);
- a tanúsítvány letagadhatatlanságának ellenőrzéséhez szükséges minden adatot importáltak, az alkalmazott aláírási szabályzatnak megfelelően.

6.1.2.3.4 Az importált adatok értelmezésének képessége

A következő követelmények a TOE importált adatok értelmezési képességére vonatkoznak.

FPT_TDC.1/Elektronikus aláírás: TSF-ek közötti alapszintű TSF adat konzisztencia

FPT_TDC.1.1/Elektronikus aláírás

A TSF-nek képesnek kell lennie a TSF és más megbízható IT termékek között megosztott **elektronikus aláírások** konzisztens értelmezésére.

FPT_TDC.1.2/Elektronikus aláírás

A TSF-nek a következő értelmezési szabályokat kell alkalmaznia, amikor egy másik megbízható IT terméktől kapott TSF adatot értelmez:

- **XAdES-EPES,**
- **XAdES-T,**
- **XAdES-C,**
- **XAdES-X,**
- **XAdES-X-L,**
- **XAdES-A.**

Alkalmazási megjegyzés:
A fent felsorolt elfogadható aláírás formátumok értelmezését lásd [MMM-001].

FPT_TDC.1/Idő hivatkozás: TSF-ek közötti alapszintű TSF adat konzisztencia

FPT_TDC.1.1/Idő hivatkozás

A TSF-nek képesnek kell lennie a TSF és más megbízható IT termékek között megosztott **idő hivatkozások** konzisztens értelmezésére.

FPT_TDC.1.2/Idő hivatkozás

A TSF-nek a következő értelmezési szabályokat kell alkalmaznia, amikor egy másik megbízható IT terméktől kapott TSF adatot értelmez:

- **az [RFC 3161]-ban meghatározott időbélyeg formátumok.**

FPT_TDC.1/Tanúsítványok: TSF-ek közötti alapszintű TSF adat konzisztencia

FPT_TDC.1.1/Tanúsítványok

A TSF-nek képesnek kell lennie a TSF és más megbízható IT termékek között megosztott **tanúsítványok** konzisztens értelmezésére.

FPT_TDC.1.2/Tanúsítványok

A TSF-nek a következő értelmezési szabályokat kell alkalmaznia, amikor egy másik megbízható IT terméktől kapott TSF adatot értelmez:

- **az [RFC 5280]-ben meghatározott tanúsítvány formátumok.**

FPT_TDC.1/Tanúsítvány visszavonási adat: TSF-ek közötti alapszintű TSF adat konzisztencia

FPT_TDC.1.1/Tanúsítvány visszavonási adat

A TSF-nek képesnek kell lennie a TSF és más megbízható IT termékek között megosztott tanúsítvány visszavonási adatok konzisztens értelmezésére.

FPT_TDC.1.2/Tanúsítvány visszavonási adat

A TSF-nek a következő értelmezési szabályokat kell alkalmaznia, amikor egy másik megbízható IT terméktől kapott TSF adatot értelmez:

- **az [RFC 2560]-ben meghatározott OCSP válasz formátumok,**
- **az [RFC 5280]-ben meghatározott CRL formátumok.**

6.1.2.3.5 Az ellenőrzés állapotának visszaadása

FDP_IFC.1/Elektronikus aláírás ellenőrzés: Részleges információ áramlás ellenőrzés

FDP_IFC.1.1/Elektronikus aláírás ellenőrzés

A TSF-nek érvényt kell szereznie az **elektronikus aláírás ellenőrzés** információ áramlás ellenőrzés szabályzatnak az alábbiakon:

- szubjektum: **az ellenőrző**
- információ: **„érvényes aláírás" ellenőrzés állapot**
- művelet: **az állapot továbbítása az ellenőrzőnek.**

FDP_IFF.1/Elektronikus aláírás ellenőrzés: Egyszerű biztonsági attribútumok

FDP_IFF.1.1/Elektronikus aláírás ellenőrzés

A TSF-nek érvényt kell szereznie az **elektronikus aláírás ellenőrzés** információ áramlás ellenőrzés szabályzatnak a szubjektumok és információk alábbi biztonsági tulajdonságain alapulva:

- szubjektum: **az ellenőrző**
- információ: **„érvényes aláírás" ellenőrzés állapot (aláíró nyilvános kulcsa, a dokumentum hash értéke, a dokumentum elektronikus aláírása).**

FDP_IFF.1.2/Elektronikus aláírás ellenőrzés

A TSF-nek a következő szabályok betartása esetén engedélyeznie kell egy ellenőrzött szubjektumok és információk közötti, ellenőrzött műveleten keresztül megvalósuló információ áramlást:

Az ellenőrzés állapot átadása az ellenőrzőnek:

- **létezik egy érvényes tanúsítási útvonal az aláíró tanúsítványa és egy az aláírási szabályzat által hivatkozott megbízható pont között, ezáltal az aláíró nyilvános kulcsa hitelesnek tekinthető;**
- **a dokumentum digitális aláírása helyes, az aláíró nyilvános kulcsát az ellenőrzéshez felhasználva;**
- **az „érvénytelen aláírás" ellenőrzés állapot átadása, ha a fenti szabályok legalább egyike nem teljesül.**

FDP_IFF.1.3/Elektronikus aláírás ellenőrzés

A TSF-nek érvényt kell szereznie az alábbiaknak: **nincs**

FDP_IFF.1.4/Elektronikus aláírás ellenőrzés

A TSF-nek közvetlenül engedélyeznie kell az információ áramlást az alábbi szabályokon alapulva:

- **sikeres ellenőrzések.**

FDP_IFF.1.5/Elektronikus aláírás ellenőrzés

A TSF-nek közvetlenül vissza kell utasítania az információ áramlást az alábbi szabályokon alapulva:

- **sikertelen ellenőrzések.**

FMT_MSA.3/ Aláírás ellenőrzés állapot: Statikus tulajdonságok kezdeti értékadása

FMT_MSA.3.1/Aláírás ellenőrzés állapot

A TSF-nek érvényre kell juttatnia az **elektronikus aláírás ellenőrzés** információ áramlás ellenőrzési szabályt azzal, hogy **korlátozó** alapértékeket ad az SFP-t megvalósító biztonsági tulajdonságoknak.

FMT_MSA.3.2/Aláírás ellenőrzés állapot [Szerkesztői finomítás]

A TSF-nek **senki** számára sem szabad lehetővé tennie az alapértékek alternatív kezdeti értékekkel való felülírását egy objektum vagy információ létrehozásakor.

FMT_MSA.1/Aláírás ellenőrzés állapot: Biztonsági tulajdonságok kezelése

FMT_MSA.1.1/Aláírás ellenőrzés állapot [Szerkesztői finomítás]

A TSF-nek érvényt kell szereznie az **elektronikus aláírás ellenőrzés** információ áramlás ellenőrzés szabályzatnak azzal, hogy **senki** számára nem teszi lehetővé az **aláírás ellenőrzés állapot** biztonsági tulajdonság **módosítását.**

FDP_ETC.2/Ellenőrzési állapot: A felhasználói adatok exportálása biztonsági tulajdonságokkal

FDP_ETC.2.1/Ellenőrzési állapot

A TSF-nek érvényt kell szereznie az **elektronikus aláírás ellenőrzés** információ áramlás ellenőrzés szabályzatnak, amikor az SFP-k által ellenőrzött felhasználói adatokat exportál a TOE-n kívülre.

FDP_ETC.2.2/Ellenőrzési állapot

A TSF-nek a felhasználói adatokat az ezekhez kapcsolódó biztonsági tulajdonságokkal együtt kell exportálnia.

FDP_ETC.2.3/Ellenőrzési állapot

A TSF-nek garantálnia kell, hogy a TOE-n kívülre exportálás esetén a biztonsági tulajdonságok egyértelműen összekapcsolódjanak az exportált felhasználói adatokkal.

FDP_ETC.2.4/Ellenőrzési állapot

A TSF-nek érvényt kell szereznie a következő szabályoknak, amikor felhasználói adatokat exportál a TOE-n kívülre:

- **az ellenőrzési állapot biztonsági tulajdonságaként exportált adatok a következők:**
  - **az ellenőrzési állapot helyességének igazolásához hozzájáruló érvényesítő adatok,**
  - **az aláírási tulajdonságok.**

Alkalmazási megjegyzés:
Az érvényesítő adatok egy utólagos ellenőrzéshez való lehetséges felhasználást szolgálják.
Az aláírási tulajdonságok az ellenőrzőnek kerülnek átadásra egy API-n (XadesMagic) vagy egy MMI-n (E-Magic) keresztül.

6.1.2.4 Kriptográfiai támogatás

FCS_COP.1/Aláírás ellenőrzés: Kriptográfiai művelet

FCS_COP.1.1/Aláírás ellenőrzés

A TSF-nek végre kell hajtania az **elektronikus aláírás ellenőrzést** az alábbiak alapján:

- kriptográfiai algoritmusok: **RSA**
- kulcsméretek: **1024, 2048**
- szabványok: **[PKCS#1]**.

FCS_COP.1/Hash: Kriptográfiai művelet

FCS_COP.1.1/Hash

A TSF-nek végre kell hajtania a **hash képzést** az alábbiak alapján:

- kriptográfiai algoritmusok: **SHA1, SHA256**

- kulcsméretek: **nem alkalmazható**
- szabvány: **[FIPS PUB 180-3].**

Finomítás:
A kulcsméret fogalma nem alkalmazható a hash függvények esetében.

6.1.2.5 Biztonsági szerepkörök

FMT_SMR.1 Biztonsági szerepkörök

FMT_SMR.1.1

A TSF-nek kezelnie kell az alábbi szerepköröket:

- **aláíró (E-Magic)**
- **ellenőrző (E-Magic)**
- **hívó alkalmazás (XadesMagic).**

FMT_SMR.1.2

A TSF-nek össze kell kapcsolnia a felhasználókat a szerepkörökkel.

6.1.2.6 A TOE adminisztrálása

FMT_MTD.1/ Az aláírási szabályzat részleges kezelése: TSF adatok kezelése

FMT_MTD.1. 1/ Az aláírási szabályzat részleges kezelése

A TSF-nek az **ellenőrzőre** kell korlátoznia az aláírási szabályzat alábbi beállításait:

- **kivárási idő figyelembe vételének kikapcsolása**
- **tanúsítványlánc visszavonás ellenőrzési szabály beállítása (teljes aláírói lánc visszavonásának ellenőrzése/csak az aláírói tanúsítvány visszavonásának ellenőrzése)**
- **időbélyeghez tartozó tanúsítványlánc visszavonás ellenőrzési szabály beállítása (teljes időbélyeg aláírói lánc visszavonásának ellenőrzése/csak az időbélyeg aláírói tanúsítvány visszavonásának ellenőrzése/nincs időbélyeg visszavonás ellenőrzés)**
- **OCSP hibakezelési szabály beállítása (hiba esetén CRL használata/hiba esetén folyamat megszakítás)**
- **OCSP szolgáltató kiválasztása (CRL (nincs OCSP)/explicit OCSP szolgáltató/ tanúsítványban szereplő OCSP szolgáltató)**
- **OCSP ellenőrzési szintjének meghatározása (csak végfelhasználói tanúsítványnál/teljes tanúsítvány láncon)**
- **Az ellenőrzéssel elérendő formátum típus meghatározása (Xades-T: az ellenőrzés során időbélyeget helyez el az aláíráson / Xades-C: az ellenőrzés során begyűjti és csatolja az ellenőrzési adatokat / Xades-X-L: az ellenőrzés során a begyűjtött és csatolt ellenőrzési adatokat időbélyeggel védi meg / Xades-A: az ellenőrzés során a teljes elektronikus aláírást archív időbélyeggel védi meg)**

FMT_SMF.1/Az aláírási szabályzat részleges kezelése: Menedzsment funkciók megadása

FMT_SMF.1.1/Az aláírási szabályzatok kezelése

A TSF-nek képesnek kell lennie a következő biztonsági menedzsment funkció végrehajtására:

- **kivárási idő figyelembe vételének kikapcsolása**
- **tanúsítványlánc visszavonás ellenőrzési szabály beállítása**
- **időbélyeghez tartozó tanúsítványlánc visszavonás ellenőrzési szabály**

beállítása

- **OCSP hibakezelési szabály beállítása**
- **OCSP szolgáltató kiválasztása**
- **OCSP ellenőrzési szintjének meghatározása**
- **az ellenőrzéssel elérendő formátum típus meghatározása**

6.2 Garanciális biztonsági követelmények

Osztály	A garanciális biztonsági követelmény (SAR) megnevezése	A SAR összetevő jelölése
Fejlesztés (ALC)	Biztonsági szerkezet leírás	ADV_ARC.1
	Funkcionális specifikáció teljes összegzéssel	ADV_FSP. 3
	Szerkezeti terv	ADV_TDS.2
Útmutató dokumentumok (AGD)	Előkészítő eljárások	AGD_PRE.1
	Üzemeltetési felhasználói útmutató	AGD_OPE.1
Életciklus támogatás (ALC)	Engedélyezéssel kapcsolatos intézkedések	ALC_CMC.3
	A megvalósítási reprezentáció CM lefedettsége	ALC_CMS.3
	Szállítási eljárások	ALC_DEL.1
	A biztonsági intézkedések azonosítása	ALC_DVS.1
	A fejlesztő által meghatározott életciklus modell	ALC_LCD.1
Tesztelés (ATE)	Funkcionális tesztelés	ATE_FUN.1
	A lefedettség vizsgálata	ATE_COV.2
	Az alap terv tesztelése	ATE_DPT.1
	Független tesztelés - minta	ATE_IND.2
Sebezhetőség felmérés (AVA)	Sebezhetőség vizsgálat	AVA_VAN.2

6.3 táblázat: A garanciális biztonsági követelmények

6.3 A funkcionális biztonsági követelmények indoklása

Ez a fejezet a biztonsági szabályzatok, a feltételezések, valamint a TOE és környezeti biztonsági célok vonatkozásában áttekinti, hogy minden szabályzatot lefed-e TOE biztonsági cél, és minden feltételezéshez szerepel-e környezet által teljesítendő biztonsági cél.

