InfoSigno AC SDK v1.0.0.6
(+ ACTest v1.0.1.4)
Attribútum tanúsítványok érvényességét ellenőrző SDK

Biztonsági előirányzat
v1.0

Verzió:	1.0
Dátum:	2010. július 19.
Fájl:	InfoSigno_AC_SDK_v1.0_ST
Minősítés:	Publikálás előtt nem nyilvános
Oldalak:	54

Tartalomjegyzék

Változás kezelés

Verzió	Dátum	Leírás	Készítette
0.01		Szerkezeti vázlat	Hunguard
0.02	2009.01.31.	Biztonsági probléma meghatározás, főbb követelménycsoportok és a TOE leírás első verziójának elkészítése	Lengyel Csaba
0.03	2009.03.16.	Követelmények elkészítése	Lengyel Csaba
0.04	2009.12.13.	Biztonsági funkciók elkészítése és a fejlesztők által biztosított dokumentációkban szereplő követelmények átvezetése	Lengyel Csaba
0.05	2009.12.15.	Értékelői megjegyzéseket figyelembe vevő, javított változat	Lengyel Csaba
0.06	2010.06.06	Kiegészített változat	Lengyel Csaba
0.07	2010.06.17.	Pontosított változat	Lengyel Csaba
0.08	2010.06.26.	Kiegészített változat	Lengyel Csaba
0.09	2010.06.28.	Véglegesítés előtti változat	Lengyel Csaba
1.0	2010.07.19	Az InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4 értékeléshez elfogadott változat	Lengyel Csaba

1 Bevezetés

Ez a fejezet dokumentum-kezelő és áttekintő információkat tartalmaz.

Az "ST hivatkozás" alfejezet egyértelműen azonosítja a biztonsági előirányzatot.

A "TOE hivatkozás" alfejezet egyértelműen azonosítja az értékelés tárgyát

.

A „TOE áttekintés” alfejezet összefoglalja a TOE használatát és fő biztonsági tulajdonságait, valamint azonosítja a TOE típusát és a TOE által megkövetelt valamennyi nem TOE hardvert/szoftvert/förmvert.

A „TOE leírás” alfejezet leírja a TOE fizikai és logikai hatókörét, valamint a TOE funkcionalitását.

1.1 ST hivatkozás

Cím:	InfoSigno AC SDK Attribútum tanúsítványok érvényességét ellenőrző SDK - Biztonsági előirányzat
Verzió szám:	1.0
Dátum:	2010.07.19.
Szerző:	Lengyel Csaba Infoscope Kft.

1.2 TOE hivatkozás

Az értékelés tárgya:	InfoSigno AC SDK Attribútum tanúsítványok érvényességét ellenőrző SDK
Az értékelés tárgya rövid neve:	InfoSigno AC SDK InfoSigno ACTest
Verzió szám:	InfoSigno AC SDK: 1.0.0.6 InfoSigno ACTest: 1.0.1.4
Dátum:	2010 07.19
Szponzor szervezet:	Infoscope Kft.
Garanciaszint:	MIBÉTS kiemelt (CC EAL4)
Kulcsszavak:	Nyilvános kulcsú infrastruktúra (PKI), attribútum tanúsítvány (AC)

1.3 TOE áttekintés

Jelen biztonsági előirányzat egy C++ szoftverkönyvtár és egy erre épülő web alapú alkalmazás biztonsági szolgáltatásait és az ezekre vonatkozó követelményeket írja le.

A szoftverkönyvtár (InfoSigno AC SDK v1.0.0.4) felhasználásával attribútum tanúsítványok (AC-k) érvényessége ellenőrizhető.

Az alkalmazás (InfoSigno ACTest v1.0.1.4) segítségével az InfoSigno AC SDK összes funkciója kipróbálható, ellenőrizhető és tesztelhető.

Az InfoSigno AC SDK célja, hogy egyszerűen kezelhető fejlesztői eszközt biztosítson azok számára, akik szabványos attribútum tanúsítványokon alapuló rendszereket vagy megoldásokat kívánnak fejleszteni. Az InfoSigno AC SDK nem önálló alkalmazás, hanem egy olyan komponens, amely más alkalmazásokba építve támogatja az attribútum tanúsítványok kezelését.

Az alábbi funkciók tartoznak az InfoSigno AC SDK v1.0.0.4 szolgáltatásai közé:

- Szabványos attribútum tanúsítvány beolvasása
- Attribútum tanúsítvány érvényesség ellenőrzése, és ebből következően az alábbi alfunkciók:
    - A kapcsolódó nyilvános kulcs tanúsítványok feldolgozása, tanúsítási útvonalak érvényesség ellenőrzése, CRL és OCSP feldolgozás
    - A tanúsítványokon lévő aláírások ellenőrzése (a tanúsítási útvonal nyilvános kulcs tanúsítványain és az attribútum tanúsítványon lévő digitális aláírás ellenőrzése)
    - Tanúsítvány visszavonási lista feldolgozása (ACRL) az attribútum tanúsítványokra
- Attribútum tanúsítvány elemeinek .NET objektumokra történő leképzése
- Az attribútum tanúsítványban található összes mező elérhetővé tétele

Az InfoSigno AC SDK az attribútum tanúsítványok feldolgozása során az alábbi szabványokat, ajánlásokat veszi figyelembe:

- RFC 3281: An Internet Attribute Certificate Profile for Authorization
- RFC 4476: Attribute Certificate (AC) Policies Extension
- ITU-T X.509-2000 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Az IT környezet jellemzői

Az InfoSigno AC SDK függvénykönyvtárnak az alábbi informatikai elemekből álló környezetben kell működnie:

- .NET Framework 3.5,
- Windows XP Professional, Windows 2000 szerver vagy újabb verziók
- Web szerver: Internet Information Server 5.0 vagy újabb verziók
- Microsoft SQL szerver 2000 vagy újabb verziók

1.3.1 A TOE típusa

Az InfoSigno AC SDK fejlesztői programkönyvtár egy olyan speciális elektronikus aláírás termék, melynek fő funkciója az attribútum tanúsítványok (Attribute Certificate, röv.:AC) érvényességének ellenőrzése. A „speciális” jelző arra utal, hogy attribútum tanúsítványok érvényességének ellenőrzése jelenti az alapfunkcionalitást, az aláírás létrehozás nem tartozik a funkciói közé.

Az InfoSigno AC SDK olyan funkcionalitást biztosít, amellyel attribútum tanúsítványok ellenőrzése, az ellenőrzéshez érvényesítő információk feldolgozása, tanúsítási útvonal felépítése, tanúsítványok érvényességének ellenőrzése, visszavonási információk érvényesség ellenőrzése valósítható meg.

1.4 TOE leírás

Az InfoSigno AC SDK által biztosított funkcionalitás magába foglalja az alábbiakat:

- AC megfelelés ellenőrzése az RFC 3281-beli szerkezeti profil szerint, az *1.4.3 A TOE funkcionalitás* fejezetben leírt megszorításokkal;
- Az AC által megjelölt PKI tanúsítvány érvényességének ellenőrzése az RFC 5280 által meghatározott módon.

Az ellenőrzött attribútum tanúsítványok elektronikus aláíráshoz, hitelesítéshez és jogosultság ellenőrzéshez egyaránt alkalmazhatók, de ezek a funkciók nem tartoznak bele a TOE értékelés hatókörébe.

A függvénykönyvtár tartalmazza az attribútum tanúsítványok ellenőrzésével kapcsolatos függvényeket, az ellenőrző alkalmazás pedig egy olyan egyszerű alkalmazás, amely az AC érvényesség ellenőrző függvények alkalmazására épül, illetve egy megjelenítő interfészt biztosít az AC által tartalmazott attribútumok lekérdezésére.

Az InfoSigno AC SDK v1.0.0 fejlesztői függvénykönyvtár az alábbi funkciókat biztosítja a felhasználók (fejlesztők) számára:

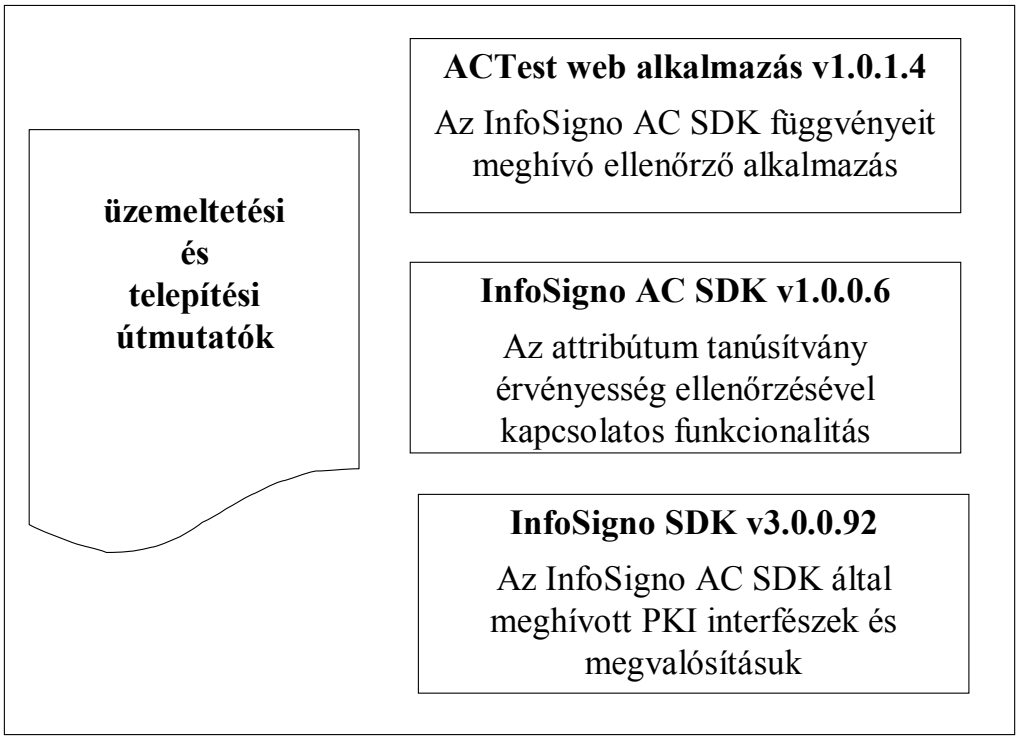
- biztonságosan kezel kulcsokat, megbízható pontokat és tanúsítványokat;
- elfogad és feldolgoz X509 v3 nyilvános kulcs és attribútum tanúsítványokat;
- ellenőrzi a nyilvános kulcs tanúsítványok érvényességét, az RFC 5280-ban leírt eljárások felhasználásával, beleértve a visszavonás ellenőrzését is;
- ellenőrzi az attribútum tanúsítványok érvényességét, az RFC 3281-ben leírt eljárások felhasználásával, beleértve a visszavonás ellenőrzését is;
- hozzáfér pontos és megbízható időforráshoz a tanúsítványok, visszavonási adatok dátumának, idejének ellenőrzése érdekében.

1.4.1 A TOE fizikai határai

Az értékelt InfoSigno AC SDK-t alkotó fizikai összetevőket szemlélteti az 1. ábra.

- InfoSigno AC SDK .NET DLL
- AC ellenőrző alkalmazás: Web alapú teszt alkalmazás az SDK összes funkciójának bemutatásához
- Fejlesztői dokumentáció, SDK leírás

Az InfoSigno AC SDK-t használó rendszer alkalmazás-hívásokkal fér hozzá a TOE által biztosított funkciókhoz. Az InfoSigno AC SDK-t használó rendszer az IT környezet része, csakúgy, mint azon hardver összetevők, melyeken az operációs rendszer és maga a TOE fut. Az IT környezet részét képezi az operációs rendszer is, amelyen az InfoSigno AC SDK működik.



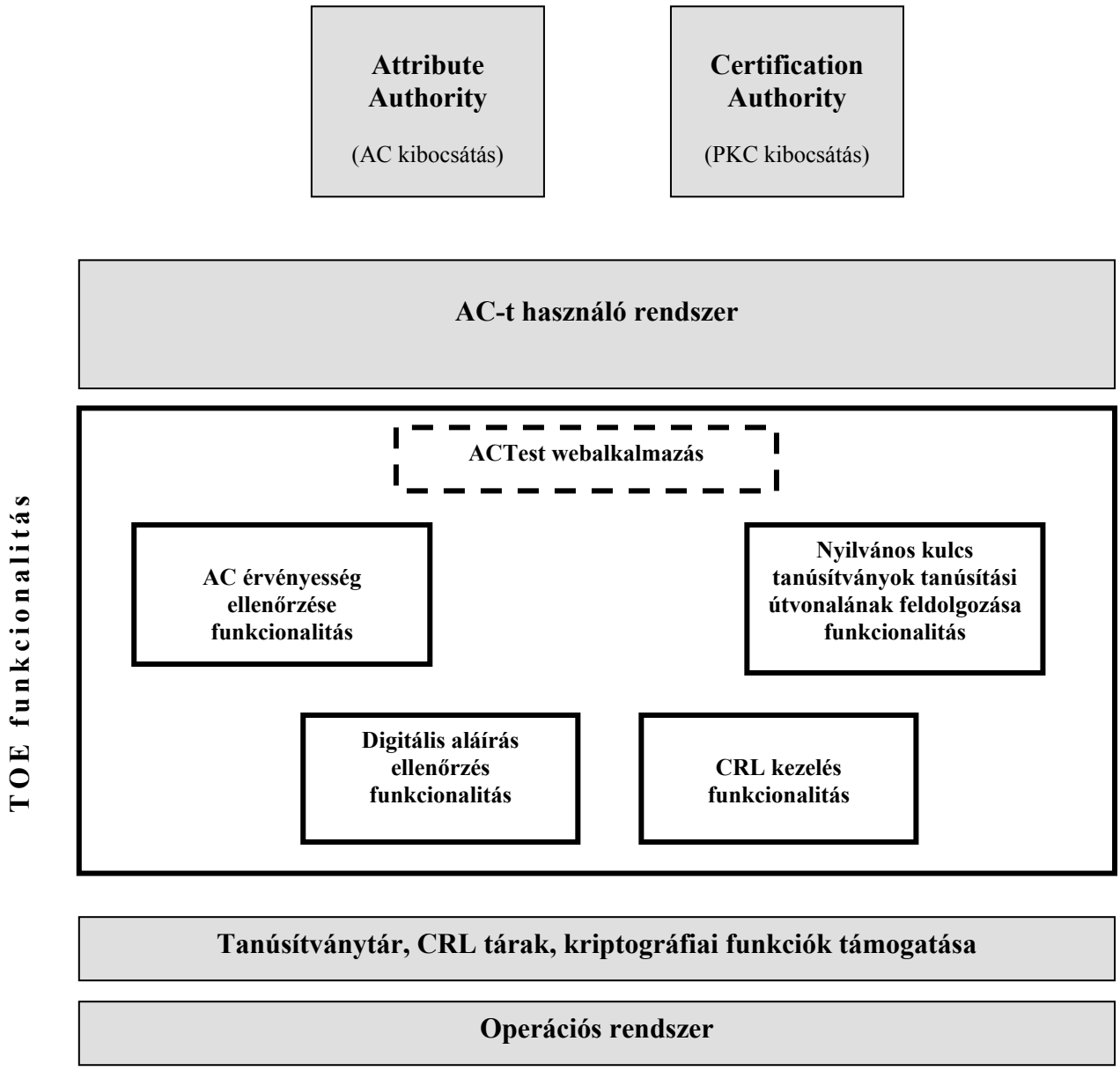
1. ábra A TOE fizikai elemei

Útmutatók:

- Az ACTest teszt website telepítői dokumentációja - Attribútum tanúsítványok érvényességét ellenőrző programkönyvtár (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4)
- Az ACTest tesztprogram felhasználói dokumentációja - Attribútum tanúsítványok érvényességét ellenőrző programkönyvtár (InfoSigno AC SDK v1.0.0.6 + ACTest v1.0.1.4)

1.4.2 A TOE logikai határai

A 2. ábra a TOE-t alkotó összetevőket mutatja azok tágabb üzemeltetési környezetébe eső más komponensekkel együtt. A szürke mezők a működtetési környezet által biztosított szolgáltatásokat jelentik, a fehér dobozok pedig a TOE logikai határaiba eső funkcionalitást mutatják.



