Tanúsítási JELENTÉS

InfoSigno for Developers
fejlesztő készlet
minősített elektronikus aláíráshoz
v1.0.0 r119

HUNG-TJ-31-2006

Verzió:	1.0
Fájl:	HUNG_TJ_31_2006_v10.pdf
Minősítés:	Nyilvános
Oldalak:	39

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2006.05.19	• A szerkezet felállítása.
v0.8	2006.05.21	• A tanúsítás eredményeit tartalmazó teljes változat.
v0.81	2006.05.22	• Apró módosítás.
v0.9	2006.05.28	• Utolsó egyeztetésre kiadott változat
v1.0	2006.05.29.	• Végleges verzió

A tanúsítási jelentést készítette:

Farkas Gábor
HunGuard Kft
Tanúsítási divízió

Tartalomjegyzék

1 Összefoglaló

1.1 Az értékelés jellemzői

Az értékelt termék neve:	**InfoSigno for Developers fejlesztő készlet minősített elektronikus aláíráshoz**
Verzió szám:	**1.0.0**
Rövid elnevezés:	**InfoSigno v1.0.0**
Az értékelt termék típusa:	fejlesztő készlet (könyvtár)
Értékelő szervezet:	HunGuard Kft.
Értékelés befejezése:	2006. május 08
Az értékelés módszere:	a MIBÉTS séma értékelési módszertana1
Az értékelés garanciaszintje:	kiemelt (EAL4)
Az értékelt termék funkcionalitása:	A fejlesztő készlet által támogatott nyilvános kulcsú szolgáltatások az alábbiak: • elektronikus aláírás létrehozása; • elektronikus aláírás ellenőrzése, a kapcsolódó tanúsítvány útvonal felépítési és érvényesítési szolgáltatásokkal; • aszimmetrikus (kulcsátvitelhez) és szimmetrikus kulcsú (adatátvitelhez) titkosítás és dekódolás; • időbélyegzés (kérése és ellenőrzése).
Konfigurációs követelmények:	Szoftver konfiguráció: • Operációs rendszer: Windows XP/2003 CE, • CURL v7.15.1, • OpenSSL v 0.9.8.a • XERXES C++ v2.7.0 • ZLIB v1.2.3.

[1] Az értékelés az alábbi dokumentumokban leírt módszertant és eljárásrendet követte:
- 1. számú MIBÉTS kiadvány: **A MIBÉTS nemzeti séma általános modellezése** /0.95 verzió, 2005 február/,
- 2. számú MIBÉTS kiadvány: **Az értékelés és a tanúsítás folyamatai** /0.95 verzió, 2005 február/,
- 3. számú MIBÉTS kiadvány: Az értékelés módszertana 1 - **A biztonsági előirányzat értékelésének módszertana** /0.95 verzió, 2005 február/,
- 3. . számú MIBÉTS kiadvány: Az értékelés módszertana 4 **- A kiemelt garanciaszint értékelésének módszertana** /0.95 verzió, 2005 február/

2 Azonosítás

Az értékelt termék neve:	**InfoSigno for Developers fejlesztő készlet minősített elektronikus aláíráshoz**
Verzió szám:	**1.0.0**
Az értékelt termék alkotó elemei (a felhasználókhoz, vagyis a fejlesztő készlet felhasználásával alkalmazást fejlesztőkhöz kiszállított tételek):	• infosigno.dll v1.0.0 R119 • InfoSigno dokumentáció

3 Biztonsági szabályzat

Ez a fejezet azokat a szabályokat írja le, melyek alapján az InfoSigno v1.0.0 irányítja az erőforrásaihoz való hozzáférést, s ezen keresztül minden általa ellenőrzött információt és szolgáltatást.
Először az InfoSigno v1.0.0 két üzemmódját határozzuk meg, melyekre eltérő szabályok vonatkoznak. Ezt követően a szabályokat érvényre juttató biztonsági funkciókat tekintjük át.

3.1 Üzemmódok

A TOE két használati esetet különböztet meg:

- Fokozott biztonságú aláírás létrehozás használati esete
  - A TOE-t biztonságos aláírás létrehozó eszköz nélkül használják elektronikus aláírások generálására és ellenőrzésére. Ezen belüli esetek:
    - KHE (kriptográfiai hardver eszköz) használata;
    - PKCS#12 szoftveres kulcstároló állomány használata
    - Windows tanúsítványtár.
- Minősített elektronikus aláírás létrehozás használati esete
  - Minősített aláírás létrehozása esetén kötelező a BALE használata, illetve nem megbízható környezetben a BALE és az aláírás létrehozó alkalmazás (TOE) között megbízható útvonal kiépítésére van szükség. Az aláírás létrehozásához használt tanúsítványnak minősítettnek kell lennie. Az az InfoSigno v1.0.0BALE-hez való hozzáférést PKCS#11 interfészen keresztül valósítja meg.

3.2 Biztonsági funkciók

A TOE által megvalósított biztonsági funkciók a követezőek:

- BF1 Aláírás létrehozása
- BF2 Digitális aláírás ellenőrzés
- BF3 Üzenet digitális aláírása
- BF4 Elektronikus aláírás ellenőrzése
- BF5 Időbélyeg kérés
- BF6 Időbélyeg ellenőrzés
- BF7 Tanúsítvány útvonal felépítése és érvényesség ellenőrzése
- BF8 Titkosítás, megoldás
- BF9 A TSF védelme és menedzsmentje

3.2.1 BF1 Aláírás létrehozása

A **BF1 Aláírás létrehozása** biztonsági funkció hozza létre az aláírói dokumentumra és az aláírási információkra az elektronikus aláírást az aláírói magánkulcs felhasználásával.

Az InfoSigno v1.0.0 lehetőséget biztosít fokozott biztonságú és minősített elektronikus aláírások létrehozására. Fokozott biztonságú aláírások esetén képes fájlban (PKCS#12-es formátumban), Microsoft tanúsítványtárban, vagy kriptográfiai hardver eszközben (KHE) tárolt magánkulcs használatára.
(Fájl formátumban nem csak PKCS#12-es privát kulcsfájlokat, hanem tanúsítványokat és CRL-eket is kezel a rendszer.)
A magánkulcs közvetlen aktivizálása előtt a TOE a paraméterként kapott aláíró hitelesítő adatot (vagy a kapott függvénnyel bekért) hitelesítő adatot használja az aláíró hitelesítéséhez.

Minősített elektronikus aláírás létrehozása esetén az InfoSigno v1.0.0 kommunikációt kezdeményez az aláírás létrehozását ténylegesen végző BALE-vel. Az aláíró által kiválasztott tanúsítványhoz tartozó magánkulccsal és az ennek megfelelő algoritmussal (ami az InfoSigno esetén az RSA algoritmus 1024 bit kulcshosszal) létrehozza az aláírást. A BALE eszköz végzi a magánkulcs aktivizáláshoz szükséges aláíró hitelesítő adat bekérést. Ez esetben az aláírás létrehozásához használt tanúsítványnak minősített tanúsítványnak kell lennie (qCStatement kiterjesztés használatával, ETSI TS 101 862 v1.3.3, és a keyUsage kiterjesztésben csak a nonRepudiation bit lehet beállítva.

Fokozott biztonságú aláírás létrehozása esetén

- Aktivizálja a PKCS#12-es fájlban tárolt magánkulcsot, és az RSA algoritmus és 1024 bit kulcshossz használatával létrehozza a lenyomatra az aláírást, amit beletesz az XML aláírásba.

Vagy

- Aktivizálja a Microsoft tanúsítványtárában tárolt magánkulcsot, és az RSA algoritmus és 1024 bit kulcshossz használatával létrehozza a lenyomatra az aláírást, amit beletesz az XML aláírásba.

Vagy

- Kezdeményezi a KHE (Kriptográfiai hardver eszköz) felé az aláírás létrehozását, majd a kapott aláírás érték felhasználásával összeállítja az XML aláírást.

Fokozott biztonságú aláírás létrehozása esetén a keyUsage kiterjesztésben a kötelezően beállított nonRepudiation bit mellett opcionálisan a digitalSignature bit lehet még beállítva.

A funkció által létrehozott elektronikus aláírás formátuma megfelel a ETSI TS 101 903 v1.2.2 dokumentumban leírt XAdES-C formátumnak.

Lenyomat készítés
Az aláírás létrehozás biztonsági funkció ezen alfunkciója hozza létre a lenyomatot, amire az aláírás készül. Az aláírás létrehozása során az aláírandó adatokra alkalmazott lenyomatoló algoritmus: SHA-1 [FIPS 180-1].

Megengedett dokumentum formátumok:
Az InfoSigno v1.0.0 háromféle dokumentum formátum aláírását engedi meg: XML, JPEG, TXT, PNG.
Aláírás előtt megvizsgálja a kapott dokumentum kiterjesztését; ha nem a fentiek egyike, de WORD, NOTES vagy HTML formátum, akkor figyelmeztetést ad vissza a hívó félnek, egyébként nem engedi a dokumentum hozzáadását.