6.3.1 Az aláírás létrehozására vonatkozó funkcionális biztonsági követelmények indoklása

6.3.1.1 A biztonsági célok lefedése a funkcionális biztonsági követelményekkel

Általános célok

O.Certificate/Private_Key_Association:
Ezt a biztonsági célt az alábbi követelmény fedi le: ***FDP_IFF.1/Aláírás létrehozás,*** mely megköveteli, hogy a TOE képes legyen aktivizálni az aláíró által kiválasztott tanúsítványhoz tartozó aláíró magánkulcsot.

O.Administration:
Ezt a biztonsági célt az alábbi funkcionális biztonsági követelmények fedik le:

- ***FMT_SMR.1*** megköveteli, hogy a TOE különböztesse meg az aláíró szerepkörét az ellenőrző szerepkörétől.
- ***FMT_MTD.1/Dokumentum formátum/megjelenítő összerendelés tábla*** és ***FMT_SMF.1/A dokumentum formátum/megjelenítő összerendelés tábla kezelése***, melyek lehetővé teszik az aláíró számára (és csak az ő számára), hogy módosítsa a dokumentum formátumokat és a megjelenítő alkalmazásokat összerendelő táblát.
- ***FMT_SMF.1/Az aláírási szabályzatok kezelése***, mely meghatározza az aláírási szabályzatok kezelésének műveleteit, valamint ***FMT_MTD.1/Az aláírási szabályzatok kezelése***, mely ezek használatát az aláíróra korlátozza.

Az aláíróval való köcsönhatásra vonatkozó célok

O.Signature_Attributes_Presentation:
Ezt a biztonsági célt az alábbi követelmény fedi le: ***FDP_IFF.1/Aláírás létrehozás,*** mely megköveteli, hogy a TOE képes legyen megjeleníteni az aláírási tulajdonságokat az aláírási folyamat megkezdése előtt.

O.Explicit_Agreement:
Ezt a biztonsági célt az alábbi követelmény fedi le: ***FDP_ITC.1/Az aláíró közvetlen egyetértése,*** mely nem nyilvánvaló műveletek sikeres végrehajtását követeli meg az aláírással való egyetértési szándék kifejezésére.

O.Signature_Process_Interruption:
Ezt a biztonsági célt az alábbi követelmény fedi le: ***FDP_ROL.2/Az aláírási folyamat megszakítása,*** mely biztosítja, hogy az aláíró lemondhatja az aláírást, mielőtt az SCDev-nek továbbítja az adatokat.

O. Documents_To_Be_Signed:
Ezt a biztonsági célt az alábbi funkcionális biztonsági követelmények fedik le:

- ***FMT_MSA.1/Kiválasztott dokumentumok***, mely az aláíróra korlátozza az aláírandó dokumerntumok kiválasztásának lehetőségét.
- ***FMT_SMF.1/Egy dokumentum lista kiválasztása***, mely megköveteli, hogy a TOE tegye lehetővé az aláírandó dokumentumok kiválasztását mindaddig, amíg az aláíró nem fejezi ki aláírásra vonatkozó egyetértését.
- ***FMT_MSA.1/Aláírási tulajdonságok***, mely az aláíróra korlátozza az aláírási tulajdonságok kiválasztásának lehetőségét.
- ***FMT_SMF.1/Az aláírási tulajdonságok módosítása***, mely megköveteli, hogy a TOE tegye lehetővé az aláírási tulajdonságok értékének módosítását mindaddig, amíg az aláíró nem fejezi ki aláírásra vonatkozó egyetértését.

A fentiek következményeképp az összes kiválasztott dokumentumra ugyanazok az aláírási tulajdonságok kerülnek alkalmazásra.

Az aláírási szabályzat alkalmazására vonatkozó célok

O.Signatory_Certificate_Conformity:
Ennek a biztonsági célnak a lefedése az alábbi módon történik:

- A TOE-nak a tanúsítvány importálása során alkalmaznia kell egy információ áramlás ellenőrzés szabályzatot: ***FDP_IFC.1/Az aláíró tanúsítványának importálása.*** Az ***FDP_IFF.1/Az aláíró tanúsítványának importálása*** funkcionális biztonsági követelmény csak akkor engedi meg a tanúsítvány TOE-ba importálását, ha az aláírási szabályzatban meghatározott, az aláíró tanúsítványára vonatkozó szabályok teljesülnek. A kiválasztott tanúsítvány megfelelősége akkor garantált, ha annak tulajdonságai teljesítik az aláírási szabályzatban meghatározott szabályokat
- ***FDP_ITC.2/Az aláíró tanúsítványa*** és ***FPT_TDC.1/Az aláíró tanúsítványa*** garantálják, hogy egyrészt a TOE figyeli az információ áramlás ellenőrzés szabályzat szabályait a kiválasztott tanúsítvány importálása során, másrészt a TOE képes az importált tanúsítványban található adatok konzisztens értelmezésére.

Hozzájárulnak még e cél lefedéséhez az információ áramlás ellenőrzés szabályzat szubjektumaira és információira vonatkozó biztonsági tulajdonságok kezelésével kapcsolatos alábbi funkcionális biztonsági követelmények is:

- ***FMT_MSA.3/Az aláíró tanúsítványának importálása*** biztosítja, hogy az információ áramlás ellenőrzés szabályban érintett biztonsági tulajdonságok alapértékei korlátozó értékeket vesznek fel.

- ***FMT_MSA.1/Az aláíró tanúsítványa*** és ***FMT_SMF.1/Az aláíró tanúsítványának kiválasztása*** biztosítja, hogy kizárólag az aláíró joga kiválasztani a megfelelő tanúsítványt az általa végrehajtani kívánt elektronikus aláíráshoz.

O.Signatory_Certificate_Validity:
Ennek a biztonsági célnak a lefedése az alábbi módon történik:

- A TOE-nak a tanúsítvány importálása során alkalmaznia kell egy információ áramlás ellenőrzés szabályzatot: ***FDP_IFC.1/Az aláíró tanúsítványának importálása.*** Az ***FDP_IFF.1/Az aláíró tanúsítványának importálása*** funkcionális biztonsági követelmény csak akkor engedi meg a tanúsítvány TOE-ba importálását, ha az aláírási szabályzatban meghatározott, az aláíró tanúsítványára vonatkozó szabályok teljesülnek. A kiválasztott tanúsítvány megfelelősége akkor garantált, ha annak tulajdonságai teljesítik az aláírási szabályzat szabályait.
- ***FDP_ITC.2/Az aláíró tanúsítványa*** és ***FPT_TDC.1/Az aláíró tanúsítványa*** garantálják, hogy egyrészt a TOE figyeli az információ áramlás ellenőrzés szabályzat szabályait a kiválasztott tanúsítvány importálása során, másrészt a TOE képes az importált tanúsítványban található adatok konzisztens értelmezésére.

Hozzájárulnak még e cél lefedéséhez az információ áramlás ellenőrzés szabályzat szubjektumaira és információira vonatkozó biztonsági tulajdonságok kezelésével kapcsolatos alábbi funkcionális biztonsági követelmények is:

- ***FMT_MSA.3/Az aláíró tanúsítványának importálása*** biztosítja, hogy az információ áramlás ellenőrzés szabályban érintett biztonsági tulajdonságok alapértékei korlátozó értékeket vesznek fel.
- ***FMT_MSA.1/Az aláíró tanúsítványa*** és ***FMT_SMF.1/Az aláíró tanúsítványának kiválasztása*** biztosítja, hogy kizárólag az aláíró joga kiválasztani a megfelelő tanúsítványt az általa végrehajtani kívánt elektronikus aláíráshoz.

O.Signature_Attributes_Conformity:
Ennek a biztonsági célnak a lefedése az alábbi módon történik:

- A TOE-nak az aláírás létrehozása során alkalmaznia kell egy információ áramlás ellenőrzés szabályzatot: ***FDP_IFC.1/Aláírás létrehozás.*** Az ***FDP_IFF.1/Aláírás létrehozás*** funkcionális biztonsági követelmény csak akkor engedi meg az aláírás létrehozását (azaz a formattált DTBS átküldését az SCDev-nek), ha az aláírási szabályzatban meghatározott szabályok teljesülnek. Ez a követelmény az aláírási tulajdonságokra vonatkozó szabályokat is meghatározza. Az aláírási tulajdonságok megfelelősége akkor garantált, ha ezek a tulajdonságok teljesítik az aláírási szabályzatban meghatározott szabályokat.

Hozzájárulnak még e cél lefedéséhez az információ áramlás ellenőrzés szabályzat szubjektumaira és információira vonatkozó biztonsági tulajdonságok kezelésével kapcsolatos alábbi funkcionális biztonsági követelmények is:

- ***FMT_MSA.3/Aláírás létrehozás*** biztosítja, hogy az információ áramlás ellenőrzés szabályban érintett biztonsági tulajdonságok alapértékei korlátozó értékeket vesznek fel.
- ***FMT_MSA.1/Aláírási tulajdonságok*** és ***FMT_SMF.1/Az aláírási tulajdonságok módosítása*** biztosítja, hogy kizárólag az aláíró joga módosítani az aláírási tulajdonságokat.

O.Electronic_Signature_Export:
Ennek a biztonsági célnak a lefedése az alábbi módon történik:

- A TOE-nak egy elektronikus aláírás aláíróhoz történő exportálása során alkalmaznia kell egy információ áramlás ellenőrzés szabályzatot: ***FDP_IFC.1/Elektronikus aláírás exportálása.*** Az ***FDP_IFF.1/ Elektronikus aláírás exportálása*** funkcionális biztonsági követelmény meghatározza a TOE

által létrehozott elektronikus aláírás exportálására alkalmazandó szabályokat.

- ***FDP_ETC.2/Elektronikus aláírás exportálása*** megköveteli, hogy a TOE az elektronikus aláírást az ehhez kapcsolódó biztonsági tulajdonságokkal együtt, ezekkel egyértelműen összekapcsolva exportálja.

Hozzájárulnak még e cél lefedéséhez az információ áramlás ellenőrzés szabályzat szubjektumaira és információira vonatkozó biztonsági tulajdonságok kezelésével kapcsolatos alábbi funkcionális biztonsági követelmények is:

- ***FMT_MSA.3/Elektronikus aláírás exportálása*** biztosítja, hogy az információ áramlás ellenőrzés szabályban érintett biztonsági tulajdonságok alapértékei korlátozó értékeket vesznek fel.
- ***FMT_SMF.1/Az SCDev aláírás létrehozás állapotának lekérdezése*** megköveteli, hogy a TOE képes legyen fogadni az SCDev-től a digitális aláírás létrehozás műveletének állapotát.
- ***FMT_MSA.1/Az SCDev aláírás létrehozás állapota*** senkinek sem teszi lehetővé az aláírás létrehozás művelet SCDev-től visszakapott állapotát módosítani.

A kriptográfiai műveletekre vonatkozó cél

O.Cryptographic_Operations:
Ezt a biztonsági célt az alábbi követelmény fedi le: ***FCS_COP.1/Hash függvény****,* mely lehetővé teszi az ST szerzőinek a TOE-ben implementált hash algoritmusok meghatározását.