2. ábra A TOE logikai határai és üzemeltetési környezete

A 2.ábrán látható InfoSigno AC SDK és IT környezeti alkotóelemek szerepe:

Attribute Authority: Az attribútum tanúsítványok kibocsátását végző szervezet, rendszer.
Certification Authority: Az attribútum tanúsítványokhoz kapcsolódó nyilvános kulcsú tanúsítványok (AC tulajdonos, AC kibocsátó nyilvános kulcsú tanúsítványainak) kibocsátását végző szervezet.
AC-t használó rendszer: Az attribútum tanúsítványok által tartalmazott engedélyek feldolgozását végző rendszer. Ennek bemenete a TOE által szolgáltatott érvényesség ellenőrzés eredménye, az attribútum tanúsítványban tartalmazott attribútumokkal.

A 2. ábrán látható, a TOE hatókörébe tartozó szolgáltatások részletes leírását a következő alfejezet tartalmazza.

1.4.3 A TOE funkcionalitás

A InfoSigno AC SDK által biztosított funkcionalitás az alábbiakat foglalja magába:

1. **Attribútum tanúsítvány megfelelés ellenőrzése**
   Az attribútum tanúsítvány érvényesség ellenőrzése az RFC 3281-ben specifikált szerkezeti profil szerint, az alábbi megszorításokkal:
   - az AC kibocsátás egyszintű jogosultság kiosztás alapján történik (AA alatt nem állhat másik AA)
   - az alábbi opcionális tulajdonságokat az értékelt TOE verzió nem támogatja:
     - Proxying
     - Use of ObjectDigestInfo
     - AA Controls
     - Attribute Encryption

2. **Az AC által megjelölt PKI tanúsítvány érvényességének ellenőrzése**
   Az attribútum tanúsítvány ellenőrzésében szerepet játszó nyilvános kulcsú tanúsítványok (AC tulajdonos és az AC kibocsátó nyilvános kulcs tanúsítványai) érvényesség ellenőrzése az RFC 5280 által meghatározott módon, az AC kibocsátó tanúsítványa esetén kiegészítve az RFC 3281 vonatkozó követelményeivel (RFC 3281 4.5 fejezet).

3. **Attribútum tanúsítvány eredményének visszaadása és az aláírt attribútumok megjelenítése/továbbítása**
   Ezt a funkciót az 1. ábrán látható InfoSigno AC ellenőrző alkalmazás végzi. Meghívja az InfoSigno AC SDK megfelelő funkcióit, és érvényes AC esetén megjeleníti/továbbítja az attribútumokat az azokat felhasználó IT környezeti összetevők felé.

A fenti fő funkcionalitást az alábbi szolgáltatások meghívásával hajtja végre a TOE:

Az attribútum tanúsítványokra vonatkozó visszavonás állapot (ACRL) feldolgozása

A TOE támogatja mindkét alábbi visszavonási sémát:

- „visszavonás nélküli” séma („never revoke” scheme)
- „AC-beli mutató” séma („Pointer in AC” scheme)

Az attribútum tanúsítvány visszavonási lista (ACRL) érvényesség ellenőrzése során a TOE megvizsgálja a tanúsítványok ellenőrzésében szerepet játszó ACRL-ek érvényességét. A TOE csak teljes visszavonási lista feldolgozását kezeli a tanúsítvány crlDistributionPoint kiterjesztésben mutatott lista feldolgozásával, delta CRL-eket nem kezel.

A nyilvános kulcs tanúsítványokra vonatkozó visszavonás állapot (CRL/OCSP) feldolgozása

A tanúsítvány visszavonási lista (CRL) érvényesség ellenőrzése során a TOE megvizsgálja a nyilvános kulcs tanúsítványok ellenőrzésében szerepet játszó CRL-ek érvényességét. A TOE csak teljes CRL feldolgozását kezeli a tanúsítvány crlDistributionPoint kiterjesztésben mutatott CRL feldolgozásával, delta CRL-eket nem dolgoz fel.

Az Online Certificate Status Protocol (OCSP) követelményei lehetővé teszik, hogy a TOE online tanúsítvány állapot kéréséket kezdeményezzen a nyilvános kulcs tanúsítványokra vonatkozóan, és ellenőrizze az OCSP válaszokat.

Tanúsítási útvonal érvényesség ellenőrzés szolgáltatás

A **tanúsítási útvonal érvényesség ellenőrzése** gondoskodik az attribútum tanúsítványhoz kapcsolódó nyilvános kulcs tanúsítvány (AC tulajdonos nyilvános kulcs tanúsítványának), illetve az AC kibocsátó nyilvános kulcs tanúsítványának érvényesség ellenőrzéséről. Ez a funkcionalitás a tanúsítási útvonal érvényességének ellenőrzésével és a tanúsítási útvonal felépítésével foglalkozik. A feldolgozás megfelel az RFC 5280 szabványnak.

A nyilvános kulcs tanúsítványok esetén *háromféle* tanúsítványt különböztetünk meg:
- **Megbízható pontok**: Ezek önaláírt tanúsítványok, melyek nem igényelnek semmilyen érvényesség ellenőrzést. A megbízható pont (önaláírt tanúsítvány) általában tanúsítvány formában jelenik meg. A megbízható pont elsődleges célja a megkülönböztető név (Distinguished Name), a nyilvános kulcs és az algoritmus azonosító megállapítása. A megbízható pontok hozzáadását, törlését, menedzselését az InfoSigno AC SDK hatáskörén kívül, a Windows tanúsítványtárban kell kezelni.
- **Közbenső tanúsítványok**: Ezek a hitelesítés-szolgáltatók (CA-k) számára kibocsátott tanúsítványok. Egy tanúsítási útvonal minden tanúsítványa ennek tekintendő, kivéve a megbízható pontot és a végtanúsítványt.
- **Végtanúsítvány:** A tanúsítási útvonal legutolsó tanúsítványa, melyet a szóban forgó egyed (aláíró) részére bocsátottak ki.

A nyilvános kulcs tanúsítványok érvényességének ellenőrzése során a tanúsítványhoz felépíthető teljes tanúsítási útvonalat figyelembe kell venni.

Az InfoSigno AC SDK a nyilvános kulcs tanúsítványok ellenőrzésekor a **keyUsage**, **extendedKeyUsage** és a **basicConstraints** biztonsággal kapcsolatos tanúsítvány kiterjesztési ellenőrzéseket veszi számításba.

PKI aláírás ellenőrzése szolgáltatás

A PKI aláírás ellenőrzése során az InfoSigno AC SDK feldolgozza az aláírási információkat és a nyilvános kulcsot használja az aláírás ellenőrzéséhez. A PKI aláírás ellenőrzésével kapcsolatos funkció a tanúsítási útvonal sikeres ellenőrzésétől függ.

Az üzemeltetési környezettel kapcsolatos feltételezések

Az InfoSigno AC SDK IT környezetére vonatkozó feltételezés, hogy az tárolja, kezeli a TOE funkciók működéséhez szükséges tanúsítványokat, visszavonási információkat; a CRL-ek, ACRL-ek és OCSP válaszok rendelkezésre állnak a PKI szolgáltatás részeként. Az IT környezet része a megbízható pontok biztonságos tárolása is. (Lásd a 2. ábrát.)

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.

2.2 PP megfelelőség

Jelen biztonsági előirányzat PP megfelelőségi nyilatkozatot nem tesz a TOE specifikus biztonsági jellemzői miatt, de a PKE PP 2.8 verzió figyelembe vételével készült.

2.3 Biztonsági követelmény csomag megfelelőség

Jelen biztonsági előirányzat megfelel a CC v3.1 3. rész EAL 4 garanciacsomagnak (a MIBÉTS szerinti kiemelt értékelési garanciaszintnek).

3 Biztonsági probléma meghatározás

Értékek

Az értékelés tárgya által védendő értékek közé tartozik minden olyan objektum, amelyet az InfoSigno AC SDK-nak átadásra kerül, vagy az továbbítja a hívó IT környezet felé.
A védendő TOE felhasználói adatok közé tartozik az

- ellenőrizendő attribútum tanúsítvány,
- az ellenőrzéshez felhasznált:
    - megbízható pontok,
    - tanúsítványok,
    - visszavonási listák (CRL, ACRL),
    - OCSP kérések és válaszok,
- a megjelenített attribútumok,

A védendő TSF adatok közé tartozik az

- az érvényesség ellenőrzéshez használt időérték,
- az ellenőrzés eredménye,
- a tesztalkalmazás adminisztrátori beállításai az ellenőrzéshez.

A veszélyek forrásai

A fenyegetéseknek kitett értékek a TOE-n áthaladó információk. Általánosságban, a veszély források (de nem kizárólagosan) az alábbiak:

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

3.1 Fenyegetések

Mivel a biztonsági előirányzat RFC (RFC 5280 és RFC 3281) ajánlásokon alapuló követelményeket tartalmaz, ezért nem fenyegetések, hanem szabályok formájában képeztük le ezen követelményeket, így a biztonsági előirányzat fenyegetéseket formálisan nem tartalmaz.

3.2 Szervezeti biztonsági szabályzatok

Ez az alfejezet tartalmazza a TOE által teljesítendő biztonsági szabályokat.

Azonosító	Szabályzat leírása
P.PKC_Certificate_Validity	A TOE-nak ellenőriznie kell, hogy az attribútum tanúsítvány aláírójának (azaz az attribútum tanúsítvány kibocsátójának) vagy az attribútum tanúsítvány birtokosának (tulajdonosának) nyilvános kulcs tanúsítványa érvényes-e az ellenőrzéskor.
P.AC_Conformity	A TOE által ellenőrzött attribútum tanúsítványoknak meg kell felelniük az RFC 3281-ben lefektetett kötelező szabályoknak.
P.AC_Validity	A TOE-nak ellenőriznie kell, hogy az attribútum tanúsítvány érvényes-e az ellenőrzéskor.
P.Certificate_Authenticity	A TOE-nak biztosítania kell, hogy érvényes tanúsítási útvonal létezik az AC kibocsátó és egy megbízható pont, illetve az AC tulajdonos nyilvános kulcs tanúsítványa és egy megbízható pont között, továbbá az AC és AA között.
P.Validation_Data_Authenticity /Integrity	A TOE-nak ellenőriznie kell a felhasznált érvényesítő adatok eredetének hitelességét és sértetlenségét.
P.Attributes_Communication	A TOE-nak lehetővé kell tennie, hogy az ellenőrző megnézhesse az aláírt attribútumokat.
P.Hash_Algorithm	A TOE által megvalósított lenyomat-készítő algoritmusnak meg kell felelnie az alábbi kriptográfiai szabványnak: SHA-1 [FIPS 180-2].
P.Signature_Algorithm	A TOE által megvalósított kriptográfiai algoritmusnak és kulcshosszának meg kell felelnie az alábbi kriptográfiai szabványnak: RSA Encryption Standard, PKCS#1 v. 1.5, 1024 bit.
P.AC_CheckFrame	A TOE-nak képesnek kell lennie az AC ellenőrzési funkciók helyességének bemutatására egy erre alkalmas környezetben.

3.1 táblázat Az TOE által teljesítendő szabályzatok

3.3 Az üzemeltetési környezetre vonatkozó feltételezések

Az alábbi feltételezések az üzemeltetési környezetre vonatkoznak. A TOE-tól nem elvárás, hogy az ebben indirekt módon megfogalmazott fenyegetések ellen hatékony védelmet nyújtson.

Azonosító	Feltételezés leírása
A.Host_Platform	Feltételezés, hogy az a hoszt, 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. Alkalmazási megjegyzések: - a hoszt adminisztrátor szerepe eltér a TOE biztonsági adminisztrátor szerepétől. - ez a feltételezés azon veszélyeket fedi le, amelyek a TOE szolgáltatásinak végrehajtását zavarnák meg, és például módosítanának olyan felhasználói adatokat, mint a tanúsítványok és érvényesítő adatok.
A.Services_Integrity	A TOE környezetéről feltételezés, hogy a biztonsági adminisztrátorok számára biztosít olyan eszközöket, melyekkel a TOE szolgáltatásainak és paramétereinek sértetlensége kontrollálható.
A.Validation_Data_Access	A TOE-nak birtokolnia kell –vagy hozzá kell tudni férnie– minden olyan érvényesítő adathoz, amely az attribútum tanúsítvány aláírásának ellenőrzéséhez szükséges.
A.Trusted_Security_ Administrator	A TOE biztonsági adminisztrátorai megbízhatónak tekintendők, a TOE használatára kiképezték őket, és rendelkezésükre állnak azok az eszközök, amelyekkel a feladataikat megfelelően el tudják látni.
A.AC_CheckFrame	A TOE környezete biztosítja a TOE biztonsági funkciói helyes működésének bemutatásához szükséges IT környezetet a tesztekben részt vevő felhasználói adatok tárolásához.

3.2. táblázat Az IT környezetre vonatkozó feltételezések

4 Biztonsági célok

4.1 Az értékelés tárgyára vonatkozó biztonsági célok

Azonosító	Biztonsági cél leírása
O.Inic_AC	A TOE-nak gondoskodnia kell az ellenőrzés időpontjául szolgáló megbízható *időérték*, a nyilvános kulcs tanúsítványokhoz és az attribútum tanúsítvány ellenőrzésekor használt *megbízható pont*, továbbá az *ellenőrzési paraméterek* betöltéséről.
O.Certificates_Validity	Az RFC 5280-nak megfelelően a tanúsítási útvonal minden nyilvános kulcs tanúsítványára (ideértve a végtanúsítványokat 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.AC_Conformity	A TOE-nak ellenőriznie kell, hogy az attribútum tanúsítvány megfelel-e az RFC 3281-ben lefektetett kötelező szabályoknak.
O.AC_Validity	A TOE-nak az attribútum tanúsítványra ellenőriznie kell az alábbiakat: - a tanúsítvány eredetének hitelessége és a tanúsítvány sértetlensége; - a tanúsítvány érvényes volt a digitális aláírás ellenőrzésekor; - a tanúsítvány nem volt visszavont állapotú a digitális aláírás ellenőrzésekor.
O.Certification_Path	A TOE-nak ellenőriznie kell, hogy érvényes tanúsítási útvonal építhető fel az alábbiak között: - AC kibocsátó nyilvános kulcs tanúsítványa és egy megbízható pont között; - AC tulajdonos nyilvános kulcs tanúsítványa és egy megbízható pont között.
O.Validation_Data_ Conformity	A TOE-nak ellenőriznie kell, hogy a tanúsítványokon lévő aláírások ellenőrzéséhez használt érvényesítő adatok megfelelőek-e, különös tekintettel arra, hogy azokat a küldőjük írta alá, biztosítván ezzel a tanúsítványok sértetlenségét és eredtének hitelességét.
O.Attributes_ Communication	A TOE-nak képesnek kell tennie, hogy továbbítsa (vagy AC Test esetén megjelenítse) az AC-ben lévő attribútumokat az ellenőrző számára.
O.Cryptographic_Support	A TOE-nak az alábbi kriptográfiai tulajdonságokkal rendelkező kriptográfiai algoritmusokat kell alkalmazni: • A lenyomatoló algoritmus(ok)nak olyannak kell lennie, 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 a vonatkozó kriptográfiai szabványoknak: RSA Encryption Standard, PKCS#1 v. 1.5, 1024 bit SHA-1 FIPS-180-2
O.AC_CheckFrame	A TOE-nak rendelkeznie kell olyan funkcióval, melynek segítségével demonstrálja az AC ellenőrzési funkciók helyességét egy erre alkalmas környezetben, és kijelzi ennek eredményét.