Az aláírást az InfoSigno v1.0.0 az alábbi szabályok alapján készíti el:

- Az elektronikus aláírásban csak az aláíró tanúsítvány azonosítója szükséges.
- A [keyinfo] elemben az aláíró tanúsítványt kell megadni.
- A kötelező aláírási tulajdonságok:
- Aláírás ideje
- Aláírási szabályzat azonosítója
- Aláírói tanúsítvány

3.2.2 BF2 Digitális aláírás ellenőrzés

Az InfoSigno v1.0.0 ezen biztonsági funkciójának képessége biztosítja egy létrehozott digitális aláírás érték ellenőrzését. A funkció kiszámítja az aláírt adat lenyomatát, majd az aláírónak az aláírásba foglalt nyilvános kulcs tanúsítványában található nyilvános kulcs és az aláírási algoritmus felhasználásával ellenőrzi a digitális aláírást. Amennyiben a kiszámított lenyomat és a digitális aláírás ellenőrzése során kapott érték megegyezik, akkor a digitális aláírás érték helyes.

3.2.3 BF3 Üzenet digitális aláírása

Az InfoSigno v1.0.0 ezen biztonsági funkciója az adat sértetlenség követelmény biztosítása érdekében digitális aláírást képes létrehozni felhasználói adatokra. A funkció az SHA-1 algoritmust használja az adat lenyomat elkészítésére, és ezt kódolja az RSA/1024 bites aláíró algoritmussal.

3.2.4 BF4 Elektronikus aláírás ellenőrzése

Ez a biztonsági funkció valósítja meg – a **BF2 Digitális aláírás ellenőrzés** biztonsági funkciónak csak az aláírás érték kriptográfiai érvényesség ellenőrzésével szemben –, az elektronikus aláírás ellenőrzését az aláíró tanúsítványának felhasználásával.
A funkció paraméterezésétől függően kezdeti vagy utólagos ellenőrzést végez.
A kezdeti ellenőrzés folyamata három lépésből áll: első lépésben a funkció megnézi, hogy kapcsolódik-e időbélyeg az aláíráshoz. Amennyiben nem, akkor végrehajtja a **BF5 Időbélyeg kérés** és a **BF6 Időbélyeg ellenőrzés** biztonsági funkciókat. Az ellenőrzés második lépéseként az aláírás érvényességének megállapításához szükséges információk összegyűjtését végzi. Ezt a **BF7 Tanúsítványlánc felépítése és érvényesség ellenőrzése** biztonsági funkció végzi el. Végül a harmadik lépésben kerül sor az elektronikus aláírás ellenőrzésére.
A kezdeti ellenőrzésnek három lehetséges kimeneti állapota lehet:

- befejezetlen;
- sikeres;
- sikertelen.

Sikeres esetben befejeződött az összes érvényesítő adat összegyűjtése, és az aláírás ezek alapján érvényesnek tekinthető.
Sikertelen ellenőrzés olyan esetben történhet, ha például az aláírás formátuma nem megfelelő vagy a digitális aláírás értéke érvénytelen.
Befejezetlen esetben nincs elegendő információ az aláírás érvényességének pozitív megállapításhoz.

Az utólagos ellenőrzés folyamata a már korábban (a kezdeti ellenőrzés során) begyűjtött információk alapján közvetlenül (BF7 aktivizálása nélkül) végrehajtja az elektronikus aláírás ellenőrzését. Csak két lehetséges kimeneti állapota lehet:

- sikeres;
- sikertelen (ez utóbbi azt az esetet is lefedi, amikor nem áll rendelkezésre elegendő információ az aláírás ellenőrzéséhez).

A funkció által ellenőrizni képes elektronikus aláírás formátumok: XML digital signature szabvány, XAdES v1.2.2.

3.2.5 BF5 Időbélyeg kérés

Az InfoSigno v1.0.0 biztosítja az időbélyeg kérés képességét **az aláírás ellenőrzése során**. Az RFC 3161-ben specifikáltaknak megfelelően összeállítja az időbélyeg kérést a hash értékkel, és elküldi a külső időbélyeg szolgáltatóhoz.

3.2.6 BF6 Időbélyeg ellenőrzés

Az InfoSigno v1.0.0 a szolgáltatótól kapott időbélyeg választ importálja, és elvégzi a szükséges ellenőrzéseket: ellenőrzi a válasz státuszt, azt, hogy érvényes-e az időbélyegen lévő aláírás, ellenőrzi az időbélyeg aláírásához használt tanúsítvány érvényességét.

3.2.7 BF7 Tanúsítási útvonal felépítése és érvényesség ellenőrzése

Ez a biztonsági funkció végzi az aláíró tanúsítványból kiindulva a megbízható pontig (gyökértanúsítványig) tartó tanúsítvány lánc elemeinek összegyűjtését.
Az InfoSigno v1.0.0 az IT környezet által sértetlenségében megvédett konfigurációs fájlból olvassa be a kulcsadat tárolók elérését, amiket a tanúsítási útvonal érvényesség ellenőrzése során felhasznál. Ezen fájl tartalmának módosítása kívül esik a TOE hatókörén.

A tanúsítási útvonal felépítéséhez az InfoSigno betöltésekor lefut egy ***inicializáló*** rutin, amely elvégzi a használt tanúsítványtárak inicializálást.
Ehhez az alábbi tanúsítványtár funkciókat biztosítja:

- megbízható pont (gyökér tanúsítvány) hozzáadása
- megbízható pontok (gyökér tanúsítványok) listázása
- közbenső tanúsítvány hozzáadása
- közbenső tanúsítványok listázása
- végfelhasználói tanúsítvány hozzáadása
- végfelhasználói tanúsítványok listázása
- PKCS#12 formátumú magánkulcsok hozzáadása
- CRL tárolása

Az InfoSigno v1.0.0 az érvényesség ellenőrzés során a végtanúsítványra **visszavonási információkat (CRL) gyűjt** be. A paraméterezhető türelmi idő letelte után megismétli a visszavonási információk lekérését, hogy az aláírás érvényességének ellenőrzése a legfrissebb CRL-ek alapján történjen meg. Ellenőrzi a tanúsítványokon és a CRL-eken lévő aláírásokat.
A **tanúsítványlánc tanúsítványai**ra megnézi, hogy az érvényességi idejükbe beleesik-e az aláíráshoz csatolt időbélyegben szereplő időpont. Továbbá megvizsgálja, hogy szerepel-e a visszavonási listán a tanúsítvány, és amennyiben igen, akkor az időbélyeg által meghatározott időpontban visszavont állapotú volt-e.

3.2.8 BF8 Titkosítás, megoldás

Az InfoSigno v1.0.0 titkosítás és kapcsolódó megoldás biztonsági funkciója aszimmetrikus RSA/1024 algoritmust használ a szimmetrikus AES/256 rejtjelezés/megoldás által használt titkos kulcs továbbítására.
Támogatott kulcs átviteli algoritmusok:

- RSA algoritmus 1024 bit kulcshosszal.

Támogatott szimmetrikus titkosítási algoritmusok:

- • AES 256 bit [FIPS PUB 197].

A küldő fél a címzett nyilvános kulcsát tartalmazó tanúsítvány felhasználásával rejtjelezi az adatok titkosításához használt véletlen kulcsot.
A küldő fél a támogatott szimmetrikus algoritmus és a hozzá tartozó kulcshossz alapján rejtjelezi a továbbítandó adatokat.
A fogadó fél a saját magánkulcsának felhasználásával dekódolja az adatok titkosításához használt véletlen kulcsot.
A fogadó fél a támogatott szimmetrikus algoritmus és a hozzá tartozó kulcshossz alapján megoldja a kapott rejtjeles adatokat.

3.2.9 BF9 A TSF védelme és menedzsmentje

Ez a biztonsági funkció az alábbi feladatok végrehajtására képes:

- PIN kód közvetlen használat utáni törlése a memóriából;
- magánkulcs közvetlen használat utáni törlése a memóriából;
- PIN kód cseréje PKCS#12 formátumú kulcstároló fájl esetén.

4 Feltételezések és hatókör

Az értékelés pozitív következtetése az alábbi feltétel csoportok teljesülésén múlik:

- a biztonsági előirányzat feltételezései (az értékelés tárgyát képező fejlesztő készlet biztonságához szükséges, az informatikai környezetre vonatkozó feltételek),
- a biztonságos felhasználás feltételei (az értékelés tárgyát képező fejlesztő készlet felhasználásával készített alkalmazások biztonságához szükséges, ezen alkalmazások megfelelő kialakítására vonatkozó feltételezések, javaslatok).

4.1 Feltételezések az InfoSigno v1.0.0 informatikai környezetére

Az alábbi (a biztonsági előirányzatban is szereplő) feltételezések az informatikai környezetre vonatkoznak:

1. Az engedéllyel rendelkező felhasználók (alkalmazás fejlesztők) megbízhatók a tekintetben, hogy a számukra kijelölt funkciókat megfelelően hajtják végre (AE.Authorized_Users).
2. Az InfoSigno v1.0.0-t megfelelően telepítik és konfigurálják (AE.Configuration).
3. Fokozott biztonságú elektronikus aláírás létrehozása esetén az InfoSigno v1.0.0 által meghívott kriptográfiai funkciók (OpenSSL) megbízhatónak tekinthetők az elvárt kriptográfiai funkciók megvalósítása terén. (AE.Crypto_Module).
4. Minősített elektronikus aláírás létrehozása esetén az InfoSigno v1.0.0 környezete tartalmaz egy vagy több NHH által nyilvántartott, tanúsított BALE-t, mely(ek) tárolják és védik az aláíró magánkulcsát, illetve végrehajtják a digitális aláírást (AE.Crypto_Module).
5. Az InfoSigno v1.0.0 környezete fizikailag biztonságos (AE.Physical_Protection).
6. A tanúsítvány és tanúsítvány visszavonási információk az InfoSigno v1.0.0 rendelkezésére állnak (AE.PKI_Info)
7. Az InfoSigno v1.0.0 környezete GMT formában és a megkívánt pontossággal gondoskodik a pontos rendszeridőről (AE.Time).
8. Az InfoSigno v1.0.0 környezete biztosítja az időbélyegzés szolgáltatóhoz való hozzáférést (AE.TimeStamp).