A dokumentum szamantikai stabilitásának ellenőrzésére vonatkozó cél

O.Document_Stability_Control:
Ennek a biztonsági célnak a lefedése az alábbi módon történik:

- A TOE-nak egy dokumentum TOE-ba importálása során alkalmaznia kell egy információ áramlás ellenőrzés szabályzatot: ***FDP_IFC.1/Dokumentum elfogadás.*** Az ***FDP_IFF.1/Dokumentum elfogadás*** funkcionális biztonsági követelmény meghatározza a TOE által a dokumentum elfogadására alkalmazandó szabályokat.
- ***FDP_ITC.1/Dokumentum elfogadás*** megköveteli, hogy a TOE határozza meg a dokumentum szemantikájáról, hogy az stabil vagy nem, amikor importálja azt.

Hozzájárulnak még e cél lefedéséhez az információ áramlás ellenőrzés szabályzat szubjektumaira és információira vonatkozó biztonsági tulajdonságok kezelésével kapcsolatos alábbi funkcionális biztonsági követelmények is:

- ***FMT_MSA.3/Dokumentum elfogadás*** biztosítja, hogy az információ áramlás ellenőrzés szabályban érintett biztonsági tulajdonságok alapértékei korlátozó értékeket vesznek fel.
- ***FMT_MSA.1/Dokumentum szemantika stabilitás állapota*** és ***FMT_SMF.1/A dokumentum stabilitás állapot megszerzése*** megköveteli, hogy egyrészt a TOE képes legyen a dokumentum szemantika stabilitásának megállapítására, másrészt senki sem módosíthatja az ellenőrzés eredményét.
- ***FMT_MSA.1/Az aláíró egyetértése nem stabil dokumentum aláírására*** és ***FMT_SMF.1/Az aláíró egyetértésének megszerzése nem stabil dokumentum aláírására*** biztosítja, hogy csak az aláíró módosíthatja azt a biztonsági tulajdonságot, mely lehetővé teszi egy olyan dokumentum aláírási folyamatának folytatását, melynek szemantikája nem tekinthető stabilnak.

Az aláírandó dokumentumum megjelenítésére vonatkozó cél

O.Viewer_Application_Execution:
Ezt a biztonsági célt az alábbi funkcionális biztonsági követelmények fedik le:

- ***FDP_IFF.1/Aláírás létrehozás***, mely biztosítja, hogy az aláíró egy külső megjelenítő alkalmazással megtekinthesse a dokumentumot. A TOE automatikusan vérehajtja az aláírandó dokumentum formátumának megfelelő megjelenítő alkalmazást a dokumentum formátum/megjelenítő összerendelés tábla felhasználásával.
- ***FMT_MTD.1/Dokumentum formátum/megjelenítő összerendelés tábla*** és ***FMT_SMF.1/A dokumentum formátum/megjelenítő összerendelés tábla kezelése***, melyek lehetővé teszik az aláíró számára (és csak az ő számára), hogy módosítsa a dokumentum formátumokat és a megjelenítő alkalmazásokat összerendelő táblát.

6.3.1.2 Megfeleltetés a biztonsági célok és a biztonsági követelmények között

Biztonsági célok	Funkcionális biztonsági követelmények
O.Certificate/Private_Key_Association	FDP_IFF.1/Aláírás létrehozás
O.Administration	FMT.SMR.1 FMT_MTD.1/Dokumentum formátum/megjelenítő összerendelés tábla FMT_SMF.1/A dokumentum formátum/megjelenítő összerendelés tábla kezelése FMT_SMF.1/Az aláírási szabályzatok kezelése FMT_MTD.1/Az aláírási szabályzatok kezelése
O.Signature_Attributes_Presentation	FDP_IFF.1/Aláírás létrehozás
O.Explicit_Agreement	FDP_ITC.1/Az aláíró közvetlen egyetértése
O.Signature_Process_Interruption	FDP_ROL.2/Az aláírási folyamat megszakítása
O.Documents_To_Be_Signed	FMT_MSA.1/Kiválasztott dokumentumok FMT_SMF.1/Egy dokumentum lista kiválasztása FMT_MSA.1/Aláírási tulajdonságok FMT_SMF.1/Az aláírási tulajdonságok módosítása
O.Signatory_Certificate_Conformity	FDP_IFC.1/Az aláíró tanúsítványának importálása. FDP_IFF.1/Az aláíró tanúsítványának importálása FDP_ITC.2/Az aláíró tanúsítványa FPT_TDC.1/Az aláíró tanúsítványa FMT_MSA.3/Az aláíró tanúsítványának importálása FMT_MSA.1/Az aláíró tanúsítványa FMT_SMF.1/Az aláíró tanúsítványának kiválasztása
O.Signatory_Certificat_Validity	FDP_IFC.1/Az aláíró tanúsítványának importálása FDP_IFF.1/Az aláíró tanúsítványának importálása FDP_ITC.2/Az aláíró tanúsítványa FPT_TDC.1/Az aláíró tanúsítványa FMT_MSA.3/Az aláíró tanúsítványának importálása FMT_MSA.1/Az aláíró tanúsítványa FMT_SMF.1/Az aláíró tanúsítványának kiválasztása
O.Signature_Attributes_Conformity	FDP_IFC.1/Aláírás létrehozás FDP_IFF.1/Aláírás létrehozás FMT_MSA.3/Aláírás létrehozás FMT_MSA.1/Aláírási tulajdonságok FMT_SMF.1/Az aláírási tulajdonságok módosítása
O.Electronic_Signature_Export	FDP_IFC.1/Elektronikus aláírás exportálása FDP_IFF.1/ Elektronikus aláírás exportálása FDP_ETC.2/Elektronikus aláírás exportálása FMT_MSA.3/Elektronikus aláírás exportálása FMT_SMF.1/Az SCDev aláírás létrehozás állapotának lekérdezése FMT_MSA.1/Az SCDev aláírás létrehozás állapota
O.Cryptographic_Operations	FCS_COP.1/Hash függvény
O.Document_Stability_Control	FDP_IFC.1/Dokumentum elfogadás FDP_IFF.1/Dokumentum elfogadás FDP_ITC.1/Dokumentum elfogadás FMT_MSA.3/Dokumentum elfogadás FMT_MSA.1/Dokumentum szemantika stabilitás állapota FMT_SMF.1/A dokumentum stabilitás állapot megszerzése FMT_MSA.1/Az aláíró egyetértése nem stabil dokumentum aláírására FMT_SMF.1/Az aláíró egyetértésének megszerzése nem stabil dokumentum aláírására
O.Viewer_Application_Execution	FDP_IFF.1/Aláírás létrehozás FMT_MTD.1/Dokumentum formátum/megjelenítő összerendelés tábla FMT_SMF.1/A dokumentum formátum/megjelenítő összerendelés tábla kezelése

6.4 táblázat: A TOE biztonsági célok lefedettsége
az aláírás létrehozásra vonatkozó funkcionális biztonsági követelményekkel

Funkcionális biztonsági követelmények	Biztonsági célok
FDP_IFC.1/Dokumentum elfogadás	O.Document_Stability_Control
FDP_IFF.1/Dokumentum elfogadás	O.Document_Stability_Control
FDP_ITC.1/Dokumentum elfogadás	O.Document_Stability_Control
FMT_MSA.3/Dokumentum elfogadás	O.Document_Stability_Control
FMT_MSA.1/Kiválasztott dokumentumok	O. Documents_To_Be_Signed
FMT_SMF.1/Egy dokumentum lista kiválasztása	O. Documents_To_Be_Signed
FMT_MSA.1/Dokumentum szemantika stabilitás állapota	O.Document_Stability_Control
FMT_SMF.1/A dokumentum stabilitás állapot meghatározása	O.Document_Stability_Control
FMT_MSA.1/Az aláíró egyetértése nem stabil dokumentum aláírására	O.Document_Stability_Control
FMT_SMF.1/Az aláíró egyetértésének megszerzése nem stabil dokumentum aláírására	O.Document_Stability_Control
FDP_ROL.2/Az aláírási folyamat megszakítása	O.Signature_Process_Interruption
FMT_MSA.1/Aláírási tulajdonságok	O. Documents_To_Be_Signed O.Signature_Attributes_Conformity
FMT_SMF.1/Az aláírási tulajdonságok módosítása	O. Documents_To_Be_Signed O.Signature_Attributes_Conformity
FDP_IFC.1/Az aláíró tanúsítványának importálása	O.Signatory_Certificate_Conformity O.Signatory_Certificat_Validity
FDP_IFF.1/Az aláíró tanúsítványának importálása	O.Signatory_Certificate_Conformity O.Signatory_Certificat_Validity
FMT_MSA.3/Az aláíró tanúsítványának importálása	O.Signatory_Certificate_Conformity O.Signatory_Certificat_Validity
FMT_MSA.1/Az aláíró tanúsítványa	O.Signatory_Certificate_Conformity O.Signatory_Certificat_Validity
FDP_ITC.2/Az aláíró tanúsítványa	O.Signatory_Certificate_Conformity O.Signatory_Certificat_Validity
FPT_TDC.1/Az aláíró tanúsítványa	O.Signatory_Certificate_Conformity O.Signatory_Certificat_Validity
FMT_SMF.1/Az aláíró tanúsítványának kiválasztása	O.Signatory_Certificate_Conformity O.Signatory_Certificat_Validity
FDP_IFC.1/Aláírás létrehozás	O.Certificate/Private_Key_Association O.Signature_Attributes_Conformity
FDP_IFF.1/Aláírás létrehozás	O.Signature_Attributes_Conformity O.Signature_Attributes_Presentation O.Viewer_Application_Execution
FMT_MSA.3/Aláírás létrehozás	O.Signature_Attributes_Conformity
FDP_ITC.1/Az aláíró közvetlen egyetértése	O.Explicit_Agreement
FDP_IFC.1/Elektronikus aláírás exportálása	O.Electronic_Signature_Export
FDP_IFF.1/ Elektronikus aláírás exportálása	O.Electronic_Signature_Export
FDP_ETC.2/Elektronikus aláírás exportálása	O.Electronic_Signature_Export
FMT_MSA.3/Elektronikus aláírás exportálása	O.Electronic_Signature_Export
FMT_MSA.1/Az SCDev aláírás létrehozás állapota	O.Electronic_Signature_Export
FMT_SMF.1/Az SCDev aláírás létrehozás állapotának lekérdezése	O.Electronic_Signature_Export
FCS_COP.1/Hash függvény	O.Cryptographic_Operations
FMT_SMR.1	O.Administration
FMT_MTD.1/Dokumentum formátum/megjelenítő összerendelés tábla	O.Administration O.Viewer_Application_Execution
FMT_SMF.1/A dokumentum formátum/megjelenítő összerendelés tábla kezelése	O.Administration O.Viewer_Application_Execution
FMT_MTD.1/Az aláírási szabályzatok kezelése	O.Administration
FMT_SMF.1/Az aláírási szabályzatok kezelése	O.Administration

6.5. táblázat: Az aláírás létrehozására vonatkozó funkcionális biztonsági követelmények lefedettsége a TOE biztonsági célokkal

6.3.2 Az aláírás ellenőrzésére vonatkozó funkcionális biztonsági követelmények indoklása

6.3.2.1 A biztonsági célok lefedése a funkcionális biztonsági követelményekkel

Általános cél

O.Administration:
Ezt a biztonsági célt az alábbi funkcionális biztonsági követelmények fedik le:

- ***FMT_SMR.1*** megköveteli, hogy a TOE különböztesse meg az ellenőrző szerepkörét az aláíró szerepkörétől.
- ***FMT_SMF.1/Az aláírási szabályzatok részleges kezelése***, mely meghatározza az aláírási szabályzatok kezelésének műveleteit, valamint ***FMT_MTD.1/Az aláírási szabályzatok rézsleges kezelése***, mely ezek használatát az ellenőrzőre korlátozza.

Az ellenőrzési szabályokra vonatkozó célok

O.Time_Reference:
Ezt a biztonsági célt az alábbi funkcionális biztonsági követelmények fedik le:

- A TOE-nak a digitális aláíráshoz kapcsolt idő hivatkozás importálása során alkalmaznia kell egy információ áramlás ellenőrzés szabályzatot: ***FDP_IFC.1/Idő hivatkozás***, hogy érvényesként elfogadja ezt az idő hivatkozást. Az ***FDP_IFF.1/Idő hivatkozás*** funkcionális biztonsági követelmény az idő hivatkozás érvényességének meghatározásához különböző adatokra határoz meg alkalmazandó szabályokat; egyes szabályok magára az idő hivatkozásra, mások pedig e hivatkozás érvényesítő adataira vonatkoznak. A követelmény felsorolja az általa meghatározott érvényesítő adatokra alkalmazandó szabályokat, az alkalmazandó aláírási szabályzat szerint ezek egy részét kell ténylegesen alkalmazni.
- ***FMT_MTD.1/Az alkalmazandó aláírási szabályzat kiválasztása*** és ***FMT_SMF.1/Az alkalmazandó aláírási szabályzat kiválasztása***, melyek megkövetelik, hogy csak az ellenőrző választhassa ki az alkalmazandó aláírási szabályzatot.
- ***FDP_ITC.2/Idő hivatkozás*** és ***FPT_TDC.1/Idő hivatkozás*** biztosítja, hogy egyrészt a TOE alkalmazza az információ áramlás ellenőrzés szabályzatot az idő hivatkozás importálása során, másrészt a TOE képes az idő hivatkozások konzisztens értelmezésére.