4.1. táblázat A TOE-ra vonatkozó biztonsági célok

4.2 Az üzemeltetési környezetre vonatkozó biztonsági célok

Azonosító	Biztonsági cél leírása
OE.Host_Platform	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 garantálja az ellenőrző fél számára, hogy az alábbi biztonsági intézkedéseket ténylegesen alkalmazzák. A hoszt platform operációs rendszerének az általa futtatott alkalmazások számára elkülönített futási környezetet kell biztosítania. Fentieken túl az alábbi intézkedések teljesülését kell garantálni: • 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. Alkalmazási megjegyzések: - a hoszt adminisztrátor szerepe eltér a TOE biztonsági adminisztrátor szerepétől.
OE.Validation_Data_ Provision	A TOE környezetének biztosítania kell az aláírások és az attribútum tanúsítvány ellenőrzéséhez szükséges érvényesítő adatokat.
OE.Services_Integrity	A TOE környezetének a biztonsági adminisztrátorok számára biztosítania kell olyan eszközöket, melyekkel a TOE szolgáltatásainak és paramétereinek sértetlensége kontrollálható.
OE.Trusted_Security_ Administrator	A TOE biztonsági adminisztrátorainak megbízhatónak kell lenniük, a TOE használatára ki kell őket képezni, és rendelkezésükre állnak azok az eszközök, amelyekkel a feladataikat megfelelően el tudják látni.
OE.AC_CheckFrame	A TOE környezete biztosítja a teszteléshez szükséges IT környezetet a tesztekben részt vevő felhasználói adatok tárolásához.

4.2. táblázat Az üzemeltetési környezetre vonatkozó biztonsági célok

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 szabályzatok és a biztonsági célok

Szervezeti biztonsági szabályzat	**Biztonsági cél**
P.PKC_Certificate_Validity	O.Inic_AC O.Certificates_Validity
P.AC_Conformity	O.AC_Conformity
P.AC_Validity	O.AC_Validity
P.Certificate_Authenticity	O.Certification_Path
P.Validation_Data_Authenticity/Integrity	O.Validation_Data_Conformity
P.Attributes_Communication	O.Attributes_Communication
P.Hash_Algorithms	O.Cryptographic_Operations
P.Signature_Algorithms	O.Cryptographic_Operations
P.AC_CheckFrame	O.AC_CheckFrame OE.AC_CheckFrame O.Inic_AC

4.3. táblázat A szabályzatok lefedettsége biztonsági célokkal

Biztonsági cél	**Szervezeti biztonsági szabályzat**
O.Inic_AC	P.PKC_Certificate_Validity P.AC_CHeckFrame
O.Certification_Path	P.Certificate_Authenticity
O.Certificates_Validity	P.PKC_Certificate_Validity
O.Validation_Data_Conformity	P.Validation_Data_Authenticity/Integrity
O.AC_Conformity	P.AC_Conformity
O.AC_Validity	P.AC_Validity
O.Attributes_Communication	P.Attributes_Communication
O.Cryptographic_Operations	P.Hash_Algorithms, P.Signature_Algorithms
O.AC_CheckFrame	P.AC_CheckFrame

4.4. táblázat A TOE biztonsági célok leképezése szabályzatokra

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

- **O.Inic_AC**, amely biztosítja, hogy az aláírást és a tanúsítványt egy megbízható időértékhez és megbízható ponthoz, valamint az adminisztrátor által beállított paraméterekhez viszonyítva ellenőrizzék.
- **O.Certificates_Validity**, amely megköveteli, hogy a TOE ellenőrizze az aláíráshoz használt tanúsítvány érvényességét az ellenőrzés időpontjában.

A **P.AC_Conformity** szabályzatot a vele megegyező szövegezésű **O.AC_Conformity** biztonsági cél maradéktalanul lefedi.

P.AC_Validity: Ezt a szabályzatot az **O.AC_Validity** biztonsági cél fedi le, amely megköveteli, hogy az attribútum tanúsítvány érvényes, hiteles, sértetlen az ellenőrzés időpontjában.

P.Certificate_Authenticity: Ezt a szabályzatot a **O.Certification_Path** biztonsági cél fedi le, amely megköveteli, hogy a TOE érvényes tanúsítási útvonal meglétét ellenőrizze az egy végtanúsítványon (PKC vagy AC) lévő aláírói tanúsítvány hitelességének ellenőrzéséhez.

P.Validation_Data_Authenticity/Integrity: Ezt a szabályzatot az **O.Validation_Data_Conformity** biztonsági cél fedi le, amely megköveteli, hogy az érvényesítő adatokat azok rendelkezésre bocsátója aláírásával hitelesítse.

P.Attributes_Communication: Ezt a szabályzatot az **O.Attributes_Communication** biztonsági cél fedi le, amely megköveteli, hogy a TOE az őt hívó rendszerelemek felé továbbítani tudja az aláírt attribútumokat.

P.Hash_Algorithms: Ezt a szabályzatot az **O.Cryptographic_Operations** biztonsági cél lefedi.

P.Signature_Algorithms: Ezt a szabályzatot az **O.Cryptographic_Operations** biztonsági cél lefedi.

P.AC_CheckFrame: Ezt a szabályt a TOE-ra vonatkozó **O.AC_CheckFrame** és **O.Inic_AC** valamint az **OE.AC_CheckFrame** környezeti biztonsági célok fedik le.

4.3.2 A feltételezések és a biztonsági célok

Feltételezések	**Biztonsági célok**
A.Host_Platform	OE.Host_Platform
A.Services_Integrity	OE.Services_Integrity
A.Validation_Data_Access	OE.Validation_Data_Provision
A.Trusted_Security_Administrator	OE.Trusted_Security_Administrator
A.AC_CheckFrame	OE.AC_CheckFrame

4.5. táblázat A feltételezések lefedése biztonsági célokkal

Biztonsági célok	**Feltételezések**
OE.Host_Platform	A.Host_Platform
OE.Validation_Data_Provision	A.Validation_Data_Access
OE.Services_Integrity	A.Services_Integrity
OE.Trusted_Security_Administrator	A.Trusted_Security_Administrator
OE.AC_CheckFrame	A.AC_CheckFrame

4.6. táblázat A biztonsági célok lefedése feltételezésekkel

A.Host_Platform
Ezt a feltételezést az **OE.Host_Platfrom** teljes mértékben lefedi, szövegezésében is megfelel a feltételezésnek.

A.Services_Integrity: Ezt a feltételezést a megegyező szövegezésű **OE.Services_Integrity** teljes mértékben lefedi.

A.Validation_Data_Access: Ezt a feltételezést az **OE.Validation_Data_Provision** fedi le, amely megköveteli, hogy gondoskodni kell az aláírás ellenőrzéséhez szükséges érvényesítő adatokról.

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

A.AC_CheckFrame: Az **OE.AC_CheckFrame** környezeti követelmény fedi le, azaz a TOE környezete biztosítja a teszteléshez szükséges IT környezetet a tesztekben részt vevő felhasználói adatok tárolásához.

5 A kiterjesztett biztonsági követelmények meghatározása

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

Az alábbi táblázat áttekinti a funkcionális biztonsági követelményeket:

Osztály	**A funkcionális biztonsági követelmény (SFR) megnevezése**	**Az SFR összetevő jelölése**
Kriptográfiai támogatás (FCS)	Kriptográfiai műveletek	FCS_COP.1/Aláírás ellenőrzés
	Kriptográfiai műveletek	FCS_COP.1/Lenyomat
A felhasználói adatok védelme (FDP)	Részleges információ áramlás ellenőrzés	FDP_IFC.1/INIC
	Egyszerű biztonsági tulajdonságok	FDP_IFF.1/INIC
	Részleges információ áramlás ellenőrzés	FDP_IFC.1/Elektronikus aláírás és attribútumok
	Egyszerű biztonsági tulajdonságok	FDP_IFF.1/Elektronikus aláírás és attribútumok
	Részleges információ áramlás ellenőrzés	FDP_IFC.1/AC érvényesség ellenőrzése
	Egyszerű biztonsági tulajdonságok	FDP_IFF.1/AC érvényesség ellenőrzése
	Részleges információ áramlás ellenőrzés	FDP_IFC.1/Tanúsítási útvonal
	Egyszerű biztonsági tulajdonságok	FDP_IFF.1/Tanúsítási útvonal
	Részleges hozzáférés ellenőrzés	FDP_ACC.1
	Biztonsági tulajdonság alapú hozzáférés ellenőrzés	FDP_ACF.1
	A felhasználói adatok exportálása biztonsági tulajdonságokkal	FDP_ETC.2 AC ellenőrzés eredménye
	Felhasználói adatok importálása biztonsági tulajdonságokkal	FDP_ITC.2/Elektronikus aláírás és attribútumok
	Felhasználói adatok importálása biztonsági tulajdonságokkal	FDP_ITC.2/Tanúsítási útvonal
Azonosítás és hitelesítés (FIA)	Felhasználói tulajdonságok megadása	FIA_ATD.1
	Az azonosítás időzítése	FIA_UID.1
	A hitelesítés időzítése	FIA_UAU.1
Biztonsági menedzsment (FMT)	A biztonsági tulajdonságok menedzsmentje	FMT_MSA.1/INIC
	A biztonsági tulajdonságok menedzsmentje	FMT_MSA.1/Elektronikus aláírás és attribútumok
	A biztonsági tulajdonságok menedzsmentje	FMT_MSA.1/AC ellenőrzés eredménye
	A biztonsági tulajdonságok menedzsmentje	FMT_MSA.1/Tanúsítványok
	A biztonsági tulajdonságok menedzsmentje	FMT_MSA.1/Tanúsítvány érvényesítő adatok
	A biztonsági tulajdonságok menedzsmentje	FMT_MSA.1/Mgmt
	Statikus tulajdonságok kezdeti értékadása	FMT_MSA.3/INIC
	Statikus tulajdonságok kezdeti értékadása	FMT_MSA.3/Elektronikus aláírás és attribútumok

	Statikus tulajdonságok kezdeti értékadása	FMT_MSA.3/ Tanúsítási útvonal
	Statikus tulajdonságok kezdeti értékadása	FMT_MSA.3/AC ellenőrzés eredménye
	Statikus tulajdonságok kezdeti értékadása	FMT_MSA.3/Mgmt
	Biztonsági szerepkörök	FMT_SMR.1
	Menedzsment funkciók megadása	FMT_SMF.1
A TOE biztonsági funkciók védelme (FPT)	TSF-ek közötti alapszintű TSF adat konzisztencia	FPT_TDC.1/Tanúsítványok
	TSF-ek közötti alapszintű TSF adat konzisztencia	FPT_TDC.1/Tanúsítvány visszavonási adatok

6.1 táblázat– A funkcionális biztonsági követelmények

Az ellenőrzéshez szükséges megbízható helyről származó információk:

FDP_IFC.1/INIC Részleges információ áramlás ellenőrzés
FDP_IFC.1.1/INIC
A TSF-nek érvényre kell juttatnia az **AC ellenőrzés inicializálása** információ áramlási szabályt az alábbiak alapján:
- szubjektum: ellenőrző folyamat;
- információk:
- megbízható pont a helyi környezetből;
- időérték a helyi környezetből;

- művelet: fenti információk importálása.

FDP_IFF.1/INIC - Egyszerű biztonsági tulajdonságok
FDP_IFF.1.1/INIC A TSF-nek érvényre kell juttatnia az **AC ellenőrzés inicializálása** információ áramlási szabályt az alábbi, szubjektumra és információkra vonatkozó biztonsági tulajdonság típusokra::
- szubjektum:
- ellenőrző folyamat;

- információk (és biztonsági tulajdonságok):
- az AC-n és a PKC-ken lévő elektronikus aláírások ellenőrzéséhez használt időérték;
- a nyilvános kulcs tanúsítványokhoz tanúsítási útvonal felépítéséhez használt megbízható pont;

FDP_IFF.1.2/INIC A TSF-nek engedélyeznie kell az információ áramlást ellenőrzött szubjektumok és információk között, ellenőrzött műveleteken keresztül, ha teljesülnek az alábbi szabályok:
- **a megbízható pont DN mezője nem üres;**

FDP_IFF.1.3/INIC A TSF-nek érvényre kell juttatnia a következő egyéb szabályokat:
- **nincsenek további szabályok**

FDP_IFF.1.4/INIC A TSF-nek explicit módon engedélyeznie kell az információ áramlást az alábbi szabályok alapján:
- **az információk fogadása sikeresen megtörtént**.

FDP_IFF.1.5/INIC A TSF-nek explicit módon meg kell akadályoznia az információ áramlást az alábbi szabályok alapján:
- **az információk fogadása sikertelen**.

FMT_MSA.3/INIC - Statikus tulajdonságok kezdeti értékadása
FMT_MSA.3.1/INIC A TSF-nek érvényre kell juttatnia az **AC ellenőrzés inicializálása** információ áramlási szabályt, hogy [**helyi környezet által biztosított**] alapértékekről gondoskodjon az SFP-t érvényre juttatásához használt biztonsági tulajdonságok értékeire.
FMT_MSA.3.2/INIC A TSF-nek **senki** számára nem szabad engedélyeznie, hogy alternatív kezdeti értékekkel felülírja az alapértelmezett értékeket egy objektum vagy információ létrejöttekor.

FMT_MSA.1/INIC A biztonsági tulajdonságok menedzsmentje
FMT_MSA.1.1/INIC A TSF-nek érvényre kell juttatnia az **AC ellenőrzés inicializálása** információ áramlási szabályt, úgy, hogy **az időérték, megbízható pont** biztonsági tulajdonságot **senki** ne tudja **módosítani**.

Az attribútum tanúsítvánnyal közvetlenül kapcsolatos követelmények

FDP_IFC.1/Elektronikus aláírás és attribútumok - Részleges információ áramlás ellenőrzés
FDP_IFC.1.1/Elektronikus aláírás és attribútumok A TSF-nek érvényre kell juttatnia az **elektronikus aláírás és attribútumok** információ áramlási szabályt az alábbiakra:
- **szubjektumok**:
  - ellenőrző folyamat,
- **információk**:
  - az attribútum tanúsítványon lévő digitális aláírás;
  - az attribútum tanúsítványban szereplő adatok;
- **művelet**:
  - fenti információk importálása, illetve kinyerése a fogadott információkból.