4.2 A biztonságos felhasználás egyéb feltételei

1. Az InfoSigno v1.0.0 kriptográfiai modul az önkibocsátott (self issued) tanúsítványokat nem támogatja. Nem támogatja azon tanúsítványláncok ellenőrzését sem, ahol a CRL-t más tanúsítvánnyal ellenőrzik, mint a végfelhasználó tanúsítványokat. A tanúsítványlánc felépítésekor a kibocsájtó-tulajdonos egyezőséget binárisan ellenőrzi. Ezért csak olyan környezetben szabad alkalmazni, ahol önkibocsátott (self issued) tanúsítvány a tanúsítványláncba nem fordul elő, a CRL-t és a végfelhasználói tanúsítványt ugyanazzal a CA tanúsítvánnyal kell ellenőrizni, valamint a tanúsítványláncban a kibocsájtó-tulajdonos név egyezőség bináris.
2. Az InfoSigno v1.0.0 fejlesztő készlett használó aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírási folyamatba ne avatkozhassanak be olyan nem megbízható rendszer és alkalmazási folyamatok, perifériák és kommunikációs csatornák, amelyek nem szükségesek az aláírás-létrehozás alkalmazás működéséhez.
3. Az InfoSigno v1.0.0 programozói könyvtár működtetési környezetében biztosítani kell az ALE eszköz jelszavának lecserélhetőségét.
4. Az InfoSigno v1.0.0 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:

a. vírusok ne ronthassák el az aláíró alkalmazást és az általa meghívott egyéb aláíró összetevőket, valamint
b. az esetlegesen vírussal fertőzött aláíró összetevőket megfelelően helyre lehessen állítani.

5. Az InfoSigno v1.0.0 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék Az InfoSigno v1.0.0 programozói könyvtár funkcionális összetevőinek sértetlenségét megakadályozva, hogy behatolók elrontsák ezt.
6. Az InfoSigno v1.0.0 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az InfoSigno v1.0.0 programozói könyvtárat, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.

4.3 Az értékelés hatóköre

Az értékelés figyelembe vette a biztonsági előirányzat valamennyi fenyegetését és az InfoSigno v1.0.0 valamennyi biztonsági funkcióját.

5 Az InfoSigno v1.0.0 szerkezeti leírása

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

- elektronikus aláírás létrehozása;
- elektronikus aláírás ellenőrzése, a kapcsolódó tanúsítvány útvonal felépítési és érvényesítési szolgáltatásokkal;
- aszimmetrikus (kulcsátvitelhez) és szimmetrikus kulcsú (adatátvitelhez) titkosítás és dekódolás;
- időbélyegzés (kérése és ellenőrzése).

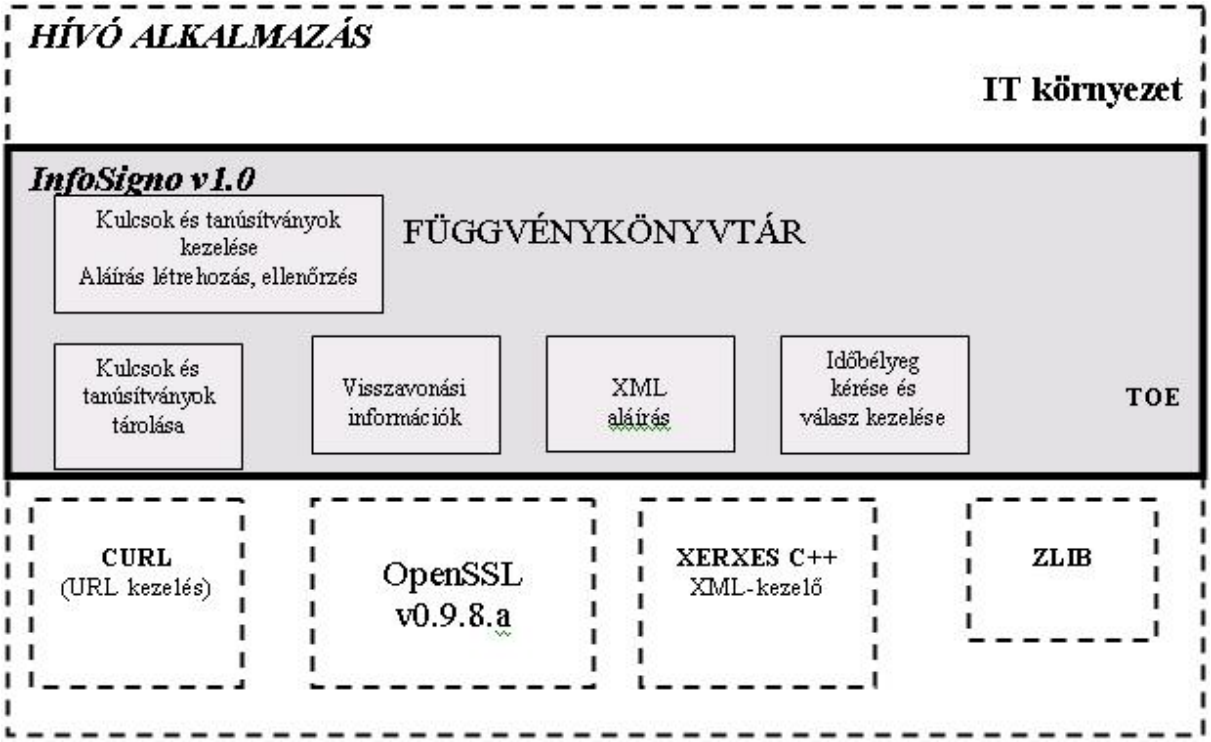
Ennek alapján az InfoSigno v1.0.0 fejlesztői készlet segítségével alkalmazások széles köre fejleszthető, melyek a nyilvános kulcsú technológia alapján bizalmasságot, sértetlenséget, hitelesítést és letagadhatatlanságot biztosító szolgáltatásokat képesek nyújtani.

Az InfoSigno v1.0.0 fejlesztői függvénykönyvtár az alábbi nyilvános kulcs szolgáltatásokat támogatja:

- Biztonságosan kezel kulcsokat, megbízható pontokat és tanúsítványokat.
- Elfogad és feldolgoz X509 v3 nyilvános kulcs tanúsítványokat.
- Képes a szükséges tanúsítványok és visszavonási adatok megszerzésére.
- Ellenőrzi minden tanúsítvány érvényességét, az RFC 3280-ban leírt eljárások felhasználásával a 4.2 pontban leírt megkötések mellett, beleértve a visszavonás ellenőrzést is.
- RFC3161 alapján kezel pontos és megbízható időforrást a tanúsítványok, visszavonási adatok és alkalmazási adatok dátumának, idejének ellenőrzése érdekében.
- Minősített elektronikus aláírás létrehozása esetén együttműködik a magyar jogszabályok által megkövetelt módon minősített aláírás létrehozásához szükséges tanúsított BALE eszközzel. Fokozott biztonságú elektronikus aláírások esetén képes szabványos szoftveres kulcstároló állományok vagy kriptográfiai hardver eszköz biztonságos kezelésére.
- Digitális aláírás algoritmusa RSA 1024 bit kulcsméretig a lenyomatoló algoritmus SHA-1 a feltöltés pkcs1-v1_5
- Xades-C aláírás formátum
- Gyűjti, tárolja és karbantartja a digitális aláírás jövőbeni ellenőrzéséhez szükséges adatokat.
- Képes automatikusan választani több magán rejtjelező kulcsból, ha nyilvános kulcs alapú megoldást végez.

5.1 Architektúra

Az 1. ábra az InfoSigno v1.0.0 struktúráját és az IT környezetbe való beágyazódását mutatja be.



1. ábra Az InfoSigno v1.0.0 és környezete

Az InfoSigno v1.0.0 közvetlen interfészeit azok az OpenSSL és egyéb alapul szolgáló hívások képezik, amelyek a magasabb szintű alkalmazások, függvénykönyvtárak fejlesztői számára biztosítanak publikus függvényeket.

A TOE közvetlenül nem kezdeményez hálózati kapcsolatot és fájlhozzáférést. A fájlokat OpenSSL-en és XERXES-en keresztül, hálózati kapcsolatokat pedig a CURL csomagon keresztül éri el.

Az InfoSigno v1.0.0 az IT környezet 1. ábrán látható elemeit az alábbi feladatok elvégzéséhez használja:

- CURL v7.15.1: URL-alapú adathozzáféréseket kiszolgáló modul.
- OpenSSL v 0.9.8.a:nyílt forrású eszközkészlet általános kriptográfiai szolgáltatások megvalósítására.
- XERXES C++ v2.7.0: XML feldolgozó modul.
- ZLIB v1.2.3: gzip formátum-kompatibilis tömörítési eljárásokat tartalmazó könyvtár.

Az OpenSSL és a CURL csomagok közvetlenül támogatják az InfoSigno v1.0.0 biztonsági funkcióit.

5.2 Alrendszerek

Az InfoSigno v1.0-nak az alábbi hat alrendszere van:

- AR0 Inicializálási alrendszer
- AR1 Kulcsadatok és tanúsítványok kezelését végző alrendszer
- AR2 Visszavonási információk kezelését végző alrendszer
- AR3 Időbélyeg kezelést végző alrendszer
- AR4 Aláírás létrehozása és ellenőrzése
- AR5 Felhasználói adatok és XML struktúrák kezelése

5.2.1 Az AR0 (Inicializálási) alrendszer

- Inicializálja az AR1 - AR4 alrendszereket, nem valósít meg biztonsági funkciókat.