Hozzájárulnak még e cél lefedéséhez az információ áramlás ellenőrzés szabályzat szubjektumaira és információira vonatkozó biztonsági tulajdonságok kezelésével kapcsolatos alábbi funkcionális biztonsági követelmények is:

- ***FMT_MSA.3/Idő hivatkozás*** biztosítja, hogy az információ áramlás ellenőrzés szabályban érintett biztonsági tulajdonságok alapértékei korlátozó értékeket vesznek fel.
- ***FMT_MSA.1/Idő hivatkozás*** biztosítja, hogy az idő hivatkozás biztonsági tulajdonságai nem módosíthatók.
- ***FMT_MSA.1/Tanúsítványok*** biztosítja, hogy az idő hivatkozás érvényességének ellenőrzését befolyásoló tanúsítványok biztonsági tulajdonságai nem módosíthatók.
- ***FMT_MSA.1/Tanúsítvány érvényesítő*** adatok biztosítja, hogy az idő hivatkozás érvényességének ellenőrzését befolyásoló tanúsítványok érvényesítő adatainak biztonsági tulajdonságai nem módosíthatók.

O.Certification_Path:
Ezt a biztonsági célt az alábbi funkcionális biztonsági követelmények fedik le:

- A TOE-nak az aláíró tanúsítványát és egy az alkalmazott aláírási szabályzat által meghatározott gyökér tanúsítványt összekötő tanúsítványláncot alkotó tanúsítványok importálása során alkalmaznia kell egy információ áramlás ellenőrzés szabályzato***t: FDP_IFC.1/ Tanúsítványlánc.***
- ***FDP_ITC.2/Tanúsítványlánc*** biztosítja, hogy a TOE alkalmazza az információ áramlás ellenőrzés szabályzatot a tanúsítványok importálása során, ***FPT_TDC.1/Tanúsítványok*** és ***FPT_TDC.1/Tanúsítvány visszavonási adat*** pedig biztosítják, hogy a TOE képes ezen adatok konzisztens értelmezésére.
- Az ***FDP_IFF.1/Tanúsítványlánc*** funkcionális biztonsági követelmény meghatározza az információ áramlás ellenőrzés szabályzat alkalmazandó szabályait. A tanúsítványlánc érvényességét biztosító ellenőrzési szabályokat az alkalmazandó aláírási szabályzat határozza meg.
- ***FMT_MTD.1/Az alkalmazandó aláírási szabályzat kiválasztása*** és ***FMT_SMF.1/Az alkalmazandó aláírási szabályzat kiválasztása***, melyek megkövetelik, hogy csak az ellenőrző választhassa ki az alkalmazandó aláírási szabályzatot.

Hozzájárulnak még e cél lefedéséhez az információ áramlás ellenőrzés szabályzat szubjektumaira és információira vonatkozó biztonsági tulajdonságok kezelésével kapcsolatos alábbi funkcionális biztonsági követelmények is:

- ***FMT_MSA.3/Tanúsítványlánc*** biztosítja, hogy az információ áramlás ellenőrzés szabályban érintett biztonsági tulajdonságok alapértékei korlátozó értékeket vesznek fel.
- ***FMT_MSA.1/Tanúsítványok*** biztosítja, hogy a tanúsítványlánc felépítéséhez alapvető fontosságú importált tanúsítvány tulajdonságok nem módosíthatók.
- ***FMT_MSA.1/Tanúsítvány érvényesítő adatok*** biztosítja, hogy az aláíró tanúsítvány érvényesítő adatainak biztonsági tulajdonságai nem módosíthatók.

O.Certificates_Conformity:
Ezt a biztonsági célt az alábbi funkcionális biztonsági követelmények fedik le:

- A TOE-nak alkalmaznia kell egy információ áramlás ellenőrzés szabályzatot (***FDP_IFC.1/Tanúsítványlánc***) az aláíró tanúsítványát és egy az alkalmazott aláírási szabályzat által meghatározott gyökér tanúsítványt összekötő tanúsítványláncot alkotó tanúsítványok importálása során.
- ***FDP_ITC.2/Tanúsítványlánc*** biztosítja, hogy a TOE alkalmazza az információ áramlás ellenőrzés szabályzatot a tanúsítványok importálása során.
- ***FPT_TDC.1/Tanúsítványok*** és ***FPT_TDC.1/Tanúsítvány visszavonási adat*** biztosítja, hogy a TOE képes a tanúsítványok konzisztens értelmezésére.
- Az információ áramlás ellenőrzés szabályzat szabályait ***FDP_IFF.1/ Tanúsítványlánc*** határozza meg, mely jelzi a megvalósítandó szabályokat.
- A tanúsítványlánc érvényességét biztosító ellenőrzési szabályokat az alkalmazott aláírási szabály határozza meg. Ezt az aláírási szabályzatot csak az ellenőrző választhatja ki (***FMT_MTD.1/Az alkalmazandó aláírási szabályzat kiválasztása*** és ***FMT_SMF.1/Az alkalmazandó aláírási szabályzat kiválasztása***).

Hozzájárulnak még e cél lefedéséhez az információ áramlás ellenőrzés szabályzat szubjektumaira és információira vonatkozó biztonsági tulajdonságok kezelésével kapcsolatos alábbi funkcionális biztonsági követelmények is:

- ***FMT_MSA.3/Tanúsítványlánc*** biztosítja, hogy az információ áramlás ellenőrzés szabályban érintett biztonsági tulajdonságok alapértékei korlátozó értékeket vesznek fel.
- ***FMT_MSA.1/Tanúsítványok*** biztosítja, hogy a tanúsítványlánc felépítéséhez importált tanúsítványok tulajdonságai nem módosíthatók.
- ***FMT_MSA.1/Tanúsítvány érvényesítő adatok*** biztosítja, hogy az aláíró tanúsítvány érvényesítő adatainak biztonsági tulajdonságai nem módosíthatók.

O.Certificates_Validity:
Ezt a biztonsági célt az alábbi funkcionális biztonsági követelmények fedik le:

- A TOE-nak alkalmaznia kell egy információ áramlás ellenőrzés szabályzatot (***FDP_IFC.1/ Tanúsítványlánc***) az aláíró tanúsítványát és egy az alkalmazott aláírási szabályzat által meghatározott gyökér tanúsítványt összekötő tanúsítványláncot alkotó tanúsítványok importálása során. Ez az információ áramlás ellenőrzés szabályzat alkalmazandó a tanúsítványokhoz kapcsolódó visszavonási információkra is.
- ***FDP_ITC.2/Tanúsítványlánc*** biztosítja, hogy a TOE alkalmazza az információ áramlás ellenőrzés szabályzatot a tanúsítványok és a visszavonási információk importálása során.
- ***FPT_TDC.1/Tanúsítványok*** és a ***FPT_TDC.1/Tanúsítvány visszavonási adat*** biztosítják, hogy a TOE képes a tanúsítványok és a visszavonási információk konzisztens értelmezésére.
- Az ***FDP_IFF.1/Tanúsítványlánc*** funkcionális biztonsági követelmény meghatározza az információ áramlás ellenőrzés szabályzat alkalmazandó szabályait. Ezek között a szabályok között vannak azok is, melyek alapján a TSF meggyőződhet arról, hogy a tanúsítványlánc tanúsítványai érvényesek, s állapotuk nem visszavont.
- A tanúsítványlánc érvényességét biztosító ellenőrzési szabályokat az alkalmazandó aláírási szabályzat határozza meg. Ezt a szabályzatot csak az ellenőrző választhatja ki (***FMT_MTD.1/Az alkalmazandó aláírási szabályzat kiválasztása*** és ***FMT_SMF.1/Az alkalmazandó aláírási szabályzat kiválasztása***).

Hozzájárulnak még e cél lefedéséhez az információ áramlás ellenőrzés szabályzat szubjektumaira és információira vonatkozó biztonsági tulajdonságok kezelésével kapcsolatos alábbi funkcionális biztonsági követelmények is:

- ***FMT_MSA.3/Tanúsítványlánc*** biztosítja, hogy az információ áramlás ellenőrzés szabályban érintett biztonsági tulajdonságok alapértékei korlátozó értékeket vesznek fel.
- ***FMT_MSA.1/Tanúsítványok*** biztosítja, hogy a tanúsítványlánc felépítéséhez importált tanúsítványok tulajdonságai nem módosíthatók.
- ***FMT_MSA.1/Tanúsítvány érvényesítő adatok*** biztosítja, hogy az aláíró tanúsítvány érvényesítő adatainak biztonsági tulajdonságai nem módosíthatók.

O.Validation_Data_Conformity:
Ezt a biztonsági célt az alábbi funkcionális biztonsági követelmények fedik le:

- A TOE-nak alkalmaznia kell egy információ áramlás ellenőrzés szabályzatot (***FDP_IFC.1/ Tanúsítványlánc***) az aláíró tanúsítványát és egy az alkalmazott aláírási szabályzat által meghatározott gyökér tanúsítványt összekötő tanúsítványláncot alkotó tanúsítványok importálása során. Ez az információ áramlás ellenőrzés szabályzat alkalmazandó a tanúsítványokhoz kapcsolódó visszavonási információkra is.

- ***FDP_ITC.2/Tanúsítványlánc*** biztosítja, hogy a TOE alkalmazza az információ áramlás ellenőrzés szabályzatot a tanúsítványok és a visszavonási információk importálása során.
- ***FPT_TDC.1/Tanúsítványok*** és a ***FPT_TDC.1/Tanúsítvány visszavonási adat*** biztosítják, hogy a TOE képes a tanúsítványok és a visszavonási információk konzisztens értelmezésére.
- Az ***FDP_IFF.1/Tanúsítványlánc*** funkcionális biztonsági követelmény meghatározza az információ áramlás ellenőrzés szabályzat alkalmazandó szabályait. Ezek között a szabályok között vannak azok is, melyek alapján a TSF meggyőződhet a tanúsítvány visszavonási adatok érvényességéről.
- A tanúsítványlánc tanúsítványaira vonatkozó visszavonási adatok érvényességét biztosító ellenőrzési szabályokat az alkalmazandó aláírási szabályzat határozza meg. Ezt a szabályzatot csak az ellenőrző választhatja ki (***FMT_MTD.1/Az alkalmazandó aláírási szabályzat kiválasztása*** és ***FMT_SMF.1/Az alkalmazandó aláírási szabályzat kiválasztása***).

Hozzájárulnak még e cél lefedéséhez az információ áramlás ellenőrzés szabályzat szubjektumaira és információira vonatkozó biztonsági tulajdonságok kezelésével kapcsolatos alábbi funkcionális biztonsági követelmények is:

- ***FMT_MSA.3/Tanúsítványlánc*** biztosítja, hogy az információ áramlás ellenőrzés szabályban érintett biztonsági tulajdonságok alapértékei korlátozó értékeket vesznek fel.
- ***FMT_MSA.1/Tanúsítványok*** biztosítja, hogy a tanúsítványlánc felépítéséhez importált tanúsítványok tulajdonságai nem módosíthatók.
- ***FMT_MSA.1/Tanúsítvány érvényesítő adatok*** biztosítja, hogy az aláíró tanúsítvány érvényesítő adatainak biztonsági tulajdonságai nem módosíthatók.

O.Signed_Attributes_Conformity:

Ezt a biztonsági célt az alábbi funkcionális biztonsági követelmények fedik le:

- A TOE-nak alkalmaznia kell egy információ áramlás ellenőrzés szabályzatot az elektronikus aláírások importálása során: ***FDP_IFC.1/Elektronikus aláírás.*** Az FDP_IFF.1/ Elektronikus aláírás funkcionális biztonsági követelmény meghatározza az információ áramlás ellenőrzés szabályzat alkalmazandó szabályait, köztük az aláírási tulajdonságok megfelelőségének ellenőrzésére vonatkozókat is. Ez a követelmény meghatározza a TOE által megvalósítandó szabályokat is. Az alkalmazott aláírási szabályzat ezen szabályok egy részét használja.
- ***FMT_MTD.1/Az alkalmazandó aláírási szabályzat kiválasztása*** és ***FMT_SMF.1/Az alkalmazandó aláírási szabályzat kiválasztása*** megkövetelik, hogy csak az ellenőrző választhassa ki az alkalmazandó aláírási szabályzatot.
- ***FDP_ITC.2/Elektronikus aláírás*** biztosítja, hogy a TOE alkalmazza az információ áramlás ellenőrzés szabályzatot az elektronikus aláírások (köztük az aláírási tulajdonságok) importálása során, ***FPT_TDC.1/Elektronikus aláírás*** pedig biztosítja, hogy a TOE képes az elektronikus aláírások (köztük az aláírási tulajdonságok) konzisztens értelmezésére.