FDP_IFF.1/ Elektronikus aláírás és attribútumok Egyszerű biztonsági tulajdonságok
FDP_IFF.1.1/ Elektronikus aláírás és attribútumok A TSF-nek érvényre kell juttatnia az **elektronikus aláírás és attribútumok** információ áramlási szabályt az alábbi, szubjektumra és információkra vonatkozó biztonsági tulajdonság típusokra::
- **szubjektumok**:
  - ellenőrző folyamat;
- **információk**::
  - az attribútum tanúsítványon lévő elektronikus aláírás;
  - az aláírt attribútumok;

FDP_IFF.1.2/ Elektronikus aláírás és attribútumok A TSF-nek engedélyeznie kell az információ áramlást ellenőrzött szubjektumok és információk között, ellenőrzött műveleteken keresztül az alábbi szabályok alapján:
- **az attribútum tanúsítványon lévő digitális aláírás ellenőrzése sikeres**

FDP_IFF.1.3/ Elektronikus aláírás és attribútumok A TSF-nek érvényre kell juttatnia a következő egyéb szabályokat:
- **a Version mező értéke az attribútum tanúsítványban v2;**

FDP_IFF.1.4/ Elektronikus aláírás és attribútumok A TSF-nek explicit módon engedélyeznie kell az információ áramlást az alábbi szabályok alapján: -
FDP_IFF.1.5/Elektronikus aláírás és attribútumok A TSF-nek explicit módon meg kell akadályoznia az információ áramlást az alábbi szabályok alapján:
- **legalább egy ellenőrzésen nem felelt meg az attribútum tanúsítvány.**

FMT_MSA.3/ Elektronikus aláírás és attribútumok - Statikus tulajdonságok kezdeti értékadása
FMT_MSA.3.1/ Elektronikus aláírás és attribútumok A TSF-nek érvényre kell juttatnia **elektronikus aláírás és attribútumok** információ áramlás ellenőrzési szabályt, hogy korlátozó alapértékeket adjon az SFP-t megvalósító biztonsági tulajdonságoknak.
FMT_MSA.3.2/ Elektronikus aláírás és attribútumok A TSF-nek **senki** számára sem szabad lehetővé tennie az alapértékek alternatív kezdeti értékekkel való felülírását egy objektum vagy információ létrehozásakor.

FMT_MSA.1 Elektronikus aláírás és attribútumok - A biztonsági tulajdonságok menedzselése
FMT_MSA.1.1/Elektronikus aláírás és attribútumok A TSF-nek érvényre kell juttatnia az **elektronikus aláírás és attribútumok** információ áramlás ellenőrzési szabályt, hogy **senki** ne tudja **módosítani** az **aláírás és az aláírt attribútumok** biztonsági tulajdonságot.

FDP_ITC.2/Elektronikus aláírás és attribútumok Felhasználói adatok importálása biztonsági tulajdonságokkal
FDP_ITC.2.1/Elektronikus aláírás és attribútumok A TSF-nek érvényre kell juttatnia az **elektronikus aláírás és attribútumok információ áramlás ellenőrzési szabályt** az SFP-k által felügyelt felhasználói adatok TOE-n kívülről történő importálása során.
FDP_ITC.2.2/Elektronikus aláírás és attribútumok A TSF-nek használnia kell az importált felhasználói adatokhoz kapcsolódó biztonsági tulajdonságokat.
FDP_ITC.2.3/Elektronikus aláírás és attribútumok A TSF-nek biztosítania kell, hogy az alkalmazott protokoll egyértelműen összekapcsolja a biztonsági tulajdonságokat és a kapott felhasználói adatokat.
FDP_ITC.2.4/Elektronikus aláírás és attribútumok A TSF-nek biztosítania kell, hogy az importált felhasználói adatok biztonsági tulajdonságának értelmezése olyan, amilyennek azt az adatok forrása szándékozta.
FDP_ITC.2.5/Elektronikus aláírás és attribútumok A TSF-nek érvényre kell juttatnia az alábbi szabályokat amikor az SFP ellenőrzése alatt a TOE-n kívülről felhasználói adatot importál:

- **megtalálja az AC tulajdonos PKC-jét (RFC 3281 5. fejezet 1. pont);**
- **megtalálja az AC kibocsátó PKC-jét (RFC 3281 5. fejezet 3. pont);**

<u>Az ellenőrzés eredményének visszaadása</u>

FDP_IFC.1/AC érvényesség ellenőrzése - Részleges információ áramlás ellenőrzés
FDP_IFC.1.1/AC érvényesség ellenőrzése A TSF-nek érvényre kell juttatnia az **AC érvényességének ellenőrzése** információ áramlás ellenőrzési szabályt az alábbiakra:

- **szubjektumok**:
- ellenőrző folyamat,
- **információ**:
- "érvényes AC" ellenőrzési státusz;
- attribútumok;
- **művelet**:
- a státusz és az attribútumok továbbítása (AC Test esetén megjelenítése) az ellenőrző fél számára.

FDP_IFF.1/AC érvényesség ellenőrzése - Egyszerű biztonsági tulajdonságok

FDP_IFF.1.1/AC érvényesség ellenőrzése A TSF-nek érvényre kell juttatnia az **AC érvényességének ellenőrzése** információ áramlás ellenőrzési szabályt, ami az alábbi szubjektum típusokon és információ biztonsági tulajdonságokon alapul:

- **szubjektumok**:
- ellenőrző folyamat,
- **információ**:
- „érvényes AC" érvényességi státusz (attribútumokkal).

FDP_IFF.1.2/AC érvényesség ellenőrzése A TSF-nek engedélyeznie kell az információ áramlást ellenőrzött szubjektumok és információk között, ellenőrzött műveleteken keresztül, ha teljesülnek az alábbi szabályok:

Az AC ellenőrzése eredményének közvetítése az ellenőrző folyamat számára:

- **az AC kibocsátó PKC-jére teljesülnek az FDP_IFF.1/Tanúsítási útvonal által megköveteltek (RFC 3281 5. fejezet 3. pont);**
- **az AC tulajdonos PKC-jére teljesülnek az FDP_IFF.1/Tanúsítási útvonal által megköveteltek (RFC 3281 5. fejezet 1. pont);**
- **az AC kibocsátó nyilvános kulcsával ellenőrizve az AC aláírása helyes (érvényes) (RFC 3281 5. fejezet 2. pont);**

FDP_IFF.1.3/AC érvényesség ellenőrzése A TSF-nek érvényre kell juttatnia a következő szabályokat:

- **a TSF képes minden kritikusnak jelölt kiterjesztést feldolgozni;**

FDP_IFF.1.4/AC érvényesség ellenőrzése A TSF-nek biztosítania kell az alábbi képességeket:

- **az „érvénytelen AC" eredmény közlésének képessége, amennyiben legalább egy információ áramlás ellenőrzési szabály nem teljesül.**

FDP_IFF.1.5/AC érvényesség ellenőrzése A TSF-nek explicit módon engedélyeznie kell az információ áramlást az alábbi szabályok alapján: -.

FDP_IFF.1.6/AC érvényesség ellenőrzése A TSF-nek explicit módon le kell tiltania az információ áramlást az alábbi szabályok alapján: -.

FDP_ETC.2/AC ellenőrzés eredménye - A felhasználói adatok exportálása biztonsági tulajdonságokkal

FDP_ETC.2.1/AC ellenőrzés eredménye A TSF-nek érvényre kell juttatnia az **AC érvényesség ellenőrzése** információ áramlás ellenőrzési szabályt, amikor az SFP ellenőrzése alatt a TOE-ből felhasználói adatokat exportál.

FDP_ETC.2.2/AC ellenőrzés eredménye A TSF-nek a felhasználói adatokat a hozzájuk kapcsolódó biztonsági tulajdonságokkal együtt kell exportálnia.

FDP_ETC.2.3/AC ellenőrzés eredménye A TSF-nek biztosítania kell, hogy a biztonsági tulajdonságok – azok TOE-n kívülre történő exportálása során-, egyértelműen hozzárendelődnek az exportált felhasználói adatokhoz.

FDP_ETC.2.4/AC ellenőrzés eredménye A TSF-nek érvényre kell juttatnia az alábbi szabályokat amikor az SFP ellenőrzése alatt a TOE-ből felhasználói adatot exportál:

Az AC ellenőrzés "megfelelt"eredmény biztonsági tulajdonságaiként exportált adatok:

- **az aláírt attribútumok.**

FMT_MSA.3/AC ellenőrzés eredménye - Statikus tulajdonságok kezdeti értékadása

FMT_MSA.3.1/AC ellenőrzés eredménye A TSF-nek érvényre kell juttatnia az **AC érvényesség ellenőrzése** információ áramlás ellenőrzési szabályt, hogy **korlátozó** alapértékeket adjon az SFP-t megvalósító biztonsági tulajdonságoknak.

FMT_MSA.3.2/AC ellenőrzés eredménye A TSF-nek **senki** számára sem szabad lehetővé tennie az alapértékek alternatív kezdeti értékekkel való felülírását egy objektum vagy információ létrehozásakor.

FMT_MSA.1/AC ellenőrzés eredménye - A biztonsági tulajdonságok menedzselése
FMT_MSA.1.1/AC ellenőrzés eredménye A TSF-nek érvényre kell juttatnia az **AC érvényesség ellenőrzése** információ áramlás ellenőrzési szabályt, hogy **senki** ne tudja **módosítani** az **AC ellenőrzés eredménye** biztonsági tulajdonságot.

A tanúsítási útvonal felépítésével kapcsolatos követelmények

FDP_IFC.1/Tanúsítási útvonal Részleges információ áramlás ellenőrzés
FDP_IFC.1.1/ Tanúsítási útvonal A TSF-nek érvényre kell juttatnia a **tanúsítási útvonal elfogadása** információ áramlási szabályt az alábbiakra:
- **szubjektumok**:
  - ellenőrző folyamat,
- **információk**:
  - a tanúsítási útvonalhoz tartozó tanúsítványok;
  - importált időérték,
  - a tanúsítási útvonal ellenőrzéséhez szükséges érvényesítő adatok (CRL, ACRL, OCSP válaszok)
  - digitális aláírás érték ellenőrzéshez biztonsági tulajdonságok: hash algoritmus, alany nyilvános kulcsa algoritmusa, alany nyilvános kulcsa
- **művelet**:
  - fenti információk importálása, illetve kinyerése a fogadott tanúsítványokból.

FDP_IFF.1/Tanúsítási útvonal Egyszerű biztonsági tulajdonságok
FDP_IFF.1.1/Tanúsítási útvonal A TSF-nek érvényre kell juttatnia a **tanúsítási útvonal elfogadása** információ áramlási szabályt az alábbi szubjektum típusokra és információ biztonsági tulajdonságokra:
- **szubjektumok**:
- ellenőrző folyamat;
- **információk**: tanúsítási útvonal érvényességével kapcsolatos adatok, ideértve az alábbiakat:
- a tanúsítási útvonalat alkotó tanúsítványok (tanúsítvány mezők): keyUsage, érvényességi idő,
- importált időérték,
- a tanúsítási útvonalat alkotó összes tanúsítványra a visszavonási adatok;
- digitális aláírás érték ellenőrzéshez biztonsági tulajdonságok: hash algoritmus, alany nyilvános kulcsú algoritmusa, alany nyilvános kulcsa

FDP_IFF.1.2/Tanúsítási útvonal A TSF-nek engedélyeznie kell az információ áramlást ellenőrzött szubjektumok és információk között, ellenőrzött műveleteken keresztül az alábbi szabályok alapján:
A tanúsítási útvonalat alkotó összetevők és a hozzájuk kapcsolódó érvényesítő adatok importálása:
- **tanúsítási útvonal köti össze az AC tulajdonos nyilvános kulcs tanúsítványát egy megbízható ponttal a tanúsítványokban lévő megkülönböztető név alapján;**
- **tanúsítási útvonal köti össze az AC kibocsátó nyilvános kulcs tanúsítványát egy megbízható ponttal a tanúsítványokban lévő megkülönböztető név alapján;**

- **a tanúsítvány kibocsátó mezője = szülő DN-je;**
- **a TSF képes minden kritikusnak jelölt kiterjesztést feldolgozni;**
- **a szülő nyilvános kulcsának, nyilvános kulcs azonosítójának használata a nyilvános kulcs tanúsítványon lévő aláírás ellenőrzéséhez;**

Csak <u>közbenső</u> nyilvános kulcs tanúsítványokra vonatkozó ellenőrzések:
- **a basicConstraints mező jelen van a CA=TRUE értékkel;**
- **a pathLenConstraint feltétel nem sérül;**
- **ha jelen van kritikus keyUsage kiterjesztés, akkor a keyCertSign bit be van állítva.**

A tanúsítási útvonal <u>minden tanúsítványra</u> teljesülnek az alábbiak az importált időérték által jelzett időpontban:
- **az importált időérték beleesik a tanúsítvány érvényességi idejébe;**
- **a tanúsítási útvonalat alkotó minden tanúsítványra a tanúsítványon lévő elektronikus aláírás megfelelő (digitális aláírás érték ellenőrzése helyes eredményt ad a felhasznált biztonsági tulajdonságok alapján: hash algoritmus, alany nyilvános kulcsa algoritmusa, alany nyilvános kulcsa);**
- **az összes visszavonási adatra a visszavonási adaton lévő elektronikus aláírás érték ellenőrzése helyes eredményt ad;**
- **a tanúsítási útvonalat alkotó minden tanúsítványra teljesül, hogy az ellenőrzés időpontjában a tanúsítvány nem volt visszavont;**
- **az RFC 5280-ban specifikált egyéb szabályok.**

Az alábbi további szabályok teljesülnek az attribútum tanúsítvány aláírójának (<u>AC kibocsátó) PKC-jére</u>:
- **a tanúsítvány kulcshasználatra vonatkozó mezője jelzi, hogy a tanúsítvány letagadhatatlansági célokra használható (keyUsage kiterjesztésben a digitalSignature bit értéke 1);**

FDP_IFF.1.3/Tanúsítási útvonal A TSF-nek érvényre kell juttatnia a következő egyéb szabályokat:
AC esetén:
- **amennyiben a tanúsítvány tartalmazza a noRevAvail kiterjesztést, akkor ki kell hagyni a visszavonási állapot ellenőrzést;**
- **AC kibocsátó DN= megbízható pont alany DN.**

FDP_IFF.1.4/ Tanúsítási útvonal A TSF-nek explicit módon engedélyeznie kell az információ áramlást az alábbi szabályok alapján: -.
FDP_IFF.1.5/ Tanúsítási útvonal A TSF-nek explicit módon meg kell akadályoznia az információ áramlást az alábbi szabályok alapján:
- **valamelyik ellenőrzés érvénytelen útvonalat mutatott ki.**

FMT_MSA.3/Tanúsítási útvonal - Statikus tulajdonságok kezdeti értékadása
FMT_MSA.3.1/Tanúsítási útvonal A TSF-nek érvényre kell juttatnia a **tanúsítási útvonal elfogadása** információ áramlási szabályzatot, hogy **korlátozó** értékekről gondoskodjon az SFP-t érvényre juttatásához használt biztonsági tulajdonságok értékeire.

FMT_MSA.3.2/Tanúsítási útvonal A TSF-nek **senki** számára sem szabad engedélyeznie, hogy alternatív kezdeti értékekkel felülírja az alapértelmezett értékeket egy objektum vagy információ létrejöttekor.

FMT_MSA.1/Tanúsítványok - A biztonsági tulajdonságok menedzsmentje
FMT_MSA.1.1/Tanúsítványok A TSF-nek érvényre kell juttatnia a **tanúsítási útvonal elfogadása** információ áramlási szabályt, úgy, hogy **az importált tanúsítványok** biztonsági tulajdonságait **senki** ne tudja **módosítani**.