5.2.2 Az AR1 (Kulcsadatok és tanúsítványok kezelését végző) alrendszer

- Közreműködik a BF1 Aláírás létrehozása biztonsági funkció megvalósításában, biztosítva az aláírás létrehozásához szükséges megfelelő tanúsítványhoz és magánkulcshoz való hozzáférést.
- Közreműködik a BF2 Digitális aláírás ellenőrzés biztonsági funkció megvalósításában, hozzájárulva a tanúsítványok és kulcsok biztonságos kezelésével a digitális aláírás érték érvényesség ellenőrzéséhez.
- Közreműködik a BF3 Üzenet digitális aláírása biztonsági funkció megvalósításában, aláírva a megadott tanúsítvány felhasználásával a kapott vagy számolt lenyomatot.
- Közreműködik a BF4 Elektronikus aláírás ellenőrzése biztonsági funkció megvalósításában, kikeresve az aláírás ellenőrzéséhez szükséges tanúsítványokat a tanúsítványtárban, valamint felhasználva a kulcsokat az ellenőrzéshez.
- Közreműködik a BF7 Tanúsítvány útvonal felépítése és érvényesség ellenőrzése biztonsági funkció megvalósításában, összegyűjtve, tárolva és kezelve a tanúsítványokat az aláírás ellenőrzéséhez szükséges tanúsítási útvonal felépítéséhez.

5.2.3 Az AR2 (Visszavonási információk kezelését végző) alrendszer

- Közreműködik a BF4 Elektronikus aláírás ellenőrzése biztonsági funkció megvalósításában, begyűjtve és ellenőrizve az aláírás ellenőrzéséhez szükséges tanúsítványok visszavonási információit.
- Közreműködik a BF7 Tanúsítvány útvonal felépítése és érvényesség ellenőrzése biztonsági funkció megvalósításában, bekérve és ellenőrizve az aláírás ellenőrzéséhez szükséges tanúsítási útvonal tanúsítványaira vonatkozó visszavonási információkat.

5.2.4 Az AR3 (Időbélyeg kezelést végző) alrendszer

- Megvalósítja a BF5 Időbélyeg kérés biztonsági funkciót, időbélyeget kérve a felhasználó által megadott lenyomatra.
- Megvalósítja a BF6 Időbélyeg ellenőrzés biztonsági funkciót, ellenőrizve a kapott időbélyeg választ.
- Közreműködik a BF4 Elektronikus aláírás ellenőrzése biztonsági funkció megvalósításában, időbélyeget szolgáltatva az aláírás ellenőrzéséhez.

5.2.5 Az AR4 (Aláírás létrehozása és ellenőrzése) alrendszer

- Megvalósítja a BF1 Aláírás létrehozása biztonsági funkciót, aláírást létrehozva a megfelelő magánkulccsal.
- Megvalósítja a BF2 Digitális aláírás ellenőrzés biztonsági funkciót, végrehajtva az aláírás értékének ellenőrzését az aláíró tanúsítvány felhasználásával.
- Megvalósítja a BF3 Üzenet digitális aláírása biztonsági funkciót, aláírva a megadott tanúsítvány felhasználásával a kapott vagy számolt lenyomatot.
- Megvalósítja a BF4 Elektronikus aláírás ellenőrzése biztonsági funkciót, ellenőrizve az aláírást a rendelkezésre álló vagy ellenőrzés során lekért tanúsítványok, visszavonási információk alapján.
- Megvalósítja a BF7 Tanúsítvány útvonal felépítése és érvényesség ellenőrzése biztonsági funkciót, az aláírás ellenőrzésének szerves részeként felépítve és ellenőrizve a tanúsítási útvonalat az aláírás létrehozására használt aláírói végtanúsítványtól a megbízható pontig, visszavonási információt kérve és ellenőrizve a tanúsítványokra, valamint ellenőrizve a tanúsítási útvonal vég és közbenső tanúsítványainak az aláírását.
- Megvalósítja a BF8 Titkosítás és megoldás biztonsági funkciót.

5.2.6 Az AR5 (Felhasználói adatok és XML struktúrák kezelése) alrendszer

- nem valósít meg biztonsági funkciót.

6 Dokumentáció

Az értékelt termék alkotó elemei (a felhasználókhoz, vagyis a fejlesztő készlet felhasználásával alkalmazást fejlesztőkhöz kiszállított tételek) az alábbiak:

- a **fejlesztésre alkalmas InfoSigno.dll v1.0.0 R119**
- InfoSigno v1.0.0 – **Fejlesztői útmutató**

A fejlesztésre alkalmas InfoSigno v1.0.0 a fejlesztésekhez szükséges dll-t tartalmazza

InfoSigno v1.0.0 – Fejlesztői útmutató bemutatja az InfoSigno v1.0.0 fejlesztő készletet, tartalmazza az adminisztrátori és felhasználói, illetve a fejlesztőknek szóló útmutatást

Az "InfoSigno v1.0.0 – A biztonságos telepítési, generálási és indítási eljárások leírása" című anyag megadja és leírja a biztonságos telepítéséhez, generálásához és indításához szükséges eljárásokat.

7 Tesztelés

A TOE fejlesztése során kialakított és alkalmazott tesztek két csoportba sorolhatóak:

- PKITS (Public Key Interoperability Public Key Interoperability Test Suite) típusú tesztek Automatikusan futtatható tesztrendszer, mely a NIST "Recommendation for X.509 Path Validation" (version 0.5, May 2004) dokumentációban meghatározott 224 teszttel a tanúsítási útvonal felépítését és érvényesítését ellenőrzi, gyakorlatilag teljeskörűen, minden reálisan szóba jöhető (224 darab) eset figyelembe vételével.
- A fejlesztők valamint az értékelő által elvégzett funkcionális tesztek.
    - A belső működési környezet tesztelése
    - Gyűjtő objektumok tesztelése
    - Kulcs és adat objektumok tesztelése
    - Aláírás és ellenőrzés tesztelése
    - Időbélyeg tesztelése

A tesztek a következő szoftver környezetben lettek elvégezve:

- Windows XP SP2
- Windows 2000 SP4
- Windows 2003

A tesztelés során az InfoSigno v1.0.0 fejlesztő készlet kulcs, tanúsítvány és CRL kezeléssel, valamint az aláírással és az aláírás ellenőrzéssel kapcsolatos függvényeit kerültek ellenőrzésre. A tesztekhez egyrészt a Fejlesztő által biztosított teszt program volt használva, másrészt az értékelő készített saját teszt programot.

A fejlesztők által végzett tesztelésről az értékelők megalapították, hogy:

- minden biztonsági funkciót és ezek minden külső interfészét tesztelték,
- minden alrendszert és ezek minden belső interfészét tesztelték,

így megfelel mind a tesztelés lefedettségére, mind pedig a tesztelés mélységére vonatkozó elvárásoknak.

A fejlesztők tesztelésre átadták az értékelőknek az InfoSigno v1.0.0 futtatható változatát és automatizált teszt rendszerét, egyúttal saját környezetükben és harmadik helyen is biztosították a közös tesztelést.

Az értékelők független tesztelést végeztek az értékelés tárgyára (a fejlesztőknél, saját tesztkörnyezetükben, illetve harmadik félnél is). Az alkalmazott tesztkonfigurációk különbözők voltak, annak megfelelően, hogy a biztonsági előirányzat deklarálja az értékelés tárgyának platform függetlenségét.

A független tesztelés eredményei megfeleltek a várakozásoknak (a tapasztalt tényleges eredmények megegyeztek a teszt tervben szereplő elvárt eredményekkel).

8 Az értékelt konfiguráció

8.1 Hardver

Hardver konfiguráció:

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

8.2 Szoftver

Szoftver konfiguráció:

- Operációs rendszer: Windows XP vagy Windows 2003 Server
- PKCS#11 interfész

8.3 BALE

Az InfoSigno v1.0.0 minősített aláírás létrehozása esetén NHH által nyilvántartásba vett biztonságos aláírás létrehozó eszköz használata kötelező. A TOE a BALE eszközt PKCS#11 interfészen keresztül éri el.

9 Az értékelés eredményei

Az InfoSigno v1.0.0 fejlesztő készlet a MIBÉTS (Magyar Informatikai Biztonsági Értékelés és Tanúsítási Séma) módszertana szerint független értékelésre és tanúsításra került, kiemelt garanciaszinten.

Az értékelés megállapította, a tanúsítás pedig megerősítette, hogy **az InfoSigno v1.0.0 megfelel a biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket.**

A fenti megállapítás a kiemelt garanciaszint (EAL4) követelményeinek teljesítésén alapul. Az alábbiak azt mutatja meg, hogy az egyes garanciaösszetevőket hogyan teljesíti az InfoSigno v1.0.0 fejlesztő készlet, illetve mely fejlesztői bizonyítékok támogatták ennek kimutatását.