Hozzájárulnak még e cél lefedéséhez az információ áramlás ellenőrzés szabályzat szubjektumaira és információira vonatkozó biztonsági tulajdonságok kezelésével kapcsolatos alábbi funkcionális biztonsági követelmények is:

- ***FMT_MSA.3/Elektronikus aláírás*** biztosítja, hogy az információ áramlás ellenőrzés szabályban érintett biztonsági tulajdonságok alapértékei korlátozó értékeket vesznek fel.

- ***FMT_MSA.1/Elektronikus aláírás*** biztosítja, hogy az aláírási tulajdonságok nem módosíthatók.

Az aláírt adatok megjelenítésére vonatkozó célok

O.Presentation_Application_Execution:
Ezt a biztonsági célt az alábbi funkcionális biztonsági követelmények fedik le:

- ***FDP_IFF.1/Elektronikus aláírás***, mely biztosítja, hogy az ellenőrző megtekintheti a dokumentumot egy külső megjelenítő alkalmazáson keresztül.

O.Signed_Attributes_Communication:
Ezt a biztonsági célt az alábbi funkcionális biztonsági követelmény fedi le:

- ***FDP_IFF.1/Elektronikus aláírás***, mely megköveteli, hogy a TOE képes legyen az aláírási tulajdonságok exportálására.

O.Validation_Data_Export:
Ezt a biztonsági célt az alábbi funkcionális biztonsági követelmények fedik le:

- A TOE-nak alkalmaznia kell egy információ áramlás ellenőrzés szabályzatot az aláírás ellenőrzés eredményének exportálása során (***FDP_IFC.1/Elektronikus aláírás ellenőrzés*** és ***FDP_IFF.1/ Elektronikus aláírás ellenőrzés***).
- ***FDP_ETC.2/Ellenőrzési állapot***, mely megköveteli az aláírás ellenőrzési állapot továbbítását az ellenőrző számára, a pontosságot bizonyító érvényesítő adatokkal és az aláírás feldolgozásához szükséges információkkal (aláírási tulajdonságok, az aláíró tanúsítványának egyes mezői, …) együtt.

Hozzájárulnak még e cél lefedéséhez az információ áramlás ellenőrzés szabályzat szubjektumaira és információira vonatkozó biztonsági tulajdonságok kezelésével kapcsolatos alábbi funkcionális biztonsági követelmények is:

- ***FMT_MSA.3/Aláírás ellenőrzés állapot*** biztosítja, hogy az információ áramlás ellenőrzés szabályban érintett biztonsági tulajdonságok alapértékei korlátozó értékeket vesznek fel.
- ***FMT_MSA.1/Aláírás ellenőrzés állapot*** biztosítja, hogy az aláírás ellenőrzés állapota nem módosítható.

Az ellenőrizendő dokumentumok szemantikai stabilitásának ellenőrzésére vonatkozó célok

O.Document_Stability_Control:
Ennek a biztonsági célnak a lefedése az alábbi módon történik:

- A TOE-nak egy dokumentum TOE-ba importálása során alkalmaznia kell egy információ áramlás ellenőrzés szabályzatot: ***FDP_IFC.1/Dokumentum elfogadás.*** Az ***FDP_IFF.1/Dokumentum elfogadás*** funkcionális biztonsági követelmény meghatározza a TOE által a dokumentum elfogadására alkalmazandó szabályokat.
- ***FDP_ITC.1/Dokumentum elfogadás*** megköveteli, hogy a TOE határozza meg a dokumentum szemantikájáról, hogy az stabil vagy nem, amikor importálja azt.

Hozzájárulnak még e cél lefedéséhez az információ áramlás ellenőrzés szabályzat szubjektumaira és információira vonatkozó biztonsági tulajdonságok kezelésével kapcsolatos alábbi funkcionális biztonsági követelmények is:

- ***FMT_MSA.3/Dokumentum elfogadás*** biztosítja, hogy az információ áramlás ellenőrzés szabályban érintett biztonsági tulajdonságok alapértékei korlátozó értékeket vesznek fel.
- ***FMT_MSA.1/Dokumentum szemantika stabilitás állapota*** és ***FMT_SMF.1/A dokumentum stabilitás állapot megszerzése*** megköveteli, hogy egyrészt a TOE

képes legyen megállapítani a dokumentum szemantikai stabilitását, másrészt senki sem módosíthatja az ellenőrzés eredményét.

A kriptográfiai műveletekre vonatkozó cél

O.Cryptographic_Operations:
Ezt a biztonsági célt az alábbi funkcionális biztonsági követelmények fedik le:

- ***FCS_COP.1/Hash függvény***, mely garantálja az ütközés-mentes tulajdonságot a hash algoritmust megvalósító alkalmazás által készített lenyomatok között.
- ***FCS_COP.1/Aláírás ellenőrzés***, mely garantálja, hogy az elektronikus aláírás ellenőrzési folyamatában használt valamennyi kriptográfiai algoritmus ellenáll a kriptográfiai támadásoknak. Ezen belül a kulcsok méretének kellően nagynak kell lennie, hogy a tanúsítványban megtalálható nyilvános kulcs ellenálljon a támadásoknak a tanúsítvány teljes érvényességi időszakában.

6.3.2.2 Megfeleltetés a biztonsági célok és a biztonsági követelmények között

Biztonsági célok	Funkcionális biztonsági követelmények
O.Administration	FMT_SMR.1 FMT_SMF.1/Az aláírási szabályzat részleges kezelése FMT_MTD.1/Az aláírási szabályzat részleges kezelése
O.Time_Reference	FDP_IFC.1/Idő hivatkozás FDP_IFF.1/Idő hivatkozás FMT_MTD.1/Az alkalmazandó aláírási szabályzat kiválasztása FMT_SMF.1/Az alkalmazandó aláírási szabályzat kiválasztása FDP_ITC.2/Idő hivatkozás FPT_TDC.1/Idő hivatkozás FMT_MSA.3/Idő hivatkozás FMT_MSA.1/Idő hivatkozás FMT_MSA.1/Tanúsítványok FMT_MSA.1/Tanúsítványérvényesítő adatok
O.Certification_Path	FDP_IFC.1/Tanúsítványlánc. FDP_ITC.2/Tanúsítványlánc FPT_TDC.1/Tanúsítványok FPT_TDC.1/Tanúsítvány visszavonási adat FDP_IFF.1/Tanúsítványlánc FMT_MTD.1/Az alkalmazandó aláírási szabályzat kiválasztása FMT_SMF.1/Az alkalmazandó aláírási szabályzat kiválasztása FMT_MSA.3/Tanúsítványlánc FMT_MSA.1/Tanúsítványok FMT_MSA.1/Tanúsítványérvényesítő adatok
O.Certificates_Conformity	FDP_IFC.1/Tanúsítványlánc FDP_ITC.2/Tanúsítványlánc FPT_TDC.1/Tanúsítványok FPT_TDC.1/Tanúsítvány visszavonási adat FDP_IFF.1/Tanúsítványlánc FMT_MTD.1/Az alkalmazandó aláírási szabályzat kiválasztása FMT_SMF.1/Az alkalmazandó aláírási szabályzat kiválasztása FMT_MSA.3/Tanúsítványlánc FMT_MSA.1/Tanúsítványok FMT_MSA.1/Tanúsítványérvényesítő adatok
O.Certificates_Validity	FDP_IFC.1/Tanúsítványlánc FDP_ITC.2/Tanúsítványlánc FPT_TDC.1/Tanúsítványok FPT_TDC.1/Tanúsítvány visszavonási adat FDP_IFF.1/Tanúsítványlánc FMT_MTD.1/Az alkalmazandó aláírási szabályzat kiválasztása FMT_SMF.1/Az alkalmazandó aláírási szabályzat kiválasztása FMT_MSA.3/Tanúsítványlánc FMT_MSA.1/Tanúsítványok FMT_MSA.1/Tanúsítványérvényesítő adatok

Biztonsági célok	Funkcionális biztonsági követelmények
O.Validation_Data_Conformity	FDP_IFC.1/Tanúsítványlánc FDP_ITC.2/Tanúsítványlánc FPT_TDC.1/Tanúsítványok FPT_TDC.1/Tanúsítvány visszavonási adat FDP_IFF.1/Tanúsítványlánc FMT_MTD.1/Az alkalmazandó aláírási szabályzat kiválasztása FMT_SMF.1/Az alkalmazandó aláírási szabályzat kiválasztása FMT_MSA.3/Tanúsítványlánc FMT_MSA.1/Tanúsítványok FMT_MSA.1/Tanúsítványérvényesítő adatok
O.Signed_Attributes_Conformity	FDP_IFC.1/Elektronikus aláírás FDP_IFF.1/ Elektronikus aláírás FMT_MTD.1/Az alkalmazandó aláírási szabályzat kiválasztása FMT_SMF.1/Az alkalmazandó aláírási szabályzat kiválasztása FDP_ITC.2/Elektronikus aláírás FPT_TDC.1/Elektronikus aláírás FMT_MSA.3/Elektronikus aláírás FMT_MSA.1/Elektronikus aláírás
O.Presentation_Application_ Execution	FDP_IFF.1/Elektronikus aláírás
O.Signed_Attributes_ Communication	FDP_IFF.1/Elektronikus aláírás
O.Validation_Data_Export	FDP_IFC.1/Elektronikus aláírás ellenőrzés FDP_IFF.1/Elektronikus aláírás ellenőrzés FDP_ETC.2/Ellenőrzési állapot FMT_MSA.3/Aláírás ellenőrzés állapot FMT_MSA.1/Aláírás ellenőrzés állapot
O.Document_Stability_Control	FDP_IFC.1/Dokumentum elfogadás FDP_IFF.1/Dokumentum elfogadás FDP_ITC.1/Dokumentum elfogadás FMT_MSA.3/Dokumentum elfogadás FMT_MSA.1/Dokumentum szemantika stabilitás állapota FMT_SMF.1/A dokumentum stabilitás állapot megszerzése
O.Cryptographic_Operations	FCS_COP.1/Hash függvény FCS_COP.1/Aláírás ellenőrzés

6.6. táblázat: A TOE biztonsági célok lefedettsége
az aláírás ellenőrzésére vonatkozó funkcionális követelményekkel

Funkcionális biztonsági követelmények	Biztonsági célok
FDP_IFC.1/Dokumentum elfogadás	O.Document_Stability_Control
FDP_IFF.1/Dokumentum elfogadás	O.Document_Stability_Control
FDP_ITC.1/Dokumentum elfogadás	O.Document_Stability_Control
FMT_MSA.3/Dokumentum elfogadás	O.Document_Stability_Control
FMT_MSA.1/Dokumentum szemantika stabilitás állapota	O.Document_Stability_Control
FMT_SMF.1/A dokumentum stabilitás állapot meghatározása	O.Document_Stability_Control
FMT_SMF.1/Az alkalmazandó aláírási szabályzat kiválasztása	O.Time_Reference O.Certification_Path O.Certificates_Conformity O.Certificates_Validity O.Validation_Data_Conformity O.Signed_Attributes_Conformity
FMT_MTD.1/Az alkalmazandó aláírási szabályzat kiválasztása	O.Time_Reference O.Certification_Path O.Certificates_Conformity O.Certificates_Validity O.Validation_Data_Conformity O.Signed_Attributes_Conformity
FDP_IFC.1/Elektronikus aláírás	O.Signed_Attributes_Conformity
FDP_IFF.1/ Elektronikus aláírás	O.Signed_Attributes_Conformity O.Presentation_Application_Execution O.Signed_Attributes_Communication
FMT_MSA.3/Elektronikus aláírás	O.Signed_Attributes_Conformity
FMT_MSA.1/Elektronikus aláírás	O.Signed_Attributes_Conformity
FDP_ITC.2/Elektronikus aláírás	O.Signed_Attributes_Conformity
FDP_IFC.1/Idő hivatkozás	O.Time_Reference
FDP_IFF.1/Idő hivatkozás	O.Time_Reference
FMT_MSA.3/Idő hivatkozás	O.Time_Reference
FMT_MSA.1/Idő hivatkozás	O.Time_Reference
FDP_ITC.2/Idő hivatkozás	O.Time_Reference
FMT_MSA.1/Tanúsítványok	O.Time_Reference O.Certification_Path O.Certificates_Conformity O.Certificates_Validity O.Validation_Data_Conformity
FMT_MSA.1/Tanúsítványérvényesítő adatok	O.Time_Reference O.Certification_Path O.Certificates_Conformity O.Certificates_Validity O.Validation_Data_Conformity
FDP_IFC.1/Tanúsítványlánc	O.Certification_Path O.Certificates_Conformity O.Certificates_Validity O.Validation_Data_Conformity
FDP_IFF.1/Tanúsítványlánc	O.Certification_Path O.Certificates_Conformity O.Certificates_Validity O.Validation_Data_Conformity