FMT_MSA.1/Tanúsítvány érvényesítő adatok - A biztonsági tulajdonságok menedzsmentje
FMT_MSA.1.1 Tanúsítvány érvényesítő adatok A TSF-nek érvényre kell juttatnia a **tanúsítási útvonal elfogadása** információ áramlási szabályt, úgy, hogy **a tanúsítványok érvényesítő adatainak** biztonsági tulajdonságait **senki** ne tudja **módosítani**.

FDP_ITC.2/ Tanúsítási útvonal - Felhasználói adatok importálása biztonsági tulajdonságokkal
FDP_ITC.2.1/ Tanúsítási útvonal A TSF-nek érvényre kell juttatnia a **tanúsítási útvonal elfogadása információ áramlás ellenőrzési szabályt** az SFP-k által felügyelt felhasználói adatok TOE-n kívülről történő importálása során.
FDP_ITC.2.2/ Tanúsítási útvonal A TSF-nek használnia kell az importált felhasználói adatokhoz kapcsolódó biztonsági tulajdonságokat.
FDP_ITC.2.3/ Tanúsítási útvonal A TSF-nek biztosítania kell, hogy az alkalmazott protokoll egyértelműen összekapcsolja a biztonsági tulajdonságokat és a kapott felhasználói adatokat.
FDP_ITC.2.4/ Tanúsítási útvonal A TSF-nek biztosítania kell, hogy az importált felhasználói adatok biztonsági tulajdonságának értelmezése olyan, amilyennek azt az adatok forrása szándékozta.
FDP_ITC.2.5/ Tanúsítási útvonal A TSF-nek érvényre kell juttatnia az alábbi szabályokat amikor az SFP ellenőrzése alatt a TOE-n kívülről felhasználói adatot importál:

- **érvényes időérték importálása (lásd FDP_IFC.1/INIC és egyéb vonatkozó követelmény);**
- **minden olyan adat, amely a tanúsítványok letagadhatatlanságát segít ellenőrizni, importálásra kerül.**

FPT_TDC.1/Tanúsítványok – TSF-ek közötti alapszintű TSF adat konzisztencia
FPT_TDC.1.1/ Tanúsítványok A TSF-nek gondoskodnia kell olyan képességről, amely segítségével konzisztens módon értelmezhetők a **tanúsítványok,** amikor a TSF és más megbízható IT termék között megosztásra kerül.
FPT_TDC.1.2/ Tanúsítványok A TSF-nek az **RFC 5280-ban (X509v3) és RFC 3281-ben definiált tanúsítvány formátumokat** kell használnia, amikor más megbízható IT terméktől származó TSF adatot értelmez.

FPT_TDC.1/ Tanúsítvány visszavonási adatok – TSF-ek közötti alapszintű TSF adat konzisztencia
FPT_TDC.1.1/ Tanúsítvány visszavonási adatok A TSF-nek gondoskodnia kell olyan képességről, amely segítségével konzisztens módon értelmezhetők a **tanúsítvány visszavonási adatok,** amikor a TSF és más megbízható IT termék között megosztásra kerül.

FPT_TDC.1.2/ Tanúsítvány visszavonási adatok A TSF-nek használnia **kell az RFC 5280-ban definiált CRL formátumot (X509v2**) vagy az RFC 2560-ban **definiált OCSP formátumot** amikor más megbízható IT terméktől származó TSF adatot értelmez.

Kriptográfiai támogatás

FCS_COP.1/Aláírás ellenőrzés – Kriptográfiai műveletek
FCS_COP.1.1/ Aláírás ellenőrzés A TSF-nek **digitális aláírás ellenőrzést** kell végrehajtania az alábbi kriptográfiai algoritmus és kulcsméret és szabvány alapján: **RSA Encryption Standard, PKCS#1 v. 1.5, 1024 bit.**

FCS_COP.1/Lenyomat – Kriptográfiai műveletek
FCS_COP.1.1/Lenyomat A TSF-nek **lenyomat létrehozást** kell végrehajtania egy megadott kriptográfiai algoritmus és kulcsméret és szabvány alapján: **SHA-1 FIPS-180-2.**

Egyéb követelmények

FMT_SMR.1 Biztonsági szerepkörök
FMT_SMR.1.1 A TSF-nek kezelnie kell az alábbi szerepköröket
- **felhasználó („ellenőrző fél”)**
- **adminisztrátor**

FMT_SMR.1.2 A TSF-nek képesnek kell lennie, hogy a felhasználókat szerepkörökhöz rendelje.

FIA_ATD.1 Felhasználói tulajdonságok megadása

FIA_ATD.1.1 A TSF-nek az egyedi felhasználókhoz tartozó alábbi biztonsági tulajdonságokat kell kezelnie:

- „a felhasználóhoz van hozzárendelt AC”.

FIA_UID.1 Az azonosítás időzítése

FIA_UID.1.1 A TSF-nek a felhasználó azonosítása előtt lehetővé kell tennie az alábbi tevékenységek felhasználó nevében történő végrehajtását:
- **portletek leírásának megtekintése,**
- **a login-ból való visszalépés.**

FIA_UID.1.2 A TSF-nek meg kell követelnie minden felhasználó sikeres azonosítását, mielőtt bármilyen TSF által közvetített más tevékenységet lehetővé tenne az adott felhasználó nevében.

FIA_UAU.1 A hitelesítés időzítése
FIA_UAU.1.1 A TSF-nek a felhasználó hitelesítése előtt lehetővé kell tennie az alábbi tevékenységek felhasználó nevében történő végrehajtását:
- **portletek leírásának megtekintése,**
- **a login-ból való visszalépés.**

FIA_UAU.1.2 A TSF-nek meg kell követelnie minden felhasználó sikeres hitelesítését, mielőtt bármilyen TSF által közvetített más tevékenységet lehetővé tenne az adott felhasználó nevében.

FMT_SMF.1 Menedzsment funkciók megadása
FMT_SMF.1.1 A TSF-nek képesnek kell lennie a következő biztonság menedzsment funkciók végrehajtására:

- **targetName beállítás**
- **targetGroup beállítás**
- **felhasználóhoz név hozzárendelése a tesztelő keretalkalmazáshoz,**
- **felhasználóhoz név/jelszó pár megadása a teszteléshez,**
- **jogosult csoportok nevének megadása a teszteléshez,**
- **szerepkör nevek és kapcsolódó AC-k megadása a teszteléshez,**
- **felhasználókhoz AC-k hozzárendelése az ACTest alkalmazásban.**

FDP_ACC.1 Részleges hozzáférés ellenőrzés
FDP_ACC.1.1 A TSF-nek érvényre kell juttatnia az „**Attribútumok ellenőrzése keret”** hozzáférés ellenőrzési szabály SFP-t az alábbi szubjektumok és objektumok között, az alábbi műveletekre:
szubjektum:

- **ACTest hitelesített felhasználója,**

objektumok:

- **felhasználóhoz rendelt AC-k;**

művelet:

- **AC ellenőrzési funkciók végrehajtása.**

FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés
FDP_ACF.1.1 A TSF-nek érvényre kell juttatnia az „**Attribútumok ellenőrzése keret”**hozzáférés ellenőrzés szabály SFP-t a következők alapján:

szubjektum:	objektum	biztonsági tulajdonság
ACTest hitelesített felhasználója	**ACTest-be feltöltött AC-k**	**„a felhasználóhoz van hozzárendelt AC”**

FDP_ACF.1.2 A TSF-nek érvényre kell juttatnia a következő szabályokat annak megállapítása érdekében, hogy egy művelet megengedett-e az ellenőrzött szubjektumok és ellenőrzött objektumok között:

szubjektum:	hozzáférés ellenőrzési szabály
ACTest hitelesített felhasználója	**AC-vel rendelkező felhasználó hitelesítés után olvashatja az AC-ket és végrehajthatja az AC ellenőrzéseket**

FDP_ACF.1.3 A TSF-nek explicit módon kell megadnia a szubjektumok objektumokhoz való hozzáférési engedélyeit a következő kiegészítő szabályok alapján: **nincsenek további szabályok.**
FDP_ACF.1.4 A TSF-nek explicit módon le kell tiltania a szubjektumok objektumokhoz való hozzáféréseit az alábbiak alapján: **a felhasználóhoz nincs hozzárendelt AC.**

FMT_MSA.3/Mgmt - Statikus tulajdonságok kezdeti értékadása

FMT_MSA.3.1/Mgmt A TSF-nek érvényre kell juttatnia az „**Attribútumok ellenőrzése keret”** hozzáférés ellenőrzési szabályt, hogy az **adminisztrátor** alapértékekről gondoskodjon az SFP-t érvényre juttatásához használt biztonsági tulajdonságok értékeire.
FMT_MSA.3.2/Mgmt A TSF-nek az **adminisztrátor** számára szabad engedélyeznie, hogy alternatív kezdeti értékekkel felülírja az alapértelmezett értékeket egy objektum vagy információ létrejöttekor.

FMT_MSA.1/Mgmt A biztonsági tulajdonságok menedzsmentje
FMT_MSA.1.1/Mgmt A TSF-nek érvényre kell juttatnia az „**Attribútumok ellenőrzése keret”**hozzáférés ellenőrzési szabályt, úgy, hogy **a „felhasználóhoz van hozzárendelt AC”** biztonsági tulajdonságot **az adminisztrátor** tudja **módosítani**.

6.2 A garanciális biztonsági követelmények

Osztály	A garanciális biztonsági követelmény (SAR) megnevezése	Az SAR összetevő jelölése
Fejlesztés (ALC)	Biztonsági szerkezet leírás	ADV_ARC.1
	Teljes funkcionális specifikáció	ADV_FSP. 4
	Alap moduláris terv	ADV_TDS.3
	A TSF megvalósítási reprezentációja	ADV_IMP.1
Útmutató dokumentumok (AGD)	Üzemeltetési felhasználói útmutató	AGD_OPE.1
	Előkészítő eljárások	AGD_PRE.1
Életciklus támogatás (ALC)	A TOE előállítás támogatása, átvételi eljárások és automatizálás	ALC_CMC.4
	A probléma követés CM lefedettsége	ALC_CMS.4
	Szállítási eljárások	ALC_DEL.1
	A biztonsági intézkedések azonosítása	ALC_DVS.1
	A fejlesztő által meghatározott életciklus modell	ALC_LCD.1
	Jól meghatározott fejlesztő eszközök	ALC_TAT.1
Tesztelés (ATE)	Funkcionális tesztelés	ATE_FUN.1
	A lefedettség vizsgálata	ATE_COV.2
	A biztonságot érvényre juttató modulok tesztelése	ATE_DPT.2
	Független tesztelés - minta	ATE_IND.2
Sebezhetőség felmérés (AVA)	Célirányos sebezhetőség vizsgálat	AVA_VAN.3

6.2 táblázat– A garanciális biztonsági követelmények

6.3 A funkcionális biztonsági követelmények indoklása

A biztonsági célok és a biztonsági követelmények közötti lefedettség elemzése:

A 6.3 táblázat kimutatja, hogy minden SFR visszavezethető legalább egy TOE biztonsági célra.

SFR	TOE biztonsági cél
FCS_COP.1/Aláírás ellenőrzés	O.Cryptographic_Operations
FCS_COP.1/Lenyomat	O.Cryptographic_Operations
FDP_IFC.1/INIC	O.Inic_AC
FDP_IFF.1/INIC	O.Inic_AC
FDP_IFC.1/Elektronikus aláírás és attribútumok	O.AC_Conformity, O.AC_Validity
FDP_IFF.1/ Elektronikus aláírás és attribútumok	O.AC_Conformity O.AC_Validity
FDP_IFC.1/AC érvényesség ellenőrzése	O.Attributes_Communication
FDP_IFF.1/AC érvényesség ellenőrzése	O.Attributes_Communication
FDP_IFC.1/Tanúsítási útvonal	O.Certification_Path O.Certificates_Validity O.Validation_Data_Conformity O.Certificates_Conformity
FDP_IFF.1/Tanúsítási útvonal	O.Certification_Path O.Certificates_Validity O.Validation_Data_Conformity O.Certificates_Conformity
FDP_ACC.1	O.AC_CheckFrame
FDP_ACF.1	O.AC_CheckFrame
FDP_ETC.2 AC ellenőrzés eredménye	O.Attributes_Communication
FDP_ITC.2/Elektronikus aláírás és attribútumok	O.AC_Conformity O.AC_Validity
FDP_ITC.2/Tanúsítási útvonal	O.Certification_Path O.Certificates_Validity O.Validation_Data_Conformity O.Certificates_Conformity
FIA_ATD.1	O.AC_CheckFrame
FIA_UID.1	O.Certification_Path O.Certificates_Validity O.Validation_Data_Conformity O.Certificates_Conformity O.AC_CheckFrame
FIA_UAU.1	O.AC_CheckFrame
FMT_MSA.1/INIC	O.Inic_AC
FMT_MSA.1/Elektronikus aláírás és attribútumok	O.AC_Conformity O.AC_Validity

FMT_MSA.1/AC ellenőrzés eredménye	O.Attributes_Communication
FMT_MSA.1/Tanúsítvány érvényesítő adatokt	O.Certification_Path O.Certificates_Validity O.Validation_Data_Conformity O.Certificates_Conformity
FMT_MSA.1/Mgmt	O.AC_CheckFrame
FMT_MSA.1/Tanúsítványok	O.Certification_Path O.Certificates_Validity O.Validation_Data_Conformity O.Certificates_Conformity
FMT_MSA.3/INIC	O.Inic_AC
FMT_MSA.3/Elektronikus aláírás és attribútumok	O.AC_Conformity O.AC_Validity
FMT_MSA.3/AC ellenőrzés eredménye	O.Attributes_Communication
FMT_MSA.3/Tanúsítási útvonal	O.Certification_Path O.Certificates_Validity O.Validation_Data_Conformity O.Certificates_Conformity
FMT_MSA.3/Mgmt	O.AC_CheckFrame
FMT_SMR.1	O.Certification_Path O.Certificates_Validity O.Validation_Data_Conformity O.Certificates_Conformity O.AC_CheckFrame
FMT_SMF.1	O.AC_CheckFrame
FPT_TDC.1/Tanúsítványok	O.Certification_Path O.Validation_Data_Conformity O.Validation_Data_Conformity
FPT_TDC.1/Tanúsítvány visszavonási adatok	O.Certification_Path O.Certification_Path O.Validation_Data_Conformity O.Certificates_Conformity

6.3 táblázat– A funkcionális követelmények leképezése a biztonsági célokra

A 6.4 táblázat, majd az azt követő indoklás kimutatja, hogy a TOE összes biztonsági céljára az SFR-k alkalmasak az adott TOE biztonsági cél teljesítésére.