Garancia-osztály	Garancia-összetevő	A követelmények kielégítésének módja, /s az ezt leíró fejlesztői bizonyíték/
Konfiguráció menedzselés	ACM_CAP.4	Az értékelésre átadott szoftver (fejlesztő készlet) egyedi azonosításra került. A konfiguráció lista leírja az InfoSigno v1.0.0 alkotó konfiguráció elemeket, megfelelve az ACM_SCP-ben megadott minimális körnek(megvalósítási reprezentáció, tervezési dokumentációk, tesztelési dokumentáció, fejlesztői útmutató, a konfiguráció menedzselés dokumentáció, valamint a biztonsági hibák). A konfiguráció lista elemeit a dokumentált rendszer szerint kezelik InfoSigno v1.0.0 – **A konfiguráció menedzselés dokumentációja**
	ACM_SCP.2	A konfiguráció menedzselés dokumentációban megadott konfiguráció lista tartalmazza a konfiguráció menedzselés rendszer által nyomon követendő, a CC és a MIBÉTS által megkövetelt minimális konfiguráció elem készletet. A konfiguráció menedzselés dokumentáció leírja az egyes konfiguráció elem állapotok nyomon követésének módját az InfoSigno teljes életciklusa során. InfoSigno v1.0.0 – **A konfiguráció menedzselés dokumentációja**
	ACM_AUT.1	A konfiguráció menedzselés terv tartalmazza az InfoSigno megvalósítási reprezentációhoz való hozzáférést felügyelő automatizmusok leírását. Az automatizált hozzáférés ellenőrzési intézkedések hatékonyan gátolják az InfoSigno megvalósítási reprezentációjának jogosulatlan módosításait. InfoSigno v1.0.0 – **A konfiguráció menedzselés dokumentációja**
Kiszállítás és működtetés	ADO_DEL.2	A szállítási eljárások alkalmasak a biztonsági cél kielégítésére (vagyis annak garantálása, hogy a szállítási eljárások kielégítően biztosítják, hogy a kifejlesztett értékelés tárgya sértetlenül jut el a felhasználó telephelyére, valamint detektálhatók a szállítás során végrehajtott módosítások és álcázásos próbálkozások). A szállítási dokumentáció leírja, hogy a különböző eljárások és technikai intézkedések milyen módon járulnak hozzá a fejlesztői eredeti példány és a felhasználó telephelyén megkapott verzió közötti módosítások vagy más ellentmondások észleléséhez. A szállítási dokumentáció leírja, hogy a különböző mechanizmusok és eljárások hogyan teszik lehetővé az álcázási kísérletek észlelését, még olyan esetekben is, amikor a fejlesztő nem küldött semmit sem a felhasználónak. A szállítási eljárásokat alkalmazzák. "InfoSigno v1.0.0 – **Fejlesztői útmutató** /Reference Manual/"

	ADO_IGS.1	A dokumentáció megadja és leírja a biztonságos telepítéséhez, generálásához és indításához szükséges eljárásokat illetve azokat a lépéseket, amelyek az InfoSigno v1.0.0 biztonságos telepítéséhez, generáláshoz és indításához szükségesek. "InfoSigno v1.0.0 – **Fejlesztői útmutató** /Reference Manual/"
Fejlesztés	ADV_FSP.2	A funkcionális specifikáció informális módon leírja a megvalósítandó biztonsági funkciókat és azok külső interfészeit. Teljes körűen meghatározza a biztonsági funkciókat. Illetőleg meggyőző indoklást tartalmaz arról, hogy teljes mértékben bemutatta a biztonsági funkciókat. A funkcionális specifikáció lefed minden biztonsági előirányzatban szereplő funkcionális biztonsági követelményt. "InfoSigno - **Funkcionális specifikáció**"
	ADV_HLD.2	A magas szintű terv az összes szükséges informális magyarázatot tartalmazza. Leírja a biztonsági funkciókat az alrendszerek szintjén, azonosítja a biztonsági funkciók által megkövetelt összes hardvert, förmvert és szoftvert. Az alrendszerek interfészeit leírja az egyes alrendszerek interfészeit azok célja és használati módja szerint, valamint megadja a következmények részleteit, a kivételeket és hibaüzeneteket. A biztonsági funkciókat pontosan írja le. A biztonsági funkciók között nincs olyan függőségi kapcsolat, mely nem szerepel a magas szintű tervben A magas szintű terv lefedi a biztonsági előirányzat összes funkcionális biztonsági követelményét. "InfoSigno - **Magas szintű terv**"
	ADV_LLD.1	Az alacsony szintű terv az összes szükséges informális magyarázatot tartalmazza. Leírja a biztonsági funkciókat a modulok szintjén és az összes modul célját valamint a modulok közötti kapcsolatokat. Leírja a modulok interfészeit, azok célja és használatának módja szerint, valamint részletezi a hatásokat, kivételeket, illetve hibaüzeneteket.Az alacsony szintű terv a funkcionális biztonsági követelmények pontos leképezése és lefedi a biztonsági előirányzat összes funkcionális biztonsági követelményét "InfoSigno - **Alacsony szintű terv**"
	ADV_IMP.1	A megvalósítási reprezentáció (pontosabban annak biztonsági szempontból kritikus része) pontosan képezi le az érintett funkcionális biztonsági követelményeket "InfoSigno - **Forráskód**"

	ADV_RCR.1	A biztonsági előirányzat összefoglaló előírása és a funkcionális specifikáció közötti megfeleltetés-elemzés alapján megállapítható, hogy a funkcionális specifikáció az InfoSigno v1.0.0 biztonsági funkcióinak helyes és teljes reprezentációja. A funkcionális specifikáció és a magas szintű terv közötti megfeleltetés-elemzés alapján megállapítható, hogy a magas szintű terv helyes és teljes megvalósulása a funkcionális specifikációnak. A magas szintű terv és az alacsony szintű terv közötti megfeleltetés-elemzés alapján megállapítható, hogy az alacsony szintű terv helyes és teljes megvalósulása a magas szintű tervnek. Az alacsony szintű terv és a megvalósítás reprezentáció részhalmaza közötti megfeleltetés-elemzés alapján megállapítható, hogy a részhalmaz helyes és teljes megvalósulása az alacsony szintű terv azon részének, melyet a megvalósítási reprezentáció finomított. „InfoSigno v1.0.0 – **Megfeleltetés elemzések**”
Útmutató dokumentumok	AGD_ADM.1	Az adminisztrátoroknak (is) szóló útmutatás: • leírja az adminisztrátor rendelkezésére álló adminisztratív biztonsági funkciókat és interfészeket, • leírja az InfoSigno v1.0.0 biztonságos üzemeltetéséhez szükséges adminisztrálás módját, • tartalmazza az azokkal a funkciókkal és jogosultságokkal kapcsolatos figyelmeztetéseket, melyeket egy biztonságos feldolgozási környezetben felügyelni kell. • leír minden olyan feltételezést, mely a biztonságos üzemeltetés szempontjából lényeges felhasználói viselkedéssel kapcsolatos. • leír minden, az adminisztrátor ellenőrzése alá tartozó biztonsági paramétert, szükség esetén jelezve a biztonságos értékeket is. • leírja a végrehajtandó adminisztrátori funkcióhoz kapcsolódó, biztonsági szempontból lényeges események típusát, beleértve a biztonsági tulajdonságok megváltoztatását is. • konzisztens az értékeléshez beadott többi dokumentációval, leír minden, az InfoSigno v1.0.0 informatikai környezetére vonatkozó, az adminisztrátor számára lényeges biztonsági követelményt. "InfoSigno v1.0.0 – **Fejlesztői útmutató** /Reference Manual/"
	AGD_USR.1	A felhasználóknak szóló útmutatás: • leírja a nem adminisztrátor felhasználók rendelkezésére álló valamennyi interfész és funkció leírását, • leírja az InfoSigno v1.0.0 által biztosított, felhasználók által hozzáférhető biztonsági funkciók használatát, • megadja a felhasználó által hozzáférhető azon funkciókkal és jogosultságokkal kapcsolatos figyelmeztetéseket, melyeket egy biztonságos feldolgozási környezetben felügyelni kell, • leír minden olyan felhasználói feladatot, amely az InfoSigno v1.0.0 biztonságos üzemeltetéséhez szükséges, beleértve a biztonsági környezet leírásában szereplő, a felhasználói viselkedésre vonatkozó feltételezéseket is, • konzisztens az értékeléshez beadott többi dokumentációval, leír minden, az InfoSigno v1.0.0 informatikai környezetére vonatkozó, a felhasználó számára lényeges biztonsági követelményt. "InfoSigno v1.0.0 – **Fejlesztői útmutató** /Reference Manual/"