Funkcionális biztonsági követelmények	Biztonsági célok
FMT_MSA.3/Tanúsítványlánc	O.Certification_Path O.Certificates_Conformity O.Certificates_Validity O.Validation_Data_Conformity
FDP_ITC.2/Tanúsítványlánc	O.Certification_Path O.Certificates_Conformity O.Certificates_Validity O.Validation_Data_Conformity
FPT_TDC.1/Elektronikus aláírás	O.Signed_Attributes_Conformity
FPT_TDC.1/Idő hivatkozás	O.Time_Reference
FPT_TDC.1/Tanúsítványok	O.Certification_Path O.Certificates_Conformity O.Certificates_Validity O.Validation_Data_Conformity
FPT_TDC.1/Tanúsítvány visszavonási adat	O.Certification_Path O.Certificates_Conformity O.Certificates_Validity O.Validation_Data_Conformity
FDP_IFC.1/Elektronikus aláírás ellenőrzés	O.Validation_Data_Export
FDP_IFF.1/Elektronikus aláírás ellenőrzés	O.Validation_Data_Export
FMT_MSA.3/Aláírás ellenőrzés állapot	O.Validation_Data_Export
FMT_MSA.1/Aláírás ellenőrzés állapot	O.Validation_Data_Export
FDP_ETC.2/Ellenőrzési állapot	O.Validation_Data_Export
FCS_COP.1/Aláírás ellenőrzés	O.Cryptographic_Operations
FCS_COP.1/Hash függvény	O.Cryptographic_Operations
FMT_SMR.1	O.Administration
FMT_MTD.1/Az aláírási szabályzat részleges kezelése	O.Administration
FMT_SMF.1/Az aláírási szabályzat részleges kezelése	O.Administration

6.7. táblázat: Az aláírás ellenőrzésére vonatkozó funkcionális követelmények lefedettsége a TOE biztonsági célokkal

6.3.3 Függőségek az aláírás létrehozás funkcionális biztonsági követelményei között

6.3.3.1 Kielégített függőségek

Követelmények	CC függőségek	Kielégített függőségek
FDP_IFC.1/Dokumentum elfogadás	FDP_IFF.1	FDP_IFF.1/Dokumentum elfogadás
FDP_IFF.1/Dokumentum elfogadás	FDP_IFC.1 és FMT_MSA.3	FDP_IFC.1/Dokumentum elfogadás FMT_MSA.3/Dokumentum elfogadás
FDP_ITC.1/Dokumentum elfogadás	(FDP_ACC.1vagy FDP_IFC.1) és FMT_MSA.3	FDP_IFC.1/Dokumentum elfogadás FMT_MSA.3/Dokumentum elfogadás
FMT_MSA.3/Dokumentum elfogadás	FMT_ MSA.1 és FMT_SMR.1	FMT_SMR.1 FMT_MSA.1/Kiválasztott dokumentumok FMT_MSA.1/Dokumentum szemantika stabilitás állapota
FMT_MSA.1/Kiválasztott dokumentumok	(FDP_ACC.1vagy FDP_IFC.1) és FMT_SMF.1 és FMT_SMR.1	FDP_IFC.1/Dokumentum elfogadás FMT_SMF.1/Egy dokumentum lista kiválasztása, FMT_SMR.1
FMT_SMF.1/Egy dokumentum lista kiválasztása	nincs függőség	
FMT_MSA.1/Dokumentum szemantika stabilitás állapota	(FDP_ACC.1vagy FDP_IFC.1) és FMT_SMF.1 és FMT_SMR.1	FDP_IFC.1/Dokumentum elfogadás FMT_SMF.1/A dokumentum stabilitás állapot megszerzése FMT_SMR.1
FMT_SMF.1/A dokumentum stabilitás állapot meghatározása	nincs függőség	
FMT_MSA.1/Az aláíró egyetértése nem stabil dokumentum aláírására	(FDP_ACC.1vagy FDP_IFC.1) és FMT_SMF.1 és FMT_SMR.1	FDP_IFC.1/Dokumentum elfogadás FMT_SMF.1/Az aláíró egyetértésének megszerzése nem stabil dokumentum aláírására, FMT_SMR.1
FMT_SMF.1/Az aláíró egyetértésének megszerzése nem stabil dokumentum aláírására	nincs függőség	
FDP_ROL.2/Az aláírási folyamat megszakítása	FDP_ACC.1vagy FDP_IFC.1	FDP_IFC.1/Aláírás létrehozás
FMT_MSA.1/Aláírási tulajdonságok	(FDP_ACC.1vagy FDP_IFC.1) és FMT_SMF.1 és FMT_SMR.1	FDP_IFC.1/Aláírás létrehozás FMT_SMF.1/Az aláírási tulajdonságok módosítása, FMT_SMR.1
FMT_SMF.1/Az aláírási tulajdonságok módosítása	nincs függőség	
FDP_IFC.1/Az aláíró tanúsítványának importálása	FDP_IFF.1	FDP_IFF.1/Az aláíró tanúsítványának importálása
FDP_IFF.1/Az aláíró tanúsítványának importálása	FDP_IFC.1 és FMT_MSA.3	FDP_IFC.1/Az aláíró tanúsítványának importálása FMT_MSA.3/Az aláíró tanúsítványának importálása
FMT_MSA.3/Az aláíró tanúsítványának importálása	FMT_ MSA.1 és FMT_SMR.1	FMT_MSA.1/Az aláíró tanúsítványa FMT_SMR.1
FMT_MSA.1/Az aláíró tanúsítványa	(FDP_ACC.1vagy FDP_IFC.1) és	FDP_IFC.1/Az aláíró tanúsítványának importálása

	FMT_SMF.1 és FMT_SMR.1	FMT_SMF.1/Az aláíró tanúsítványának kiválasztása FMT_SMR.1
FDP_ITC.2/Az aláíró tanúsítványa	(FDP_ACC.1vagy FDP_IFC.1) FPT_TDC.1 és **(FTP_ITC.1vagy FTP_TRP.1)**	FDP_IFC.1/Az aláíró tanúsítványa FPT_TDC.1/Az aláíró tanúsítványa **Lásd 6.3.3.2**
FPT_TDC.1/Az aláíró tanúsítványa	nincs függőség	
FMT_SMF.1/Az aláíró tanúsítványának kiválasztása	nincs függőség	
FDP_IFC.1/Aláírás létrehozás	FDP_IFF.1	FDP_IFF.1/Aláírás létrehozás
FDP_IFF.1/Aláírás létrehozás	FDP_IFC.1 és FMT_MSA.3	FDP_IFC.1/Aláírás létrehozás FMT_MSA.3/Aláírás létrehozás
FMT_MSA.3/Aláírás létrehozás	FMT_MSA.1 és FMT_SMR.1	FMT_SMR.1 FMT_MSA.1/Aláírási tulajdonságok FMT_MSA.1/Az aláíró tanúsítványa
FDP_ITC.1/Az aláíró közvetlen egyetértése	(FDP_ACC.1vagy FDP_IFC.1) és FMT_MSA.3	FDP_IFC.1/Aláírás létrehozás FMT_MSA.3/Aláírás létrehozás
FDP_IFC.1/Elektronikus aláírás exportálása	FDP_IFF.1	FDP_IFF.1/Elektronikus aláírás exportálása
FDP_IFF.1/Elektronikus aláírás exportálása	FDP_IFC.1 és FMT_MSA.3	FDP_IFC.1/Elektronikus aláírás exportálása FMT_MSA.3/Elektronikus aláírás exportálása
FDP_ETC.2/Elektronikus aláírás exportálása	FDP_ACC.1vagy FDP_IFC.1	FDP_IFC.1/Elektronikus aláírás exportálása
FMT_MSA.3/Elektronikus aláírás exportálása	FMT_ MSA.1 és FMT_SMR.1	FMT_MSA.1/Az SCDev aláírás létrehozás állapota FMT_SMR.1
FMT_MSA.1/Az SCDev aláírás létrehozás állapota	(FDP_ACC.1vagy FDP_IFC.1) és FMT_SMF.1 és FMT_SMR.1	FDP_IFC.1/Elektronikus aláírás exportálása FMT_SMF.1/Az SCDev aláírás létrehozás állapotának lekérdezése FMT_SMR.1
FMT_SMF.1/Az SCDev aláírás létrehozás állapotának lekérdezése	nincs függőség	-
FCS_COP.1/Hash függvény	**(FCS_CKM.1 vagy FDP_ITC.1 vagy FDP_ITC.2) és FCS_CKM.4**	**Lásd 6.3.3.2**
FMT_SMR.1	FIA_UID.1	**Lásd 6.3.3.**2
FMT_MTD.1/Dokumentum formátum/megjelenítő összerendelés tábla	FMT_SMF.1 és FMT_SMR.1	FMT_SMF.1/A dokumentum formátum/megjelenítő összerendelés tábla kezelése, FMT_SMR.1
FMT_SMF.1/A dokumentum formátum/megjelenítő összerendelés tábla kezelése	nincs függőség	
FMT_MTD.1/Az aláírási szabályzatok kezelése	FMT_SMF.1 és FMT_SMR.1	FMT_SMF.1/Az aláírási szabályzatok kezelése, FMT_SMR.1
FMT_SMF.1/Az aláírási szabályzatok kezelése	nincs függőség	

6.8. táblázat: Kielégített függőségek az aláírás létrehozás funkcionális biztonsági követelményei között

6.3.3.2 A nem teljesített függőségek indoklása

Az **FDP_ITC.2/Az aláíró tanúsítványa** követelmény alábbi függősége nem teljesül: **FTP_ITC.1vagy FTP_TRP.1**.
A függőségek teljesítése azért hiányzik, mert a nyilvános kulcsú infrastruktúrában használt protokoll önvédelmet garantál, ha nem is azonnal, de az aláírás ellenőrzésekor:

- A tanúsítványlánc tanúsítványainak sértetlenségét az aláírási szabályzatban meghatározott önaláírt tanúsítvány (megbízható pont) garantálja, melynek sértetlenségét a TOE környezete biztosítja.
- Az aláírás ellenőrzése során egy érvényes tanúsítványlánc felépítése az aláíró tanúsítványa és egy az aláírási szabályzatban meghatározott megbízható pont között garantálja a láncot alkotó különböző tanúsítványok eredetlének hitelességét.
- Végül az aláíró tanúsítványa nem igényel bizalmasság elleni védelmet.

Az **FCS_COP.1/Hash függvény** követelmény alábbi függősége nem teljesül: **(FCS_CKM.1 vagy FDP_ITC.1 vagy FDP_ITC.2) és FCS_CKM.4**
A függőségek teljesítése azért hiányzik, mert a hash függvény egy olyan speciális kriptográfiai algoritmus, amely nem igényelsem kulcs generálást, sem kulcsok TOE-ba importálását.

Az **FMT_SMR.1** követelmény alábbi függősége nem teljesül: **FIA_UID.1**
A függőség teljesítése azért hiányzik, mert a TOE az operációs rendszertől várja el az aláíró és/vagy ellenőrző szerepköröket betölteni kívánó felhasználó azonosítását.