A TOE-ra vonatkozó biztonsági cél	Funkcionális biztonsági követelmény (SFR)
O.Certification_Path	FDP_IFC.1/Tanúsítási útvonal FDP_IFF.1/Tanúsítási útvonal FMT_MSA.3/Tanúsítási útvonal FMT_MSA.1/Tanúsítványok FMT_MSA.1/Tanúsítvány érvényesítő adatok FDP_ITC.2/Tanúsítási útvonal

	FPT_TDC.1/Tanúsítványok FPT_TDC.1/Tanúsítvány visszavonási adatok FMT_SMR.1 FIA_UID.1
O.Certificates_Validity	FDP_IFC.1/Tanúsítási útvonal FDP_IFF.1/Tanúsítási útvonal FMT_MSA.3/Tanúsítási útvonal FMT_MSA.1/Tanúsítványok FMT_MSA.1/Tanúsítvány érvényesítő adatok FDP_ITC.2/Tanúsítási útvonal FPT_TDC.1/Tanúsítványok FPT_TDC.1/Tanúsítvány visszavonási adatok FMT_SMR.1 FIA_UID.1
O.Validation_Data_Conformity	FDP_IFC.1/Tanúsítási útvonal FDP_IFF.1/Tanúsítási útvonal FMT_MSA.3/Tanúsítási útvonal FMT_MSA.1/Tanúsítványok FMT_MSA.1/Tanúsítvány érvényesítő adatok FDP_ITC.2/Tanúsítási útvonal FPT_TDC.1/Tanúsítványok FPT_TDC.1/Tanúsítvány visszavonási adatok FMT_SMR.1 FIA_UID.1
O.Certificates_Conformity	FDP_IFC.1/Tanúsítási útvonal FDP_IFF.1/Tanúsítási útvonal FMT_MSA.3/Tanúsítási útvonal FMT_MSA.1/Tanúsítványok FMT_MSA.1/Tanúsítvány érvényesítő adatok FDP_ITC.2/Tanúsítási útvonal FPT_TDC.1/Tanúsítványok FPT_TDC.1/Tanúsítvány visszavonási adatok FMT_SMR.1 FIA_UID.1
O.AC_Conformity	FDP_IFC.1/Elektronikus aláírás és attribútumok FDP_IFF.1/ Elektronikus aláírás és attribútumok FMT_MSA.3/ Elektronikus aláírás és attribútumok FMT_MSA.1/ Elektronikus aláírás és attribútumok FDP_ITC.2/ Elektronikus aláírás és attribútumok
O.AC_Validity	FDP_IFC.1/Elektronikus aláírás és attribútumok FDP_IFF.1/ Elektronikus aláírás és attribútumok FMT_MSA.3/ Elektronikus aláírás és attribútumok FMT_MSA.1/ Elektronikus aláírás és attribútumok FDP_ITC.2/ Elektronikus aláírás és attribútumok
O.Attributes_Communication	FDP_IFC.1/AC érvényesség ellenőrzése FDP_IFF.1/AC érvényesség ellenőrzése FMT_MSA.3/AC ellenőrzés eredménye FMT_MSA.1/AC ellenőrzés eredménye FDP_ETC.2/AC ellenőrzés eredménye
O.Cryptographic_Operations	FCS_COP.1/Aláírás ellenőrzés

	FCS_COP.1/Lenyomat
O.Inic_AC	FDP_IFC.1/INIC FDP_IFF.1/INIC FMT_MSA.3/INIC FMT_MSA.1/INIC
O.AC_CheckFrame	FMT_SMR.1 FIA_ATD.1 FIA_UID.1 FIA_UAU.1 FMT_SMF.1 FDP_ACC.1 FDP_ACF.1 FMT_MSA.3/Mgmt FMT_MSA.1/Mgmt

6.4 táblázat– A biztonsági célok leképezése funkcionális követelményekre

Az **O.Certification_Path** biztonsági célt az alábbi funkcionális követelmények teljesítik:

A TOE-nak információáramlási szabályt kell használnia (**FDP_IFC.1/Tanúsítási útvonal**) azon eljárásban, mely során tanúsítási útvonalat alkotó tanúsítványokat importál, mely útvonal összeköti a szóban forgó végtanúsítványt (attribútum tanúsítvány kibocsátójának nyilvános kulcs tanúsítványát, illetve az attribútum tanúsítvány tulajdonosának tanúsítványát) a gyökértanúsítvánnyal.
Az **FDP_ITC.2/Tanúsítási útvonal** funkcionális összetevő azt biztosítja, hogy a TOE tényleg használja az információ áramlási szabályt a tanúsítványok importálása során.
Az **FPT_TDC.1/Tanúsítványok** és **FPT_TDC.1/Tanúsítvány visszavonási adatok** követelmények azt garantálják, hogy a TOE képes ezen adatok feldolgozására.
Az **FDP_IFF.1/Tanúsítási útvonal** követelmény adja meg az információ áramlás szabályait. Ez az összetevő adja meg a megvalósítandó szabályokat.

Az alábbi funkcionális összetevők, amelyek az információ áramlásban érintett szubjektumok és információk biztonsági tulajdonságainak kezelésével kapcsolatosak, szintén hozzájárulnak a biztonsági cél teljesüléséhez:

- Az **FMT_MSA.3/Tanúsítási útvonal** követelmény garantálja, hogy az információ áramlási szabályokban szereplő biztonsági tulajdonságok alapértékei korlátozott értékeket vegyenek fel.
- Az **FMT_MSA.1/Tanúsítványok** garantálja, hogy a tanúsítási útvonal felépítéséhez szükséges tanúsítvány attribútumok nem módosíthatók.
- Az **FMT_MSA.1/Tanúsítvány érvényesítő adatok** funkcionális összetevő garantálja, hogy az aláíró illetve attribútum tanúsítvány tulajdonos nyilvános kulcs tanúsítványának érvényesítő adatainak attribútumai nem módosíthatók.
- Az **FMT_SMR.1** megköveteli, hogy a TOE elkülönítse az ellenőrző fél és az adminisztrátor szerepköröket.
- A **FIA_UID.1** megköveteli, hogy a TOE ne hajtson végre tanúsítvány ellenőrzési funkciót a felhasználó sikeres azonosítása előtt.

Az **O.Certificates_Validity** biztonsági célt az alábbi funkcionális követelmények teljesítik:

A TOE-nak információ áramlási szabályt kell használnia (**FDP_IFC.1/Tanúsítási útvonal**) azon eljárásban, mely során tanúsítási útvonalat alkotó tanúsítványokat importál, mely útvonal összeköti a szóban forgó végtanúsítványt (attribútum tanúsítvány kibocsátójának nyilvános kulcs tanúsítványát, illetve az attribútum tanúsítvány tulajdonosának tanúsítványát) a gyökértanúsítvánnyal.
Az **FDP_ITC.2/Tanúsítási útvonal** funkcionális összetevő azt biztosítja, hogy a TOE tényleg használja az információ áramlási szabályt a tanúsítványok és a nem visszavont állapotot mutató információk importálása során.
Az **FPT_TDC.1/Tanúsítványok** és elsősorban az **FPT_TDC.1/Tanúsítvány visszavonási adatok** követelmény azt garantálja, hogy a TOE képes ezen adatok feldolgozására.
Az **FDP_IFF.1/Tanúsítási útvonal** követelmény adja meg az információ áramlás szabályait. Ez az összetevő adja meg a megvalósítandó szabályokat. Ez a követelmény azon szabályokat adja meg, amelyek lehetővé teszik a TSF számára annak megállapítását, hogy a tanúsítványokból felépített útvonal érvényes és a tanúsítványok nem visszavont állapotúak.

Az alábbi funkcionális összetevők, amelyek az információ áramlásban érintett szubjektumok és információk biztonsági tulajdonságainak kezelésével kapcsolatosak, szintén hozzájárulnak a biztonsági cél teljesüléséhez:

- Az **FMT_MSA.3/Tanúsítási útvonal** követelmény garantálja, hogy az információ áramlási szabályokban szereplő biztonsági tulajdonságok alapértékei korlátozott értékeket vegyenek fel.
- Az **FMT_MSA.1/Tanúsítványok** garantálja, hogy a tanúsítási útvonal felépítéséhez szükséges tanúsítvány attribútumok nem módosíthatók.
- Az **FMT_MSA.1/Tanúsítvány érvényesítő adatok** funkcionális összetevő garantálja, hogy az aláíró illetve attribútum tanúsítvány tulajdonos nyilvános kulcs tanúsítványának érvényesítő adatainak attribútumai nem módosíthatók.
- Az **FMT_SMR.1** megköveteli, hogy a TOE elkülönítse az ellenőrző fél és az adminisztrátor szerepköröket.
- A **FIA_UID.1** megköveteli, hogy a TOE ne hajtson végre tanúsítvány ellenőrzési funkciót a felhasználó sikeres azonosítása előtt.

Az **O.Validation_Data_Conformity** valamint az **O.Certificates_Conformity** biztonsági célt az alábbi funkcionális követelmények teljesítik:

A TOE-nak információ áramlási szabályt kell használnia (**FDP_IFC.1/Tanúsítási útvonal**) azon eljárásban, mely során tanúsítási útvonalat alkotó tanúsítványokat importál, mely útvonal összeköti a szóban forgó végtanúsítványt (attribútum tanúsítvány kibocsátójának nyilvános kulcs tanúsítványát, illetve az attribútum tanúsítvány tulajdonosának tanúsítványát) a gyökértanúsítvánnyal. Ez az információ áramlási szabály vonatkozik a tanúsítványok nem visszavont állapotát mutató információkra is.
Az **FDP_ITC.2/Tanúsítási útvonal** funkcionális összetevő azt biztosítja, hogy a TOE tényleg használja az információ áramlási szabályt a tanúsítványok és a nem visszavont állapotot mutató információk importálása során.
Az **FPT_TDC.1/Tanúsítványok** és elsősorban az **FPT_TDC.1/Tanúsítvány visszavonási adatok** követelmény azt garantálja, hogy a TOE képes ezen adatok feldolgozására.
Az **FDP_IFF.1/Tanúsítási útvonal** követelmény adja meg az információ áramlás szabályait. Ez a követelmény azon szabályokat adja meg, amelyek lehetővé teszik a TSF számára annak megállapítását, hogy a tanúsítvány visszavonási adatok érvényesek-e.

Az alábbi funkcionális összetevők, amelyek az információ áramlásban érintett szubjektumok és információk biztonsági tulajdonságainak kezelésével kapcsolatosak, szintén hozzájárulnak a biztonsági cél teljesüléséhez:

- Az **FMT_MSA.3/Tanúsítási útvonal** követelmény garantálja, hogy az információ áramlási szabályokban szereplő biztonsági tulajdonságok alapértékei korlátozott értékeket vegyenek fel.
- Az **FMT_MSA.1/Tanúsítványok** garantálja, hogy a tanúsítási útvonal felépítéséhez szükséges tanúsítvány attribútumok nem módosíthatók.
- Az **FMT_MSA.1/Tanúsítvány érvényesítő adatok** funkcionális összetevő garantálja, hogy az aláíró illetve attribútum tanúsítvány tulajdonos nyilvános kulcs tanúsítványának érvényesítő adatainak attribútumai nem módosíthatók.
- Az **FMT_SMR.1** megköveteli, hogy a TOE elkülönítse az ellenőrző fél és az adminisztrátor szerepköröket.
- A **FIA_UID.1** megköveteli, hogy a TOE ne hajtson végre tanúsítvány ellenőrzési funkciót a felhasználó sikeres azonosítása előtt.

Az **O.AC_Conformity** (az attribútum tanúsítvány RFC 3281-ben szereplő kötelező ellenőrzési szabályoknak való megfelelését megfogalmazó), valamint az AC érvényességét előíró **O.AC_Validity** biztonsági célt az alábbi követelmények teljesítik:

- A TOE az **FDP_IFC.1/Elektronikus aláírás és attribútumok** és **FDP_IFF.1/ Elektronikus aláírás és attribútumok** információ áramlás ellenőrzési szabályt használ az attribútum tanúsítványon lévő elektronikus aláírás ás az attribútum tanúsítvány adatainak importálására.
- Az **FDP_ITC.2/Elektronikus aláírás és attribútumok** funkcionális összetevő azt biztosítja, hogy a TOE tényleg használja az információ áramlási szabályt az elektronikus aláírás és attribútumok információk importálása során.
- Az **FMT_MSA.3/ Elektronikus aláírás és attribútumok** követelmény garantálja, hogy az információ áramlási szabályokban szereplő biztonsági tulajdonságok alapértékei korlátozott értékeket vegyenek fel.
- Az **FMT_MSA.1/ Elektronikus aláírás és attribútumok** követelmény garantálja, hogy a tanúsítási útvonal felépítéséhez szükséges tanúsítvány attribútumok nem módosíthatók.

Fenti követelmények tartalmazzák az érvényesség ellenőrzésre vonatkozó követelményeket is.

Az **O.Attributes_Communication** biztonsági célt az alábbi követelmények teljesítik:

A TOE-nak információáramlási szabályt kell használnia (**FDP_IFC.1/AC érvényesség ellenőrzése** és **FDP_IFF.1/AC érvényesség ellenőrzése**) azon eljárásban, mely során a TOE által ellenőrzött attribútum tanúsítvány ellenőrzésének eredményét és a tanúsítvány bizonyos információit a hívó fél számára közvetíti.
Az alábbi egyéb követelmények járulnak még a cél teljesítéséhez:

- Az **FDP_ETC.2/AC ellenőrzés eredménye** funkcionális összetevő azt biztosítja, hogy a TOE tényleg használja az információ áramlási szabályt az ellenőrzés eredményének exportálása során.
- Az **FMT_MSA.3/AC ellenőrzés eredménye** követelmény garantálja, hogy az információ áramlási szabályokban szereplő biztonsági tulajdonságok alapértékei korlátozott értékeket vegyenek fel.

- Az **FMT_MSA.1/AC ellenőrzés eredménye** követelmény garantálja, hogy az exportálandó információk nem módosíthatók.

Az **O.Cryptographic_Operations** biztonsági célt az alábbi követelmények teljesítik:

- Az **FCS_COP.1/lenyomat** funkcionális összetevő azt biztosítja, hogy a lenyomat készítő algoritmus által létrehozott hash érték ütközés-mentes eredményt adjon.
- Az **FCS_COP.1/Aláírás ellenőrzés** azt garantálja, hogy az ellenőrző folyamatban alkalmazott algoritmus ellenáll a kriptoanalízis támadásoknak. A kulcsméret megfelelő ahhoz, hogy egy tanúsítványban szereplő nyilvános kulcs támadásnak való ellenállását biztosítsa a tanúsítvány élettartama alatt.

Az **O.AC_CheckFrame** biztonsági célt az alábbi követelmények teljesítik:

- Az **FMT_SMR.1 Biztonsági szerepkörök** követelmény határozza meg a TOE és tesztalkalmazás szerepköreinek elkülönítését.
- A **FIA_ATD.1 Felhasználói tulajdonságok megadása** követelmény biztosítja, hogy biztonsági tulajdonságot lehessen a felhasználókhoz rendelni..
- A **FIA_UID.1 Az azonosítás időzítése** biztonsági követelmény lehetővé teszi, hogy a felhasználó azonosítás nélkül milyen tevékenységeket végezhet az ACTest alkalmazásban.
- A **FIA_UAU.1 A hitelesítés időzítése** biztonsági követelmény lehetővé teszi, hogy a felhasználó hitelesítés nélkül milyen tevékenységeket végezhet az ACTest alkalmazásban.
- A **FMT_SMF.1 Menedzsment funkciók megadása** megadja, hogy a TOE működéséhez milyen menedzsment funkciókat kell biztosítani.
- A TOE az **FDP_ACC.1 Részleges hozzáférés ellenőrzés** és **FDP_ACF.1Biztonsági tulajdonság alapú hozzáférés ellenőrzés** szabályt használ az attribútum tanúsítványok adott keretrendszerben (ACTest alkalmazás) történő ellenőrzésének hozzáféréseinek megadására.
- Az **FMT_MSA.3/Mgmt** követelmény garantálja, hogy a hozzáférés ellenőrzési szabályokban szereplő biztonsági tulajdonságok alapértékei korlátozott értékeket vegyenek fel.
- Az **FMT_MSA.1/Mgmt** követelmény garantálja, hogy az ellenőrzéshez alkalmazott bizonyos paraméterek módosítását csak az arra kijelölt szerepkörbe tartozó felhasználó (adminisztrátor) végezheti.