Az életciklus támogatása	ALC_DVS.1	A fejlesztés bizalmasságát és sértetlenségét garantáló szabályok vizsgálata alapján kijelenthető, hogy az alkalmazott biztonsági intézkedések kielégítők. Az értékelő a helyszíni szemlén (megfigyeléssel, mintavételi vizsgálattal és személyes kérdésekkel) megállapította, hogy a leírt biztonsági intézkedéseket be is tartják "InfoSigno v1.0.0 – **A fejlesztési biztonság dokumentációja**"
	ALC_LCD.1	Az alkalmazott életciklus modell (Microsoft Solution Framework) lefedi a fejlesztési és karbantartási folyamatot. Az életciklus modell által leírt eljárások, eszközök és technikák használata pozitív módon hozzájárul az InfoSigno fejlesztéséhez és karbantartásához. "InfoSigno v1.0.0 – **Az életciklust meghatározó dokumentáció** "
	ALC_TAT.1	A fejlesztő eszközök dokumentációja alapján megállapítható, hogy minden fejlesztő eszköz jól meghatározott. Egyértelműen megadja az implementációban használt valamennyi utasítás jelentését, valamint az összes megvalósítás-függő opció jelentését. "InfoSigno v1.0.0 – **A fejlesztő eszközök dokumentációja**"
Tesztelés	ATE_FUN.1	A tesztelési dokumentáció tartalmazza a teszt terveket, a teszt eljárások leírását és a várt eredményeket, valamint a teszt eredményeit. Azonosítja a tesztelendő biztonsági funkciókat és leírja a végrehajtott tesztek célját. A leírt teszt konfiguráció megegyezik a biztonsági előirányzatban megadott értékelendő konfigurációval. A tesztelési tervek és a megfelelő teszt eljárások leírásai összhangban vannak egymással. A teszt eljárások leírása a megismételhetőséghez szükséges kellő részletességgel meghatározza a kezdeti tesztfeltételeket, beleértve a sorrendiséget befolyásoló függőségeket, amennyiben léteznek ilyenek valamint az egyes biztonsági funkciók kiváltását (teszt input) és az ezek eredményeként várható reakciókat. A várható teszteredmények megadása megfelelő (egyértelműek, megfelelnek a tesztmódszerből adódó működésnek). A tesztelési dokumentációban leírt, várt eredmények megfelelnek a teszt tényleges eredményeivel. "InfoSigno v1.0.0 – **Tesztelési dokumentáció**"
	ATE_COV.2	A teszt lefedettség elemzés alapján megállapítható, hogy a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikáció közötti megfeleltetés pontos. Minden biztonsági funkció esetén alkalmas a várt viselkedés bemutatásához és megfelelően ellenőrzik az összes biztonsági funkciót. A teszt lefedettség elemzés alapján megállapítható, hogy a funkcionális specifikációban leírt biztonsági funkciók és a tesztelési dokumentációban szereplő tesztek közötti megfeleltetés teljes /minden biztonsági funkcióhoz és ezek külső interfészeihez tartozik teszt/. "InfoSigno v1.0.0 – **Teszt lefedettség elemzés**"

	ATE_DPT.1	A teszt mélység lefedettség elemzés alapján megállapítható, hogy a tesztelési dokumentációban azonosított tesztek és a magas szintű terv közötti megfeleltetés pontos. A leírt tesztelési módszer minden biztonsági funkció esetén alkalmas a várt viselkedés bemutatásához és megfelelően ellenőrzik az összes biztonsági funkciót. A teszt mélység elemzés alapján megállapítható, hogy a magas szintű tervben leírt biztonsági funkciók és a tesztelési dokumentációban szereplő tesztek közötti megfeleltetés teljes /vagyis a magas szintű tervben leírt minden alrendszerhez és minden belső interfészhez tartozik teszt/. "InfoSigno v1.0.0 – **Teszt mélység elemzés**"
	ATE_IND.2	A tesztelt InfoSigno-t megfelelően telepítették, és ismert állapotban volt. A fejlesztő a független teszteléshez biztosította az értékelő számára azt a környezetet és erőforrás-készletet, amivel a saját tesztelését végezte Az értékelő megismételte a tesztelést a fejlesztő tesztelési dokumentációjában leírt terv tesztek egy mintára valamint megtervezett egy teszt készletet és végrehajtotta valamint dokumentálta azokat. "InfoSigno v1.0.0 – **A tesztelésre alkalmas InfoSigno v1.0.0**"
A sebezhetőség felmérése	AVA_MSU.2	Az útmutató helytelen használhatóságának elemzése alapján megállapítható, hogy az útmutató az InfoSigno v1.0.0 valamennyi működési módjában útmutatást ad a biztonságos működtetésre "InfoSigno v1.0.0 **Az útmutató helytelen használhatóságának elemzése**"
	AVA_SOF.1	Az InfoSigno v1.0.0 nem alkalmaz nem kriptográfiai, valószínűségi vagy permutációs mechanizmusokat. Ezért a biztonsági funkcióerősség elemzésre nincs szükség, az erre vonatkozó követelmény kielégítettnek tekinthető.
	AVA_VLA.2	Az értékelő az áthatolás tesztelések eredményei, valamint a sebezhetőségi elemzések következtetései alapján megállapította, hogy az InfoSigno v1.0.0 a tervezett (cél)környezetében képes ellenállni egy alacsony támadási képességgel rendelkező támadónak. Az értékelő jelentést írt az összes kihasználható sebezhetőségről és maradvány sebezhetőségről „InfoSigno v1.0.0 - **Sebezhetőség elemzés**"

Az értékelés másik következtetése az alábbi:
Az InfoSigno v1.0.0 fejlesztő készlet (A 4.2 fejezetben megfogalmazott feltételek teljesülése esetén) **megfelel a CEN CWA 14170:2004 és CEN CWA 14171:2004 által az elektronikus aláíró alkalmazásokra támasztott valamennyi olyan funkcionális és garanciális biztonsági követelménynek, mely a fejlesztő készletre vonatkozik.**

10 Értékelői megjegyzések és javaslatok

Az értékelő nem adott a tanúsítási jelentésbe megjelentendő megjegyzést illetve javaslatot.

11 Mellékletek

A 9. fejezetben foglaltak szerint az értékelés döntően annak megállapítására irányult, hogy az értékelés tárgya kielégíti-e a biztonsági előirányzatban megfogalmazott funkcionális és garanciális biztonsági követelményeket.

Az InfoSigno v1.0.0 fejlesztő készletre (mint elektronikus aláírás létrehozásának és ellenőrzésének megvalósítására felhasználható elektronikus aláírási termékre) ugyanakkor az alábbi két nemzetközi követelményrendszer is vonatkozik:

- CEN/ISSS/E-Sign 14170:2004 CEN Workshop Agreement: Security requirements for signature creation applications /May 2004/
- CEN/ISSS/E-Sign 14171:2004 CEN Workshop Agreement: General guidelines for electronic signature verification /May 2004/

A fenti dokumentumokban megfogalmazott funkcionális és biztonsági követelményeknek való megfelelőséget külön is vizsgálta az értékelés, melynek módszere a következő volt:
Az értékelés az egyes követelményekre külön-külön határozatot hozott, hogy az alábbiakból melyik vonatkozik az adott követelményre:

- megfelel,
- nem felel meg,
- nem vonatkozik rá a követelmény,
- feltétellel megfelel.

Egyetlen követelményre sem születhet "nem megfelel" határozat, mert ez az egész értékelés tárgyára nézve "nem megfelelt" eredménnyel járna.

A "feltétellel megfelel" határozat olyan feltételt támaszt (nem az értékelés tárgyára, hanem annak működtetési környezetére, vagy egy kiegészítő termékre), melynek kielégítése szükséges az értékelés tárgyának jövőbeli biztonságos használathoz.

Az egyes követelményekre meghozott határozatok az alábbiak alapján születhetnek:

- interjú: a fejlesztőkkel való személyes konzultációk során kapott információk alapján,
- dokumentáció: a fejlesztők által készített írásos dokumentációk alapján,
- tapasztalat: a program felhasználói felületének működtetése, illetve a tesztelés során szerzett „felhasználói” tapasztalatokból leszűrt következtetések alapján,
- teszt: az értékelők által végzett tesztelés eredményei alapján,
- forrás kód: a fejlesztők által átadott forráskód értékelők általi elemzése alapján.

A fent leírt külön vizsgálatnak a következtetése az alábbi:

Az InfoSigno v1.0.0 fejlesztő készlet (A 4.2 fejezetben megfogalmazott feltételek teljesülése esetén) **megfelel a CEN CWA 14170:2004 és CEN CWA 14171:2004 által az elektronikus aláíró alkalmazásokra támasztott valamennyi olyan funkcionális és garanciális biztonsági követelménynek, mely a fejlesztő készletre vonatkozik.**

Mivel az értékelés 9. fejezetben megfogalmazott fő következtetése ettől látszólag független állítást fogalmaz meg, így indoklásra szorul.

A jelen tanúsítási jelentés alapját képező értékelés egy olyan biztonsági előirányzatból indult ki, mely a korábbi hazai (aláíró alkalmazások támogatását megvalósító fejlesztő készletekre vonatkozó) értékelésektől eltérően nem a CWA 14170 és CWA 14171 mértékadó követelményrendszer általános, hanem az InfoSigno v1.0.0-ra vonatkozó konkrét követelményrendszert határozza meg az értékelés viszonyítási alapjaként. Ez teljes mértékben összhangban van a MIBÉTS (és a CC) módszertanával, ugyanakkor nem teszi összehasonlíthatóvá a jelen értékelés eredményét a korábbi értékelési eredményekkel.

A fentiek indokolják, hogy a biztonsági előirányzatnak való megfelelés mellett (ami az értékelés fő következtetése), megfogalmazásra került a CEN követelményeknek való megfelelőség is.

A két következtetés nincs ellentmondásban egymással, kiegészítik egymást.

Az alábbiak (táblázatos formában) a CEN követelményeknek való megfelelésre vonatkozó vizsgálat eredményét foglalja össze.