6.3.4 Függőségek az aláírás ellenőrzés funkcionális biztonsági követelményei között

6.3.4.1 Kielégített függőségek

Követelmények	CC függőségek	Kielégített függőségek
FDP_IFC.1/Dokumentum elfogadás	FDP_IFF.1	FDP_IFF.1/Dokumentum elfogadás
FDP_IFF.1/Dokumentum elfogadás	FDP_IFC.1 és FMT_MSA.3	FDP_IFC.1/Dokumentum elfogadás FMT_MSA.3/Dokumentum elfogadás
FDP_ITC.1/Dokumentum elfogadás	(FDP_ACC.1vagy FDP_IFC.1) és FMT_MSA.3	FDP_IFC.1/Dokumentum elfogadás FMT_MSA.3/Dokumentum elfogadás
FMT_MSA.3/Dokumentum elfogadás	FMT_ MSA.1 és FMT_SMR.1	FMT_MSA.1/Dokumentum szemantika stabilitás állapota, FMT_SMR.1
FMT_MSA.1/Dokumentum szemantika stabilitás állapota	(FDP_ACC.1vagy FDP_IFC.1) és FMT_SMF.1 és FMT_SMR.1	FDP_IFC.1/Dokumentum elfogadás FMT_SMF.1/A dokumentum stabilitás állapot megszerzése, FMT_SMR.1
FMT_SMF.1/A dokumentum stabilitás állapot meghatározása	nincs függőség	
FMT_SMF.1/Az alkalmazandó aláírási szabályzat kiválasztása	nincs függőség	
FMT_MTD.1/Az alkalmazandó aláírási szabályzat kiválasztása	FMT_SMF.1 és FMT_SMR.1	FMT_SMF.1/Az alkalmazandó aláírási szabályzat kiválasztása, FMT_SMR.1
FDP_IFC.1/Elektronikus aláírás	FDP_IFF.1	FDP_IFF.1/Elektronikus aláírás
FDP_IFF.1/Elektronikus aláírás	FDP_IFC.1 és FMT_MSA.3	FDP_IFC.1/Elektronikus aláírás FMT_MSA.3/Elektronikus aláírás
FMT_MSA.3/Elektronikus aláírás	FMT_ MSA.1 és FMT_SMR.1	FMT_MSA.1/Elektronikus aláírás FMT_SMR.1
FMT_MSA.1/Elektronikus aláírás	(FDP_ACC.1vagy FDP_IFC.1) és **FMT_SMF.1** és FMT_SMR.1	FDP_IFC.1/Elektronikus aláírás **Lásd 6.3.4.2** FMT_SMR.1
FDP_ITC.2/Elektronikus aláírás	(FDP_ACC.1vagy FDP_IFC.1) FPT_TDC.1 és **(FTP_ITC.1 vagy FTP_TRP.1)**	FDP_IFC.1/Elektronikus aláírás FPT_TDC.1/Elektronikus aláírás **Lásd 6.3.4.2**
FDP_IFC.1/Idő hivatkozás	FDP_IFF.1	FDP_IFF.1/Idő hivatkozás
FDP_IFF.1/Idő hivatkozás	FDP_IFC.1 és FMT_MSA.3	FDP_IFC.1/Idő hivatkozás FMT_MSA.3/Idő hivatkozás
FMT_MSA.3/Idő hivatkozás	FMT_ MSA.1 és FMT_SMR.1	FMT_MSA.1/Idő hivatkozás FMT_MSA.1/Tanúsítványok FMT_MSA.1/Tanúsítvány érvényesítő adatok, FMT_SMR.1
FMT_MSA.1/Idő hivatkozás	(FDP_ACC.1 vagy FDP_IFC.1) és **FMT_SMF.1** és FMT_SMR.1	FDP_IFC.1/Idő hivatkozás **Lásd 6.3.4.2** FMT_SMR.1

Követelmények	CC függőségek	Kielégített függőségek
FDP_ITC.2/Idő hivatkozás	(FDP_ACC.1vagy FDP_IFC.1) FPT_TDC.1 és **(FTP_ITC.1vagy FTP_TRP.1)**	FDP_IFC.1/Idő hivatkozás FPT_TDC.1/Idő hivatkozás FPT_TDC.1/Tanúsítványok FPT_TDC.1/Tanúsítvány visszavonási adatok **Lásd 6.3.4.2**
FMT_MSA.1/Tanúsítványok	(FDP_ACC.1vagy FDP_IFC.1) és **FMT_SMF.1** és FMT_SMR.1	FDP_IFC.1/Tanúsítványlánc **Lásd 6.3.4.2** FMT_SMR.1
FMT_MSA.1/Tanúsítvány érvényesítő adatok	(FDP_ACC.1vagy FDP_IFC.1) és **FMT_SMF.1** és FMT_SMR.1	FDP_IFC.1/Tanúsítványlánc **Lásd 6.3.4.2** FMT_SMR.1
FDP_IFC.1/Tanúsítványlánc	FDP_IFF.1	FDP_IFF.1/Tanúsítványlánc
FDP_IFF.1/Tanúsítványlánc	FDP_IFC.1 és FMT_MSA.3	FDP_IFC.1/Tanúsítványlánc FMT_MSA.3/Tanúsítványlánc
FMT_MSA.3/Tanúsítványlánc	FMT_SMR.1és FMT_MSA.1	FMT_SMR.1 FMT_MSA.1/Tanúsítványok FMT_MSA.1/Tanúsítvány érvényesítő adatok
FDP_ITC.2/Tanúsítványlánc	(FDP_ACC.1vagy FDP_IFC.1) FPT_TDC.1 és **(FTP_ITC.1 vagy FTP_TRP.1)**	FDP_IFC.1/Tanúsítványlánc FPT_TDC.1/Tanúsítványok FPT_TDC.1/Tanúsítvány visszavonási adatok **Lásd 6.3.4.2**
FPT_TDC.1/Elektronikus aláírás	nincs függőség	
FPT_TDC.1/Idő hivatkozás	nincs függőség	
FPT_TDC.1/Tanúsítványok	nincs függőség	
FPT_TDC.1/Tanúsítvány visszavonási adat	nincs függőség	
FDP_IFC.1/Elektronikus aláírás ellenőrzés	FDP_IFF.1	FDP_IFF.1/Elektronikus aláírás ellenőrzés
FDP_IFF.1/Elektronikus aláírás ellenőrzés	FDP_IFC.1 és FMT_MSA.3	FDP_IFC.1/Elektronikus aláírás ellenőrzés FMT_MSA.3/Elektronikus aláírás ellenőrzés
FMT_MSA.3/Aláírás ellenőrzés állapot	FMT_SMR.1 és FMT_MSA.1	FMT_SMR.1 FMT_MSA.1/Aláírás ellenőrzés állapot
FMT_MSA.1/Aláírás ellenőrzés állapot	(FDP_ACC.1 vagy FDP_IFC.1) és **FMT_SMF.1** és FMT_SMR.1	FDP_IFC.1/Elektronikus aláírás ellenőrzés **Lásd 6.3.4.2** FMT_SMR.1
FDP_ETC.2/Ellenőrzési állapot	FDP_ACC.1vagy FDP_IFC.1	FDP_IFC.1/Elektronikus aláírás ellenőrzés
FCS_COP.1/Aláírás ellenőrzés	(FCS_CKM.1 vagy FDP_ITC.1 vagy FDP_ITC.2) és **FCS_CKM.4**	FDP_ITC.2/Tanúsítványlánc **Lásd 6.3.4.2**

FCS_COP.1/Hash függvény	**(FCS_CKM.1 vagy FDP_ITC.1 vagy FDP_ITC.2) és FCS_CKM.4**	**Lásd 6.3.4.2** **Lásd 6.3.4.2**
FMT_SMR.1	FIA_UID.1	**Lásd 6.3.4.2**
FMT_MTD.1/Az aláírási szabályzat részleges kezelése	FMT_SMF.1 és FMT_SMR.1	FMT_SMF.1/Az aláírási szabályzat részleges kezelése FMT_SMR.1
FMT_SMF.1/Az aláírási szabályzat részleges kezelése	nincs függőség	

6.9. táblázat: Kielégített függőségek
az aláírás ellenőrzés funkcionális biztonsági követelményei között

6.3.4.2 A nem teljesített függőségek indoklása

Az **FMT_MSA.1/Elektronikus aláírás** alábbi függősége nem teljesül: **FMT_SMF.1**
Mivel az FMT_MSA.1/Elektronikus aláírás követelmény nem határoz meg a biztonsági jellemzőkre egy új menedzsment tulajdonságot, ezért a függőséget nem kell teljesíteni.

Az **FDP_ITC.2/Elektronikus aláírás** alábbi függősége nem teljesül: **FTP_ITC.1 vagy FTP_TRP.1**
A függőségek teljesítése azért hiányzik, mert:

- ezek az adatok nem igényelnek bizalmasság elleni védelmet;
- az elektronikus aláírásba foglalt digitális aláírás érvényessége garantálja az összes aláírt adat sértetlenségét;
- végül az elektronikus aláírás érvényessége (amennyiben az ellenőrzési folyamat vége kimutatja ezt) bizonyítja az információk eredetének hitelességét.

Az **FMT_MSA.1/Idő hivatkozás** alábbi függősége nem teljesül: **FMT_SMF.1**
Mivel az FMT_MSA.1/Idő hivatkozás követelmény nem határoz meg a biztonsági jellemzőkre egy új menedzsment tulajdonságot, ezért a függőséget nem kell teljesíteni.

Az **FDP_ITC.2/Idő hivatkozás** alábbi függősége nem teljesül: **FTP_ITC.1 vagy FTP_TRP.1**
A függőségek teljesítése azért hiányzik, mert a nyilvános kulcsú infrastruktúrában használt protokoll önvédelmet garantál:

- Az idő hivatkozás sértetlenségét a hozzá kapcsolódó digitális aláírás garantálja.
- Az idő hivatkozás hitelességét egy érvényes tanúsítványlánc felépítése garantálja az időbélyegző egység kulcsa és egy az aláírási szabályzatban meghatározott, az időbélyegző egységhez rendelt megbízható pont között.
- Végül a TOE által kapott adatok nem igényelnek védelmet a bizalmasság szempontjából.

Az **FMT_MSA.1/Tanúsítványok** alábbi függősége nem teljesül: **FMT_SMF.1**
Mivel az FMT_MSA.1/Tanúsítványok követelmény nem határoz meg a biztonsági jellemzőkre egy új menedzsment tulajdonságot, ezért a függőséget nem kell teljesíteni.

Az **FMT_MSA.1/Tanúsítvány érvényesítő adatok** alábbi függősége nem teljesül: **FMT_SMF.1**
Mivel az FMT_MSA.1/Tanúsítvány érvényesítő adatok követelmény nem határoz meg a biztonsági jellemzőkre egy új menedzsment tulajdonságot, ezért a függőséget nem kell teljesíteni.

Az **FDP_ITC.2/Tanúsítványlánc** alábbi függősége nem teljesül: **FTP_ITC.1 vagy FTP_TRP.1**
A függőségek teljesítése azért hiányzik, mert a nyilvános kulcsú infrastruktúrában használt protokoll önvédelmet garantál:

- A tanúsítványlánc összes tanúsítványának és a visszavonási információk sértetlenségét egy szolgáltatói digitális aláírás garantálja, ahol az önaláírt gyökér tanúsítványra az aláírási szabályzat hivatkozik (melynek sértetlenségét a TOE megvédi).
- A tanúsítványláncot alkotó tanúsítványok hitelességét egy érvényes tanúsítványlánc felépítése garantálja az aláíró tanúsítványa és egy az aláírási szabályzatban meghatározott megbízható pont között.
- A TOE által kapott adatok nem igényelnek védelmet a bizalmasság szempontjából.

Az **FMT_MSA.1/Aláírás ellenőrzés állapot** alábbi függősége nem teljesül: **FMT_SMF.1**
Mivel az FMT_MSA.1/Elektronikus aláírás ellenőrzés állapot követelmény nem határoz meg a biztonsági jellemzőkre egy új menedzsment tulajdonságot, ezért a függőséget nem kell teljesíteni.

Az **FCS_COP.1/Aláírás ellenőrzés** alábbi függősége nem teljesül: **FCS_CKM.4**.
A függőségek teljesítése azért hiányzik, mert a használt kulcs egy nyilvános kulcs, így nem igényel jóváhagyott módszer szerinti megsemmisítést.

Az **FCS_COP.1/Hash függvény** alábbi függősége nem teljesül: **FCS_CKM.1 vagy FDP_ITC.1 vagy FDP_ITC.2.**
A függőségek teljesítése azért hiányzik, mert a hash függvény egy olyan speciális kriptográfiai algoritmus, amely nem igényel sem kulcs generálást, sem kulcsok TOE-ba importálását.

Az **FMT_SMR.1** követelmény alábbi függősége nem teljesül: **FIA_UID.1**
A függőség teljesítése azért hiányzik, mert a TOE az operációs rendszertől várja el az aláíró és/vagy ellenőrző szerepköröket betölteni kívánó felhasználó azonosítását.

6.4 A garanciális biztonsági követelmények indoklása

6.4.1 Az EAL3 garanciaszint indoklása

A TOE értékelés garanciaszintje EAL3. Ez kellő védelmet nyújt alapszintű támadási potenciállal rendelkező támadók ellen, mérsékelt kockázati profilú környezetekben.

6.4.2 Az EAL3 garanciaszint függőségei

A 6.10 táblázatból látható, hogy valamennyi függőség teljesül.