6.4 A funkcionális követelmények közötti függések teljesülése

Az alábbi táblázat összesíti a funkcionális követelményeket, megadva a CC v3.1 2. rész szerinti függéseket, a függés teljesülését, illetve a nem teljesülés indoklását.

Funkcionális követelmény	**Függések**	**Teljesülés**
FDP_IFC.1/INIC Részleges információ áramlás ellenőrzés	FDP_IFF.1	Teljesül: FDP_IFF.1/INIC - Egyszerű biztonsági tulajdonságok
FDP_IFF.1/INIC - Egyszerű biztonsági tulajdonságok	FDP_IFC.1	Teljesül: FDP_IFC.1/INIC Részleges információ áramlás ellenőrzés
	FMT_MSA.3	Teljesül: FMT_MSA.3/INIC - Statikus tulajdonságok kezdeti értékadása
FMT_MSA.3/INIC - Statikus tulajdonságok kezdeti értékadása	FMT_MSA.1	Teljesül FMT_MSA.1/INIC A biztonsági tulajdonságok menedzsmentje
	FMT_SMR.1	Teljesül: FMT_SMR.1 Biztonsági szerepkörök
FMT_MSA.1/INIC A biztonsági tulajdonságok menedzsmentje	FDP_IFC.1	Teljesül: FDP_IFC.1/INIC Részleges információ áramlás ellenőrzés
	FMT_SMR.1	Teljesül: FMT_SMR.1 Biztonsági szerepkörök
	FMT_SMF.1	Teljesül.
FDP_IFC.1/Elektronikus aláírás és attribútumok - Részleges információ áramlás ellenőrzés	FDP_IFF.1	Teljesül: FDP_IFF.1/ Elektronikus aláírás és attribútumok Egyszerű biztonsági tulajdonságok
FDP_IFF.1/Elektronikus aláírás és attribútumok Egyszerű biztonsági tulajdonságok	FDP_IFC.1	Teljesül: FDP_IFC.1/Elektronikus aláírás és attribútumok
	FMT_MSA.3	Teljesül: FMT_MSA.3/Elektronikus aláírás és attribútumok
FMT_MSA.3/Elektronikus aláírás és attribútumok - Statikus tulajdonságok kezdeti értékadása	FMT_MSA.	Teljesül
	FMT_SMR.1	Teljesül: FMT_SMR.1 Biztonsági szerepkörök
FMT_MSA.1 Elektronikus aláírás és attribútumok - A biztonsági tulajdonságok menedzselése	FDP_IFC.1	Teljesül: FDP_IFC.1/Elektronikus aláírás és attribútumok
	FMT_SMR.1	Teljesül: FMT_SMR.1 Biztonsági szerepkörök
	FMT_SMF.1	Teljesül.
FDP_ITC.2/Elektronikus aláírás és attribútumok Felhasználói adatok importálása biztonsági tulajdonságokkal	FDP_IFC.1	Teljesül: FDP_IFC.1/Elektronikus aláírás és attribútumok - Részleges információ áramlás ellenőrzés

	FTP_ITC.1 vagy FTP_TRP.1	Nem teljesül. Indoklás: Ezek az adatok bizalmassági védelmet nem igényelnek. Az elektronikus aláírásban lévő digitális aláírás érvényessége garantálja az aláírt adatok sértetlenségét. Az elektronikus aláírás érvényessége bizonyítja az információ eredetének hitelességét.
FDP_IFC.1/AC érvényesség ellenőrzése - Részleges információ áramlás ellenőrzés	FDP_IFF.1	Teljesül: FDP_IFF.1/AC érvényesség ellenőrzése - Egyszerű biztonsági tulajdonságok
FDP_IFF.1/AC érvényesség ellenőrzése - Egyszerű biztonsági tulajdonságok	FDP_IFC.1	Teljesül: FDP_IFC.1/AC érvényesség ellenőrzése - Részleges információ áramlás ellenőrzés
	FMT_MSA.3	Teljesül: FMT_MSA.3/AC ellenőrzés eredménye - Statikus tulajdonságok kezdeti értékadása
FDP_ETC.2/AC ellenőrzés eredménye - A felhasználói adatok exportálása biztonsági tulajdonságokkal	FDP_IFC.1	Teljesül: FDP_IFC.1/AC érvényesség ellenőrzése - Részleges információ áramlás ellenőrzés
FMT_MSA.3/AC ellenőrzés eredménye - Statikus tulajdonságok kezdeti értékadása	FMT_MSA.1	Teljesül: FMT_MSA.1/AC ellenőrzés eredménye - A biztonsági tulajdonságok menedzselése
	FMT_SMR.1	Teljesül: FMT_SMR.1 Biztonsági szerepkörök
FMT_MSA.1/AC ellenőrzés eredménye - A biztonsági tulajdonságok menedzselése	FDP_IFC.1	Teljesül: FDP_IFC.1/AC érvényesség ellenőrzése - Részleges információ áramlás ellenőrzés
	FMT_SMR.1	Teljesül: FMT_SMR.1 Biztonsági szerepkörök
	FMT_SMF.1	Teljesül.
FDP_IFC.1/Tanúsítási útvonal - Részleges információ áramlás ellenőrzés	FDP_IFF.1	Teljesül: FDP_IFF.1/Tanúsítási útvonal Egyszerű biztonsági tulajdonságok
FDP_IFF.1/Tanúsítási útvonal - Egyszerű biztonsági tulajdonságok	FDP_IFC.1	Teljesül: FDP_IFC.1/Tanúsítási útvonal Részleges információ áramlás ellenőrzés
	FMT_MSA.3	Teljesül: FMT_MSA.3/Tanúsítási útvonal - Statikus tulajdonságok kezdeti értékadása

FMT_MSA.3/Tanúsítási útvonal - Statikus tulajdonságok kezdeti értékadása	FMT_MSA.1	Teljesül: FMT_MSA.1/Tanúsítványok - A biztonsági tulajdonságok menedzsmentje, FMT_MSA.1/Tanúsítvány érvényesítő adatok - A biztonsági tulajdonságok menedzsmentje
	FMT_SMR.1	Teljesül: FMT_SMR.1 Biztonsági szerepkörök
FMT_MSA.1/Tanúsítványok - A biztonsági tulajdonságok menedzsmentje	FDP_IFC.1	Teljesül: FDP_IFC.1/Tanúsítási útvonal - Részleges információ áramlás ellenőrzés
	FMT_SMR.1	Teljesül: FMT_SMR.1 Biztonsági szerepkörök
	FMT_SMF.1	Teljesül.
FMT_MSA.1/Tanúsítvány érvényesítő adatok - A biztonsági tulajdonságok menedzsmentje	FDP_IFC.1	Teljesül: FDP_IFC.1/Tanúsítási útvonal - Részleges információ áramlás ellenőrzés
	FMT_SMR.1	Teljesül: FMT_SMR.1 Biztonsági szerepkörök
	FMT_SMF.1	Teljesül.
FDP_ITC.2/ Tanúsítási útvonal - Felhasználói adatok importálása biztonsági tulajdonságokkal	FDP_IFC.1	Teljesül: FDP_IFC.1/Tanúsítási útvonal - Részleges információ áramlás ellenőrzés
	FTP_ITC.1 vagy FTP_TRP.1	Nem teljesül. Indoklás: a PKI-ban a nyilvános kulcs tanúsítványok önmagukat védik. A tanúsítási útvonal tanúsítványai és a visszavonási információk sértetlenségét egy magasabb szintű szervezet általi aláírás biztosítja, a gyökértanúsítványt (megbízható pontot) pedig az IT környezetben adják meg. A tanúsítási útvonal sikeres felépítése garantálja, hogy az útvonalban szereplő tanúsítványok hitelesek. A TOE által fogadott tanúsítványok és visszavonási adatok bizalmasság szempontból nem igényelnek védelmet.

	FPT_TDC.1	Teljesül: FPT_TDC.1/Tanúsítványok – TSF-ek közötti alapszintű TSF adat konzisztencia FPT_TDC.1/ Tanúsítvány visszavonási adatok – TSF-ek közötti alapszintű TSF adat konzisztencia
FPT_TDC.1/Tanúsítványok – TSF-ek közötti alapszintű TSF adat konzisztencia	Nincs függés.	-
FPT_TDC.1/ Tanúsítvány visszavonási adatok – TSF-ek közötti alapszintű TSF adat konzisztencia	Nincs függés.	-
FCS_COP.1/Aláírás ellenőrzés – Kriptográfiai műveletek	(FCS_CKM.1 vagy FDP_ITC.1 vagy FDP_ITC.2) és FCS_CKM.4	Teljesül: FDP_ITC.2/ Tanúsítási útvonal Felhasználói adatok importálása biztonsági tulajdonságokkal. Az FCS_CKM.4 nem teljesül. Indoklás: A nyilvános kulcsok nem igénylik, hogy védett módon történjen a megsemmisítésük.
FCS_COP.1/Lenyomat – Kriptográfiai műveletek	(FCS_CKM.1 vagy FDP_ITC.1 vagy FDP_ITC.2) és FCS_CKM.4	Nem teljesül. Indoklás: a lenyomatoló algoritmus nem igényel kulcsot, ezért nem szükséges a kulcsgenerálásra, kulcs megsemmisítésre, importálásra követelményt megfogalmazni.
FMT_SMR.1 Biztonsági szerepkörök	FIA_UID.1	Teljesül.
FIA_UID.1 Felhasználó azonosítása bármilyen művelet előtt	Nincs függés.	-
FIA_UAU.1 A hitelesítés időzítése	FIA_UID.1	Teljesül.
FIA_ATD.1 Felhasználói tulajdonságok megadása	Nincs függés.	-
FMT_SMF.1 Menedzsment funkciók megadása	Nincs függés.	-
FDP_ACC.1 Részleges hozzáférés ellenőrzés	FDP_ACF.1	Teljesül.
FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés	FDP_ACC.1	Teljesül.
	FMT_MSA.3	Teljesül: FMT_MSA.3/Mgmt
FMT_MSA.1/Mgmt A biztonsági tulajdonságok menedzsmentje	FDP_AFC.1	Teljesül.
	FMT_SMR.1	Teljesül.
	FMT_SMF.1	Teljesül.

FMT_MSA.3/Mgmt - Statikus tulajdonságok kezdeti értékadása	FMT_MSA.1	Teljesül: FMT_MSA.1/Mgmt
	FMT_SMR.1	Teljesül: FMT_SMR.1 Biztonsági szerepkörök

6.5 táblázat– A funkcionális követelmények közötti függések és vonatkozó indoklások

6.5 A garanciális biztonsági követelmények indoklása

A TOE értékelés garanciaszintje EAL4, ami megemelt alapszintű támadási potenciállal rendelkező támadók ellen, mérsékelt kockázati profilú környezetekben nyújt védelmet.

7 TOE összefoglaló előírás

7.1 A funkcionális biztonsági követelmények teljesítésének módja

A InfoSigno AC SDK az alábbi biztonsági funkciók megvalósításával teljesíti a funkcionális biztonsági követelményekben megfogalmazott célokat:

SF1 Nyilvános kulcs tanúsítványok érvényesség ellenőrzése
SF2 A visszavonási információk feldolgozása
SF3 Digitális aláírás ellenőrzése
SF4 Attribútum tanúsítvány érvényesség ellenőrzése
SF5 Attribútumok visszaadása és megjelenítése
SF6 ACTest menedzsment

7.1.1 SF1 Nyilvános kulcs tanúsítványok érvényesség ellenőrzése

Ez a biztonsági funkció végzi az attribútum tanúsítványhoz kapcsolódó szabványos nyilvános kulcs tanúsítványok, az AC tulajdonos nyilvános kulcs tanúsítványának, illetve az AC kibocsátó nyilvános kulcs tanúsítványának érvényesség ellenőrzését. A tanúsítási útvonal érvényességének ellenőrzése és a tanúsítási útvonal felépítése az RFC 5280 szabványnak megfelelően történik.

A nyilvános kulcs tanúsítványok esetén *háromféle* tanúsítványt különböztetünk meg:
- **Megbízható pontok**: Ezek önaláírt tanúsítványok, melyek nem igényelnek semmilyen érvényesség ellenőrzést. A megbízható pont (önaláírt tanúsítvány) általában tanúsítvány formában jelenik meg. A megbízható pont elsődleges célja a megkülönböztető név (Distinguished Name), a nyilvános kulcs és az algoritmus azonosító megállapítása. A megbízható pontok hozzáadását, törlését, menedzselését az InfoSigno AC SDK hatáskörén kívül kell kezelni az erre szolgáló konfigurációs fájl segítségével.
- **Közbenső tanúsítványok**: Ezek a hitelesítés-szolgáltatók (CA-k) számára kibocsátott tanúsítványok. Egy tanúsítási útvonal minden tanúsítványa ennek tekintendő, kivéve a megbízható pontot és a végtanúsítványt.
- **Végtanúsítvány:** A tanúsítási útvonal legutolsó tanúsítványa, melyet a szóban forgó egyed (aláíró) részére bocsátottak ki.

A nyilvános kulcs tanúsítványok érvényességének ellenőrzése során a tanúsítványhoz felépíthető teljes tanúsítási útvonalat figyelembe kell venni.

Az InfoSigno AC SDK a nyilvános kulcs tanúsítványok ellenőrzésekor a keyUsage, extendedKeyUsage és a basicConstraints biztonsággal kapcsolatos tanúsítvány kiterjesztési ellenőrzéseket veszi számításba.

A tanúsítási láncban lévő nyilvános kulcs tanúsítványokra vonatkozó visszavonási információk feldolgozását az **SF2.2 PKC visszavonási információk feldolgozása** funkció végzi.

7.1.2 SF2 A visszavonási információk feldolgozása

SF2.1 AC visszavonási információk feldolgozása
Az attribútum tanúsítványokra vonatkozó visszavonás állapot (ACRL) feldolgozása

A TOE támogatja mindkét alábbi visszavonási sémát:

- „visszavonás nélküli" séma („never revoke" scheme)
    - Az AC-k megjelölhetők a noRevAvail nem kritikus kiterjesztéssel, mely azt jelzi, hogy nincs elérhető visszavonási információ. Amennyiben a noRevAvail kiterjesztés nem szerepel, az AC kibocsátó ezzel közvetve azt is állítja, hogy valamilyen visszavonás állapot ellenőrzést támogat.
- „AC-beli mutató" séma („Pointer in AC" scheme)
    - Az AC-k rámutathatnak a visszavonás állapot információ forrására, egy crlDistributionPoints kiterjesztéssel.

Az attribútum tanúsítvány visszavonási lista (ACRL) érvényesség ellenőrzése során a TOE megvizsgálja a tanúsítványok ellenőrzésében szerepet játszó ACRL-ek érvényességét. A TOE csak teljes visszavonási lista feldolgozását kezeli a tanúsítvány crlDistributionPoint kiterjesztésben mutatott lista feldolgozásával, delta CRL-eket nem kezel.

SF2.2 PKC visszavonási információk feldolgozása
A nyilvános kulcs tanúsítványokra vonatkozó visszavonás állapot (CRL/OCSP) feldolgozása

A tanúsítvány visszavonási lista (CRL) érvényesség ellenőrzése során a TOE megvizsgálja a nyilvános kulcs tanúsítványok ellenőrzésében szerepet játszó CRL-ek érvényességét. A TOE csak teljes CRL feldolgozását kezeli a tanúsítvány crlDistributionPoint kiterjesztésben mutatott CRL feldolgozásával, delta CRL-eket nem dolgoz fel.