11.1 Az InfoSigno v1.0.0 megfelelése a funkcionális követelményeknek.

Funkcionális követelmény	Teljesülés
F_SCA_1	**megfelel**
F_SDP_1	**megfelel**
F_SDP_2	**megfelel**
F_SDP_3	**megfelel**
F_SAV_1	**megfelel**
F_SAV_2	**megfelel**
F_SAV_3	**megfelel**
F_SIC_1	**nem vonatkozik rá a követelmény**
F_SIC_2	**nem vonatkozik rá a követelmény**
F_SIC_3	**megfelel**
F_DTBSF_1	**megfelel**
F_DTBSF_2	**megfelel**
F_DHC_1	**megfelel**
F_DHC_2	**megfelel**
F_SSC_1	**nem vonatkozik rá a követelmény**
F_SSC_2	**nem vonatkozik rá a követelmény**
F_SSC_3	**megfelel**
F_SSC_4	**nem vonatkozik rá a követelmény**
F_SSC_5	**megfelel**
F_SSC_6	**megfelel**
F_SSC_7	**megfelel**
F_SSC_8	**megfelel**
F_SSA_1	**nem vonatkozik rá a követelmény**
F_SDC_1	**nem vonatkozik rá a követelmény**
F_SDOC_1	**megfelel**
F_I/O-1	**nem vonatkozik rá a követelmény**
F_I/O-2	**megfelel**
F_I/O-3	**megfelel**
F_ISV-1	**megfelel**
F_ISV-2	**megfelel**
F_ISV-3	**megfelel**
F_USV-1	**megfelel**

F_human_1	**nem vonatkozik rá a követelmény**
F_human_2	**nem vonatkozik rá a követelmény**
F_human_3	**nem vonatkozik rá a követelmény**
F_human_4	**megfelel**
F_human_5	**megfelel**
F_human_6	**nem vonatkozik rá a követelmény**
F_human_7	**megfelel**
F_machine_1	**megfelel**
F_machine_2	**megfelel**
F_general_1	**nem vonatkozik rá a követelmény**
F_protocol	**megfelel**
F_format	**megfelel**
F_principles	**nem vonatkozik rá a követelmény**

11.2 Az InfoSigno v1.0.0 megfelelése a biztonsági követelményeknek.

Biztonsági követelmény	Teljesülés
S_SCA_1	**megfelel**
S_SCA_2	**megfelel**
S_SCA_3	**megfelel**
S_SCA_4	**nem vonatkozik rá a követelmény**
S_SCA_5	**megfelel**
S_SCA_6	**megfelel**
S_SCA_7	**nem vonatkozik rá a követelmény**
S_SCA_8	**nem vonatkozik rá a követelmény**
S_SCA_9	**feltétellel megfelel (1)**
S_SCA_10	**megfelel**
S_SCA_11	**megfelel**
S_SCA_12	**megfelel**
S_SDP_1	**megfelel**
S_SDP_2	**nem vonatkozik rá a követelmény**
S_SDP_3	**nem vonatkozik rá a követelmény**
S_SDP_4	**nem vonatkozik rá a követelmény**
S_SDP_5	**nem vonatkozik rá a követelmény**
S_SDP_6	**nem vonatkozik rá a követelmény**
S_SDP_7	**nem vonatkozik rá a követelmény**
S_SDP_8	**nem vonatkozik rá a követelmény**
S_SDP_9	**nem vonatkozik rá a követelmény**
S_SDP_10	**megfelel**
S_SDP_11	**megfelel**
S_SDP_12	**nem vonatkozik rá a követelmény**
S_SAV_1	**megfelel**
S_SAV_2	**megfelel**
S_SAV_3	**megfelel**
S_SAV_4	**nem vonatkozik rá a követelmény**
S_SAV_5	**nem vonatkozik rá a követelmény**
S_SAV_6	**nem vonatkozik rá a követelmény**
S_SAV_7	**megfelel**

S_SAV_8	**nem vonatkozik rá a követelmény**
S_SIC_1	**nem vonatkozik rá a követelmény**
S_SIC_2	**nem vonatkozik rá a követelmény**
S_SIC_3	**nem vonatkozik rá a követelmény**
S_SIC_4	**nem vonatkozik rá a követelmény**
S_SIC_5	**nem vonatkozik rá a követelmény**
S_SAC_1	**megfelel**
S_SAC_2	**megfelel**
S_SAC_3	**nem vonatkozik rá a követelmény**
S_SAC_4	**feltétellel megfelel (2)**
S_SAC_5	**nem vonatkozik rá a követelmény**
S_SAC_6	**feltétellel megfelel (2)**
S_SAC_7	**nem vonatkozik rá a követelmény**
S_SAC_8	**nem vonatkozik rá a követelmény**
S_SAC_9	**nem vonatkozik rá a követelmény**
S_SAC_10	**nem vonatkozik rá a követelmény**
S_SAC_11	**nem vonatkozik rá a követelmény**
S_SAC_12	**nem vonatkozik rá a követelmény**
S_DTBSF_1	**megfelel**
S_DHC_1	**megfelel**
S_DHC_2	**megfelel**
S_DHC_3	**megfelel**
S_SSC_1	**megfelel**
S_SSC_2	**nem vonatkozik rá a követelmény**
S_SSC_3	**nem vonatkozik rá a követelmény**
S_SSC_4	**nem vonatkozik rá a követelmény**
S_SSA_1	**nem vonatkozik rá a követelmény**
S_SDC_1	**nem vonatkozik rá a követelmény**
S_I/O_1	**feltétellel megfelel (3)**
S_I/O_2	**feltétellel megfelel (4)**
S_I/O_3	**nem vonatkozik rá a követelmény**
S_VER_1	**feltétellel megfelel (5)**

11.3 A tanúsított termékek listájába javasolt szöveg

Jelenleg még nincs tanúsított termékek listája. Amennyiben lenne ilyen lista, abba az alábbi szöveg felvételét javasolnánk:

"Az értékelés tárgya egy olyan fejlesztő készlet, melynek segítségével szabványos (X.509 szabványon alapuló) nyilvános kulcsú szolgáltatásokat biztosító alkalmazások fejleszthetők Az InfoSigno v1.0.0 fejlesztői függvénykönyvtár az alábbi nyilvános kulcs szolgáltatásokat támogatja:

- *Biztonságosan kezel kulcsokat, megbízható pontokat és tanúsítványokat.*
- *Elfogad és feldolgoz X509 v3 nyilvános kulcs tanúsítványokat.*
- *Képes a szükséges tanúsítványok és visszavonási adatok megszerzésére.*
- *Ellenőrzi minden tanúsítvány érvényességét, az RFC 3280-ban leírt eljárások felhasználásával, beleértve a visszavonás ellenőrzést is.*
- *Hozzáfér pontos és megbízható időforráshoz a tanúsítványok, visszavonási adatok és alkalmazási adatok dátumának, idejének ellenőrzése érdekében.*

- *Minősített elektronikus aláírás létrehozása esetén együttműködik a magyar jogszabályok által megkövetelt módon minősített aláírás létrehozásához szükséges tanúsított BALE eszközzel. Fokozott biztonságú elektronikus aláírások esetén képes szabványos szoftveres kulcstároló állományok vagy kriptográfiai hardver eszköz biztonságos kezelésére.*
- *Gyűjti, tárolja és karbantartja a digitális aláírás jövőbeni ellenőrzéséhez szükséges adatokat.*
- *Képes automatikusan választani több magán rejtjelező kulcsból, ha nyilvános kulcs alapú megoldást végez.*

Az InfoSigno v1.0.0 fejlesztő készlet a MIBÉTS (Magyar Informatikai Biztonsági Értékelés és Tanúsítási Séma) módszertana szerint független értékelésre és tanúsításra került, kiemelt garanciaszinten. Az értékelés megállapította, a tanúsítás pedig megerősítette, hogy az InfoSigno v1.0.0 megfelel biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket."

12 Biztonsági előirányzat

A jelen tanúsítási jelentés részét képező végleges biztonsági előirányzatot különálló dokumentumként csatoljuk.

13 Fogalmak és rövidítések

13.1 Fogalmak

Az alábbiakban meghatározzuk a jelen tanúsításban használt (nem nyilvánvaló) fogalmak jelentését.

biztonsági cél
Szándéknyilatkozat azonosított fenyegetések elleni fellépésről és/vagy meghatározott szervezeti biztonsági szabályzatoknak és feltételezésnek való megfelelésről.

biztonsági előirányzat
Biztonsági követelmények és előírások olyan összessége, amelyet valamilyen adott tárgy értékelésének alapjaként használnak.

biztonsági funkció
Az értékelés tárgyának olyan része vagy részei, amelyben meg kell bízni ahhoz, hogy a vonatkozó biztonsági szabályzatból egy szorosan összefüggő szabályhalmaznak érvényt lehessen szerezni.

biztonsági funkció szabályzata
A biztonsági funkció által érvényre juttatott biztonsági szabályzat.

biztonsági jellemző
Szubjektumokkal, használókkal és/vagy objektumokkal társított olyan információ, amelyet az értékelés tárgyára vonatkozó biztonsági szabályzat érvényre juttatására használnak.

biztonsági szabályzat
Szabályok olyan összessége, amely szabályozza a vagyontárgyak kezelését, védelmét, elosztását az értékelés tárgyán belül.

értékelés
A biztonsági előirányzat, illetve az értékelés tárgyának felmérése meghatározott szempontrendszer (pl. a CC vagy a MIBÉTS módszertana) alapján.

értékelés tárgya
Az az informatikai termék vagy rendszer, valamint a hozzá kapcsolódó adminisztrátori és felhasználói útmutatók (jelen esetben fejlesztői útmutató), amelyre az értékelés irányul.

értékelési garanciaszint
A CC. 3 rész olyan garanciaösszetevőiből álló csomag, amelyek egy-egy pontot képviselnek a CC előre meghatározott garanciális skáláján.

értékelési séma
Olyan igazgatási és szabályozási keret, amely szerint az értékelő szervezet egy adott közösségben alkalmazza a CC-t.