Követelmények	CC függőségek	Kielégített függőségek
ADV_ARC.1	ADV_FSP.1 és ADV_TDS.1	ADV_FSP.3, ADV_TDS.2
ADV_FSP.3	ADV_TDS.1	ADV_TDS.2
ADV_TDS.2	ADV_FSP.3	ADV_FSP.3
AGD_OPE.1	ADV_FSP.1	ADV_FSP.3
AGD_PRE.1	nincs függőség	
ALC_CMC.3	ALC_CMS.1 és ALC_DVS.1 és ALC_LCD.1	ALC_CMS.3, ALC_DVS.1, ALC_LCD.1
ALC_CMS.3	nincs függőség	
ALC_DEL.1	nincs függőség	
ALC_DVS.1	nincs függőség	
ALC_LCD.1	nincs függőség	
ASE_CCL.1	ASE_ECD.1 és ASE_INT.1 és ASE_REQ.1	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	nincs függőség	
ASE_INT.1	nincs függőség	
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1
ASE_REQ.2	ASE_ECD.1 és ASE_OBJ.2	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	nincs függőség	
ASE_TSS.1	ADV_FSP.1 és ASE_INT.1 és ASE_REQ.1	ADV_FSP.3, ASE_INT.1, ASE_REQ.2
ATE COV.2	ADV_FSP.2 és ATE_FUN.1	ADV_FSP.3, ATE_FUN.1
ATE_FUN.1	ATE COV.1	ATE COV.2
ATE_IND.2	ADV FSP.2 és AGD_OPE.1 és AGD_PRE.1 és ATE_COV.1 és ATE_FUN.1	ADV FSP.3, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
ATE_DPT.1	ADV_ARC.1 és ADV_TDS.2 és ATE_FUN.1	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1
AVA_VAN.2	ADV_ARC.1 és ADV_FSP.2 és ADV TDS.1 és AGD_OPE.1 és AGD_PRE.1	ADV_ARC.1, ADV_FSP.3, ADV_ TDS.2, AGD_OPE.1, AGD_PRE.1

6.10. táblázat: A garanciális biztonsági követelmények függőségei

7 TOE összefoglaló előírás

7.1 A funkcionális követelmények teljesítési módja

Az E-Magic az aláíró számára a főmenü „Konfiguráció” felületén elérhető funkciókkal biztosítja az alábbi SFR-eket:

- **Aláírási tulajdonságok beállítása (Beállítás\Aláírás):**
  - FMT_MSA.1/Aláírási tulajdonságok
  - FMT_SMF.1/Az aláírási tulajdonságok módosítása
  - FMT_SMF.1/Az aláíró tanúsítványának kiválasztása
- **A dokumentummal kapcsolatos konfigurációk (Beállítás\Dokumentum):**
  - FMT_MTD.1/Dokumentum formátum/megjelenítő összerendelés tábla
  - FMT_SMF.1/A dokumentum formátum/megjelenítő összerendelés tábla kezelése
- **Aláírási szabályzat beállítása (Beállítás\Időbélyeg szerver és Beállítás\OCSP):**
  - FMT_MTD.1/Az aláírási szabályzatok kezelése
  - FMT_SMF.1/Az aláírási szabályzatok kezelése

Az E-Magic az aláíró számára a főmenü „Parancsok” \ „Fájl aláíró” felületén elérhető funkciókkal biztosítja az alábbi SFR-eket:

- **Belépés a Fájl aláíró felületre:**
  - FMT_SMR.1
- **Az aláírandó dokumentum(ok) kiválasztása:**
  - FDP_IFC.1/Dokumentum elfogadás
  - FDP_IFF.1/Dokumentum elfogadás
  - FDP_ITC.1/Dokumentum elfogadás
  - FMT_MSA.3/Dokumentum elfogadás
  - FMT_MSA.1/Kiválasztott dokumentumok
  - FMT_SMF.1/Egy dokumentum lista kiválasztása
- **Az aláírandó dokumentum(ok) megtekintése:**
  - FMT_MSA.1/Dokumentum szemantika stabilitás állapota
  - FMT_SMF.1/A dokumentum stabilitás állapot meghatározása
  - FMT_MSA.1/Az aláíró egyetértése nem stabil dokumentum aláírására
  - FMT_SMF.1/Az aláíró egyetértésének megszerzése nem stabil dokumentum aláírására
- **Aláíró tanúsítvány kiválasztása:**
  - FDP_IFC.1/Az aláíró tanúsítványának importálása
  - FDP_IFF.1/Az aláíró tanúsítványának importálása
  - FMT_MSA.3/Az aláíró tanúsítványának importálása
  - FMT_MSA.1/Az aláíró tanúsítványa
  - FDP_ITC.2/Az aláíró tanúsítványa
  - FPT_TDC.1/Az aláíró tanúsítványa
  - FMT_SMF.1/Az aláíró tanúsítványának kiválasztása
- **Az aláírás közvetlen kiváltása (vagy megszakítása):**
  - FDP_ITC.1/Az aláíró közvetlen egyetértése
  - FDP_ROL.2/Az aláírási folyamat megszakítása
  - FCS_COP.1/Hash függvény
  - FMT_MSA.1/Az SCDev aláírás létrehozás állapota
  - FMT_SMF.1/Az SCDev aláírás létrehozás állapotának lekérdezése
  - FDP_IFC.1/Aláírás létrehozás
  - FDP_IFF.1/Aláírás létrehozás
  - FMT_MSA.3/Aláírás létrehozás
- **Az aláírás eredményének megtekintése:**
  - FDP_IFC.1/Elektronikus aláírás exportálása
  - FDP_IFF.1/ Elektronikus aláírás exportálása
  - FDP_ETC.2/Elektronikus aláírás exportálása
  - FMT_MSA.3/Elektronikus aláírás exportálása

Az E-Magic az ellenőrző számára a főmenü „Konfiguráció” felületén elérhető funkciókkal biztosítja az alábbi SFR-eket:

- **Aláírási szabályzat beállítása (Beállítás\Időbélyeg szerver és Beállítás\OCSP):**
  - FMT_MTD.1/Az aláírási szabályzat részleges kezelése
  - FMT_SMF.1/Az aláírási szabályzat részleges kezelése
  - FMT_SMF.1/Az alkalmazandó aláírási szabályzat kiválasztása
  - FMT_MTD.1/Az alkalmazandó aláírási szabályzat kiválasztása

Az E-Magic az ellenőrző számára a főmenü „Parancsok” \ „Ellenőrző” felületén elérhető funkciókkal biztosítja az alábbi SFR-eket:

- **Belépés az Ellenőrző felületre:**
  - FMT_SMR.1
- **Az ellenőrizendő állomány kiválasztása:**
  - FDP_IFC.1/Dokumentum elfogadás
  - FDP_IFF.1/Dokumentum elfogadás
  - FDP_ITC.1/Dokumentum elfogadás
  - FMT_MSA.3/Dokumentum elfogadás
- **Az ellenőrizendő állomány megtekintése:**
  - FMT_MSA.1/Dokumentum szemantika stabilitás állapota
  - FMT_SMF.1/A dokumentum stabilitás állapot meghatározása
- **Az elektronikus aláírás beolvasásása:**
  - FDP_IFC.1/Elektronikus aláírás
  - FDP_IFF.1/ Elektronikus aláírás
  - FMT_MSA.3/Elektronikus aláírás
  - FMT_MSA.1/Elektronikus aláírás
  - FDP_ITC.2/Elektronikus aláírás
  - FPT_TDC.1/Elektronikus aláírás
- **Az aláírás ellenőrzése – digitális aláírás ellenőrzés**
  - FCS_COP.1/Aláírás ellenőrzés
  - FCS_COP.1/Hash függvény
- **Az aláírás ellenőrzése – tanúsítványlánc felépítés**
  - FMT_MSA.1/Tanúsítványok
  - FPT_TDC.1/Tanúsítványok
  - FDP_IFC.1/Tanúsítványlánc
  - FDP_IFF.1/Tanúsítványlánc
  - FMT_MSA.3/Tanúsítványlánc
  - FDP_ITC.2/Tanúsítványlánc
- **Az aláírás ellenőrzése –tanúsítványlánc validálása**
  - FMT_MSA.1/Tanúsítványérvényesítő adatok
  - FPT_TDC.1/Tanúsítvány visszavonási adat
- **Az aláírás ellenőrzése – időbélyeg(ek) ellenőrzése**
  - FDP_IFC.1/Idő hivatkozás
  - FDP_IFF.1/Idő hivatkozás
  - FMT_MSA.3/Idő hivatkozás
  - FMT_MSA.1/Idő hivatkozás
  - FDP_ITC.2/Idő hivatkozás
  - FPT_TDC.1/Idő hivatkozás
- **Az aláírás ellenőrzése – Xades típus váltással**
  - FDP_IFC.1/Elektronikus aláírás ellenőrzés
  - FDP_IFF.1/Elektronikus aláírás ellenőrzés
- **Az aláírás ellenőrzés eredményének visszaadása:**
  - FMT_MSA.3/Aláírás ellenőrzés állapot
  - FMT_MSA.1/Aláírás ellenőrzés állapot
  - FDP_ETC.2/Ellenőrzési állapot

7.2 A fizikai és a logikai hamisítás elleni védelem

A fizikai és a logikai hamisítás elleni védelmet az E-Magic + XadesMagic a környezetétől várja el (lásd a biztonsági előirányzat A.Host_Platform feltételezését):

- a hoszt gép hardver, szoftver és förmver elemei védve vannak a jogosulatlan fizikai módosításokkal szemben;
- a hoszt védett a vírustámadásokkal szemben;
- a hoszt platform és nyílt hálózati kapcsolattal rendelkező egyéb IT elemek közötti kommunikáció tűzfallal védett;
- a hoszt platform adminisztrátori funkcióihoz való hozzáférés a platform adminisztrátorokra korlátozott ("hoszt adminisztrátor"). A felhasználói fiók különbözik a hoszt adminisztrátoritól.
- a hoszt platform szoftverének telepítése és frissítése a hoszt adminisztrátor ellenőrzése alatt áll;
- a hoszt platform operációs rendszere nem engedi nem megbízható alkalmazások végrehajtását.

7.3 A megkerülés elleni védelem

Az E-Magic biztonsági funkciói megkerülése ellen az alábbi módon védekezik:

- a felhasználó (aláíró/ellenőrző) által beállítható értékek döntő többségét a felhasználó csak kiválaszthatja az alkalmazás által felkínált lehetőségek közül,
- a felhasználó (aláíró/ellenőrző) által közvetlenül megadható értékek (pl. URI cím) feldolgozás előtt szintaktikai ellenőrzésre kerülnek.

A XadesMagic biztonsági funkciói megkerülése ellen az alábbi módon védekezik:

- a publikus paraméterekkel kívülről is meghívható függvények feldolgozás előtt ellenőrzik a paraméterek típusának és értékének megfelelőségét.

8 Rövidítések

A.x	Assumptions	feltételezések
API	Application Programming Interface	alkalmazás programozói interfész
ARL	Authority Revocation List	szolgáltató visszavonási lista
CA	Certification Authority	hitelesítés-szolgáltató
CC	Common Criteria	közös szempontok
CEN	Comité Europeen de Normalization	Európai Szabványügyi Hivatal
CRL	Certificate Revocation List	tanúsítvány visszavonási lista
CSP	Cryptographic Service Provider	kriptográfiai szolgáltatást biztosító
CWA	CEN Workshop Agreement	CEN munkacsoport megállapodás
DTBS	Data To Be Signed	aláírandó adat
DTBSR	Data To Be Signed Representation	aláírandó adat reprezentáns
EAL	Evaluation Assurance Level	értékelési garanciaszint
ETSI	European Telecommunications Standards Institute	Európai Távközlési Szabványosítási Intézet
MMI	Man-Machine Interface	ember – gép interfész
O.x	Objectives	(biztonsági) célok
OCSP	Online Certificate Status Protocol	valós idejű tanúsítvány állapot protokoll
OID	Object Identifier	objektum azonosító
OSP	Organization Security policy	szervezeti biztonsági szabályzat
P.x	Policies	(szervezeti biztonsági) szabályzatok
PKCS	Public Key Cryptography Standards	nyilvános kulcsú kriptográfiai szabvány
PKI	Public Key Infrastructure	nyilvános kulcsú infrastruktúra
PP	Protection profile	védelmi profil
RFC	Request for Comment	internet szabvány
SCDev	Signature Creation Device	aláírás létrehozó eszköz (ALE)
SD	Signatory's Document	aláírói dokumentum
SSCD	Secure Signature Creation Device	biztonságos aláírás létrehozó eszköz (BALE)
ST	Security Target	biztonsági előirányzat
TOE	Target of Evaluation	az értékelés tárgya
TSF	TOE Security Functionality	TOE biztonsági funkcionalitás
TSP	TOE Security Policy	TOE biztonsági szabályzata