Az Online Certificate Status Protocol (OCSP) használata lehetővé teszi, hogy a TOE online tanúsítvány állapot kéréseket kezdeményezzen a nyilvános kulcs tanúsítványokra vonatkozóan, és ellenőrizze az OCSP válaszokat.

7.1.3 SF3 Digitális aláírás ellenőrzése

Ez a biztonsági funkció hajtja végre a tanúsítási útvonal nyilvános kulcs tanúsítványain és az attribútum tanúsítványon lévő digitális aláírás ellenőrzését. Kiszámítja az aláírt adat lenyomatát, és a tanúsítványban található nyilvános kulcs algoritmus és nyilvános kulcs felhasználásával ellenőrzi az aláírást.

A funkció bemeneteként szolgál a lenyomat készítéséhez használt algoritmus és az aláíró nyilvános kulcs tanúsítványa, valamint az aláíró neve. További bemeneti információt jelent a biztonsági funkció végrehajtásához az ellenőrzendő tanúsítvány tanúsítási útvonalának érvényesség ellenőrzését végrehajtó biztonsági funkció (**SF1 Nyilvános kulcs tanúsítványok érvényesség ellenőrzése**) által szolgáltatott eredmény. Az **SF3 Digitális aláírás ellenőrzése** funkció ellenőrzi a szóban forgó tanúsítvány digitális aláírásra való felhasználhatóságát is (keyUsage=digitalSignature be van kapcsolva), továbbá azt, hogy valóban a megfelelő alanyhoz tartozik-e a tanúsítvány.

A funkció végrehajtásához használandó kriptográfiai műveleteket az IT környezet részét képező, *2. ábra* szerinti alsóbb rétegek végzik.

7.1.4 SF4 Attribútum tanúsítvány érvényesség ellenőrzése

Jelen értékelés tárgya fő biztonsági funkciója az attribútum tanúsítványok érvényességének ellenőrzése, és ennek visszaadása a hívó IT környezeti alkalmazásnak, azaz az AC-t használó rendszernek, amely a saját igényei alapján használja fel a TOE által szolgáltatott eredményt, illetve biztonsági funkcionalitásában épít arra.

Az SF4 biztonsági funkció valósítja meg (illetve fogja össze) az AC érvényességnek megállapítását segítő alfunkciókat. Egy AC ellenőrzése a figyelembe vett RFC 3281 ajánlás alapján az alábbi **kötelező ellenőrzések**et foglalja magába:

1. Az AC birtokosát hitelesítő (AC-ben hivatkozott) nyilvános kulcs tanúsítvány megtalálása, majd ezen PC teljes hitelesítési útvonalának ellenőrzése az RFC 5280 szerint. (Lásd: **SF1 Nyilvános kulcs tanúsítványok érvényesség ellenőrzése** biztonsági funkciót.)

2. Az AC digitális aláírásának kriptográfiai ellenőrzése (Lásd: **SF3 Digitális aláírás ellenőrzése**), valamint az AC kibocsátójának teljes hitelesítési útvonalának ellenőrzése az RFC 5280 szerint (Lásd: **SF1 Nyilvános kulcs tanúsítványok érvényesség ellenőrzése** biztonsági funkciót.).

3. Az AC kibocsátójának nyilvános kulcs tanúsítványára az alábbiak ellenőrzése:
- megfelel az RFC 5280-ban meghatározott tanúsítvány profilnak,
- a kulcshasználat (**keyusage**) kiterjesztés engedélyezi a digitális aláírás ellenőrzésére való felhasználást,
- a CA (**basic constraint**) és a kulcshasználat (**keyusage**) kiterjesztés megtiltja a PC kibocsátást (cA: false, keyCertSign bit: 0)

4. Az AC kibocsátója egy közvetlenül megbízható AC **kibocsátó** (a közvetlen megbízhatóság konfigurálással vagy más módon érhető el).

5. Az AC kiértékelésének időpontja az AC érvényességén belül van. (azaz a kiértékelés időpontja nagyobb vagy egyenlő, mint notBeforeTime, egyúttal kisebb vagy egyenlő, mint notAfterTime). Egyes alkalmazásokban az ellenőrzés időpontja eltérhet az aktuális időponttól.

6. Az AC által tartalmazott valamennyi kritikus kiterjesztést az ellenőrző alkalmazásnak támogatnia kell (azaz fel kell ismernie a kiterjesztés értékét, a kiterjesztés értékéről meg kell állapítania, hogy elfogadható-e vagy sem, nem elfogadható kiterjesztés érték esetén az AC-t vissza kell utasítani), ellenkező esetben az AC-t vissza kell utasítani.

7. Az AC visszavonási információinak ellenőrzése. Ez az ellenőrzés a két lehetséges visszavonási sémában eltérő szabályokat tartalmaz.
(Lásd: **SF2.1 AC visszavonási információk feldolgozása** biztonsági funkciót.)

7.1.5 SF5 Attribútumok visszaadása és megjelenítése

Ez a funkció biztosítja azt, hogy az ACTest és az InfoSigno AC SDK ellenőrizze az AC-ben szereplő attribútumokat, és megjelenítse a vonatkozó attribútumokat, melyek az alábbiak lehetnek:

- **AuditIdentity**: Az AuditIdentity mező visszaadott értékével garantálható, hogy az AC használója ne mentse le semmilyen logba vagy működési adatbázisba az AC tulajdonosának (Holder) adatait, hanem csak az AuditIdentity értékét kezelje.
- **authorityKeyIdentifier**: Az AC-t kiadó AA tanúsítvány aláíró kulcsának azonosítója.
- **TargetInformation**: Ez határozza meg, hogy mely szerverek/szolgáltatások fogadhatják el az AC-t. Egy adott AC-t csak az a szolgáltatás fogadhatja el, amelyik magát azon a néven kezeli, más hívó szolgáltatásnak el kell utasítania.
- **authenticationInfo**: Az AC birtokost azonosító attribútum típus, egy szerver/szolgáltatás felé azonosítja az AC tulajdonosát. Az AC ellenőrzést végző TOE ezt az információt csak továbbítja az AC-t használó alkalmazás felé.
- **accessIdentity**: Az AC birtokost azonosítja egy szerver/szolgáltatás felé (kiegészítő információkkal). Jelszót nem tartalmaz.
- **chargingIdentity**: Az AC birtokost azonosítja számlázási célokból.
- **group**: Az AC birtokos csoporttagságait azonosítja.
- **role**: Az AC birtokos szerepeit azonosítja.
- **clerance**: Az AC birtokos (biztonsági címkézéssel kapcsolatos) felhatalmazásait adja meg.
- **egyedi attribútumok.**

7.1.6 SF6 ACTest menedzsment

Ez a biztonsági funkció kezeli az InfoSigno AC SDK és ACTest alkalmazás konfigurálásával, felhasználók beállításával és biztonsági paraméterek beállításával kapcsolatos feladatokat. Az alkalmazás az adminisztrátori és felhasználói szerepköröket elkülönítve biztosít lehetőséget a különböző AC-k ellenőrzéséhez, nyolc darab ún. portleten keresztül. Nyilvános kulcs tanúsítvánnyal rendelkező felhasználók számára biztosítja a felhasználókhoz rendelt attribútum tanúsítványok ellenőrzését. Az alkalmazás paramétereinek beállítását és a felhasználók felvételét az adminisztrátor végzi.

7.2 A biztonsági funkciók és követelmények megfeleltetése

Az alábbi táblázat a biztonsági funkciókhoz hozzárendeli a 6. fejezetben szereplő funkcionális követelményeket.

Biztonsági funkció	Funkcionális követelmény
SF1 Nyilvános kulcs tanúsítványok érvényesség ellenőrzése	FDP_IFC.1/INIC Részleges információ áramlás ellenőrzés
	FDP_IFF.1/INIC - Egyszerű biztonsági tulajdonságok
	FMT_MSA.3/INIC - Statikus tulajdonságok kezdeti értékadása
	FMT_MSA.1/INIC A biztonsági tulajdonságok menedzsmentje
SF4 Attribútum tanúsítvány érvényesség ellenőrzése	FDP_IFC.1/Elektronikus aláírás és attribútumok - Részleges információ áramlás ellenőrzés
	FDP_IFF.1/Elektronikus aláírás és attribútumok Egyszerű biztonsági tulajdonságok
	FMT_MSA.3/Elektronikus aláírás és attribútumok - Statikus tulajdonságok kezdeti értékadása
	FMT_MSA.1 Elektronikus aláírás és attribútumok - A biztonsági tulajdonságok menedzselése
	FDP_ITC.2/Elektronikus aláírás és attribútumok Felhasználói adatok importálása biztonsági tulajdonságokkal
SF4 Attribútum tanúsítvány érvényesség ellenőrzése **SF5 Attribútumok visszaadása és megjelenítése**	FDP_IFC.1/AC érvényesség ellenőrzése - Részleges információ áramlás ellenőrzés
	FDP_IFF.1/AC érvényesség ellenőrzése - Egyszerű biztonsági tulajdonságok
	FDP_ETC.2/AC ellenőrzés eredménye - A felhasználói adatok exportálása biztonsági tulajdonságokkal
	FMT_MSA.3/AC ellenőrzés eredménye - Statikus tulajdonságok kezdeti értékadása
	FMT_MSA.1/AC ellenőrzés eredménye - A biztonsági tulajdonságok menedzselése
	FMT_SMR.1 Biztonsági szerepkörök
	FIA_UID.1 Felhasználó azonosítása bármilyen művelet előtt
	FIA_UAU.1 A hitelesítés időzítése
	FIA_ATD.1 Felhasználói tulajdonságok megadása
	FDP_ACC.1 Részleges hozzáférés ellenőrzés

	FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés
SF1 Nyilvános kulcs tanúsítványok érvényesség ellenőrzése **SF2 Visszavonási információk feldolgozása** **SF3 Digitális aláírás ellenőrzése**	FDP_IFC.1/Tanúsítási útvonal - Részleges információ áramlás ellenőrzés
	FDP_IFF.1/Tanúsítási útvonal - Egyszerű biztonsági tulajdonságok
	FMT_MSA.3/Tanúsítási útvonal - Statikus tulajdonságok kezdeti értékadása
	FMT_MSA.1/Tanúsítványok - A biztonsági tulajdonságok menedzsmentje
	FMT_MSA.1/Tanúsítvány érvényesítő adatok - A biztonsági tulajdonságok menedzsmentje
	FDP_ITC.2/ Tanúsítási útvonal - Felhasználói adatok importálása biztonsági tulajdonságokkal
	FPT_TDC.1/Tanúsítványok – TSF-ek közötti alapszintű TSF adat konzisztencia
	FPT_TDC.1/ Tanúsítvány visszavonási adatok – TSF-ek közötti alapszintű TSF adat konzisztencia
SF3 Digitális aláírás ellenőrzése	FCS_COP.1/Aláírás ellenőrzés – Kriptográfiai műveletek
	FCS_COP.1/Lenyomat – Kriptográfiai műveletek
SF6 ACTest menedzsment	FIA_UID.1 Felhasználó azonosítása bármilyen művelet előtt
	FIA_UAU.1 A hitelesítés időzítése
	FIA_ATD.1 Felhasználói tulajdonságok megadása
	FMT_SMF.1 Menedzsment funkciók megadása
	FMT_MSA.1/Mgmt A biztonsági tulajdonságok menedzsmentje
	FMT_MSA.3/Mgmt - Statikus tulajdonságok kezdeti értékadása
	FMT_SMR.1 Biztonsági szerepkörök

7-1. táblázat A biztonsági funkciók és funkcionális követelmények kapcsolata

A 7-2. táblázat és az alatta lévő indoklás azt mutatja, hogy a biztonsági funkciók egységes egészet alkotnak, együtt járulnak hozzá az InfoSigno AC SDK céljának megvalósításához.

A sorbeli funkció melyik oszlopbeli funkcióhoz járul hozzá	**SF1**	**SF2**	**SF3**	**SF4**	**SF5**	**SF6**
SF1 Nyilvános kulcs tanúsítványok érvényesség ellenőrzése	-	-	x	x	-	-
SF2 Visszavonási információk feldolgozása	x	-	-	x	-	-
SF3 Digitális aláírás ellenőrzése	x	x	-	x	-	-
SF4 Attribútum tanúsítvány érvényesség ellenőrzése	-	-	-	-	x	-
SF5 Attribútumok visszaadása	-	-	-	-	-	-
SF6 ACTest menedzsment	x	x	x	x	x	-

7-2. táblázat A biztonsági funkciók közötti kapcsolatok

Az SF5 biztonsági funkció a TOE kimenetét szolgáltatja a hívó alkalmazás felé.
A többi funkcióról a táblázat megmutatja, hogy kölcsönösen kiegészítik egymást a TOE biztonsági szolgáltatásainak teljesítése érdekében.
Az SF6 ACTest menedzsment biztonsági funkció a TOE alap biztonsági funkcióinak demonstrálását biztosító keretalkalmazás működésével kapcsolatos funkcióival hozzájárul az összes többi funkció sikeres teljesítéséhez.

7.3 Önvédelem a fizikai és logikai hamisítás ellen

A TOE azzal biztosítja a biztonsági funkcionalitás hamisíthatatlanságát, hogy minden futtatható kódot tartalmazó elemén PKI alapú kód védelmet alkalmaz. A bináris állományok védelme a Microsoft SDK által biztosított signtool (6.0.6000.16384) alkalmazásával valósul meg, RSA digitális aláírások és SHA1 lenyomatképzések alkalmazása mellett.

A logikai hamisítás elleni védelmet biztosítja továbbá az, hogy a felhasználók csak akkor férhetnek hozzá a TOE biztonsági funkcióinak bemutatását szolgáló felülethez, ha egy külön erre kijelölt szerepkör ehhez beállított bizonyos paramétereket, felvette a felhasználót és hozzárendelte az attribútum tanúsítványokat. A felhasználó az ellenőrzési paramétereket az egyes tesztek közben nem tudja módosítani.

7.4 Önvédelem a megkerülés ellen

Az InfoSigno AC SDK v1.0.0.4 rendszerben minden felhasználó számára az egyes ellenőrzések végrehajtása előtt kötelező belépés (login) van, és bár a tesztek leírása megtekinthető, de csak létező felhasználói név és létező, az adott felhasználóhoz rendelt AC-k birtokában lehet a biztonsági funckionalitást ténylegesen használni.

8 Rövidítések, fogalmak

Rövidítés	Megnevezés	Jelentés és/vagy leírás
AA	Atribute Authority	Az AC-t kibocsátó szervezet, RFC 3281-ben ugyanaz, mint az AC kibocsátó
AC	Attribute Certificate	Attribútum tanúsítvány
ACRL	Attribute Certificate Revocation List	Attribútum tanúsítvány visszavonási lista
CA	Certification Authority	Hitelesítés szolgáltató
CRL	Certificate Revocation List	Tanúsítvány visszavonási lista
OCSP	Online Certificate Statzus Protocol	Online Tanúsítvány állapot protokoll
PC, PKC	Public Key Certificate	nyilvános kulcs tanúsítvány
PKI	Public Key Infrastructure	nyilvános kulcs infrastruktúra
PP	Protection Profile	Védelmi profil
SDK	Sowtware Development Kit	
TOE	Target of Evaluation	Értékelés tárgya (jelen esteben InfoSigno AC SDK v1.0.0)
TSF	TOE Security Function	A TOE biztonsági funkciói (lásd 7. fejezetet jelen TOE biztonsági funkcióihoz)