értékelő szervezet
Az a testület, amely egy adott közösség keretein belül az úgynevezett értékelési séma révén valósítja meg a CC-t.

felhasználó
Az a személy, aki az InfoSigno v1.0-t alkalmazást használja, azaz az InfoSigno v1.0.0 szolgáltatásait igénybe kívánja venni.

funkcióerősség
Az értékelés tárgya valamelyik biztonsági funkciójának minősítése, amely azt fejezi ki, hogy minimálisan mekkora erőkifejtést tartanak szükségesnek az elvárt biztonsági működés legyőzéséhez a mögöttes biztonsági mechanizmusok közvetlen megtámadása esetén.

hitelesítő adat
Az az információ, amely a felhasználó állítólagos személyazonosságát igazolja.

kulcs, aláíró kulcs
Elektronikus aláírás létrehozásához használt magánkulcs.

kulcs, hitelesítő kulcs
Az azonosításhoz, hitelesítéshez és jogosultság ellenőrzéséhez használt magánkulcs.

kulcs, dekódoló kulcs
Dekódoláshoz használt magánkulcs.

kulcstároló
Kulcsot tároló hardver eszköz (token, PKCS#11, ALE, BALE), vagy titkosítással védett kulcsot tároló fájl (PKCS#12).

összetevő
Valamely csomag, védelmi profil vagy biztonsági előirányzat számára választható elemek legkisebb összessége.

tanúsítási útvonal felépítése
Egy tanúsítványhoz a tanúsítvány lánc kialakítása, úgy, hogy minden tanúsítványt az azt kibocsátó hitelesítés szolgáltató tanúsítványa kövessen. A tanúsítvány lánc a megbízható legfelső szintű tanúsítvánnyal kezdődik, ezt nulla vagy több közbenső tanúsítvány követi, és a végtanúsítvánnyal végződik.

tanúsítási útvonal érvényesítése
A tanúsítási útvonala érvényesíteni kell, mielőtt a végtanúsítvány hitelessége elfogadásra kerülne. A tanúsítási útvonal érvényesítése a tanúsítási útvonalban szereplő minden egyes tanúsítványra a PKIX szabvány szerint előírt ellenőrzések elvégzését jelenti.

tanúsítvány, megbízható legfelső szintű tanúsítvány
Olyan önaláírt tanúsítvány, amely nem igényel tanúsítási útvonal érvényesítést. A tanúsítvány láncban az első helyen szerepel.

tanúsítvány, közbenső tanúsítvány
Olyan, hitelesítés szolgáltató számára kiadott tanúsítvány, amely a tanúsítvány láncban nem az első és nem az utolsó helyen szerepel.

tanúsítvány, lejárt
Olyan tanúsítvány, melynek a notAfter értéke korábbi, mint az aktuális időpont. A lejárt tanúsítvány szerepel vagy nem szerepel a tanúsítvány visszavonási listában (CRL).

tanúsítvány, végtanúsítvány
Olyan, általában személyes tanúsítvány, amely a tanúsítvány láncban az utolsó helyen szerepel.

tanúsítvány, visszavont
Olyan tanúsítvány, amely már nem használható vagy nem megbízható. A hitelesítés-szolgáltató, amely a tanúsítvány kibocsátotta, a tanúsítványt különféle okokból vonhatja vissza. Az okok között szerepel a kulcs feltételezett vagy tényleges kompromittálódása, a tanúsítvány alanynak távozása az adott szervezettől, stb. A tanúsítvány visszavonási lista tartalmazza az összes visszavont és még nem lejárt tanúsítványt. Opcionálisan a tanúsítvány visszavonási lista tartalmazhat visszavont és már lejárt tanúsítványokat is.

tanúsítvány lánc
A tanúsítási útvonal felépítése során keletkező, tanúsítványokból álló sorozat, amelyben az első helyen egy megbízható legfelső szintű tanúsítvány áll, azt opcionális közbenső tanúsítványok követnek, az utolsó helyen egy végtanúsítvány szerepel.

tanúsítvány visszavonási lista (CRL, Certificate Revocation List)
Azoknak a visszavont tanúsítványoknak a felsorolása, amelyeket már nem használhatóak vagy nem megbízhatóak. Általában a hitelesítés szolgáltató, amely a tanúsítványt kibocsátotta, adja ki a CRL-t. A tanúsítvány visszavonási listát a kibocsátó elektronikus aláírással látja el.

termék
Informatikai szoftver, förmver és/vagy hardver által alkotott csomag, amely adott használatra vagy különböző rendszerekbe való beépítésre tervezett funkciókészletet szolgáltat.

védelmi profil
Megvalósítástól független, olyan biztonsági követelményrendszer az értékelés tárgyainak egy kategóriájára, amely adott fogyasztói igényeket elégít ki.

XAdES
Az XMLDSIG szabvány továbbfejlesztése, az EU elektronikus aláírásra vonatkozó (1999/93/EC) direktívája szerint.

XMLDSIG
XML elektronikus aláírás szintaktikáját és feldolgozását leíró szabvány.

13.2 Rövidítések

Az alábbiakban meghatározzuk a jelen értékelési jelentésben használt betűszavak jelentését.

AES **A**dvanced **E**ncryption **S**tandard

ALE **A**láírás-**l**étrehozó **e**szköz

API	**A**pplication **P**rogramming **I**nterface
AR	**Al**rendszer
BALE	**B**iztonságos **a**láírás-**l**étrehozó **e**szköz
BF	**B**iztonsági **f**unkció
CC	**C**ommon **C**riteria (Közös szempontok)
CCRA	**C**ommon **C**riteria **R**ecognition **A**rrangement (a Közös szempontok szerint kibocsátott tanúsítványok kölcsönös elismeréséről szóló nemzetközi megállapodás)
CEM	**C**ommon **E**valuation **M**ethodology (Közös értékelési módszertan)
CEN	**C**omité **E**uropeen de **N**ormalization (Európai Szabványügyi Bizottság)
CRL	**C**ertificate **R**evocation **L**ist (tanúsítvány visszavonási lista)
CWA	**C**EN **W**ork **A**greement (CEN munka megállapodás)
DHC	**D**ata **H**ashing **C**omponent (adatlenyomat-készítő összetevő)
DN	**D**istinguised **N**ame (megkülönböztetett, egyedi név)
DTBS	**D**ata **t**o **b**e **S**igned (aláírandó adat)
DTBSF	**D**ata **t**o **b**e **S**igned **F**ormatter (aláírandó adat formattáló)
EAL	**E**valuation **A**ssurance **L**evel (értékelési garanciaszint)
ETSI	**E**uropean **T**elecommunication **S**tandard **I**nstitute
FIPS	**F**ederal **I**nformation **P**rocessing **S**tandard
IT	**I**nformáció **t**echnológia
KM	**K**onfiguráció **m**enedzsment
MIBÉTS	**M**agyar **I**nformatikai **B**iztonsági és **É**rtékelési **S**éma
PKCS	**P**ublic **K**ey **C**ryptography **S**tandard
PKCS#11	Cryptographic Token Interface Standard
PKCS#12	Personal Information Exchange Information Standard
PKI	**P**ublic **K**ey **I**nfrastructure
RFC	**R**equest **f**or **C**omment
RSA	**R**ivest, **S**hamir, and **A**dleman (az RSA algoritmus)
SAC	**S**igner's **A**uthentication **C**omponent (aláírót hitelesítő összetevő)
SAV	**S**ignature **A**ttribute **V**iewer (aláírási tulajdonság megjelenítő összetevő)
SCA	**S**ecure **C**reation **A**pplication (aláírás-létrehozó alkalmazás)
SDC	**S**igner's **D**ocument **C**omposer (aláírói dokumentum szerkesztő)
SDO	**S**igned **D**ata **O**bject (aláírt adat objektum)
SDOC	**S**igned **D**ata **O**bject **C**omposer (aláírt adat objektum szerkesztő)
SDP	**S**igner's **D**ocument **P**resenter (aláírói dokumentumot megjelenítő összetevő)
SHA-1	**S**ecure **H**ash **A**lgorithm

SIC	**S**igner's **I**nteraction **C**omponent (aláíróval kölcsönható összetevő)
SLC	**S**ignature **L**ogging **C**omponent (aláírás naplózó összetevő)
SSA	**S**CDev - **S**CA **A**uthenticator (az aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás közötti hitelesítés összetevője)
SSC	**S**CDev - **S**CA **C**ommunicator (az aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás közötti kommunikátor összetevő)
SSCD	**S**ecure **S**ignature-**C**reation **D**evice (biztonságos aláírás-létrehozó eszköz)
ST	**S**ecurity **T**arget (biztonsági előirányzat)
SOF	**S**trenght **o**f **F**unction (funkcióerősség)
TOE	**T**arget **o**f **E**valuation (az értékelés tárgya)
XAdES	**XML A**dvanced **E**lectronic **S**ignature (XML formátumú elektronikus aláírás)
XML	E**x**tensible **M**arkup **L**anguage
XMLDSIG	**XML**-**D**igital **Sig**nature Syntax and Processing

14 Felhasznált dokumentumok

14.1 A tanúsításhoz felhasznált kiinduló dokumentumok

- Kérdőív a tanúsítás kérelmezéséhez
- *InfoSigno v1.0.0 Biztonsági előirányzat v1.0*
- *InfoSigno v1.0.0 Értékelési jelentés v1.0*

14.2 Az értékeléshez felhasznált fejlesztői bizonyítékok

Az értékelés, a fejlesztőkkel történt folyamatos konzultáció mellett, az alábbi fejlesztői bizonyítékok végleges verzióit használta fel:

Cím	verzió	fájl név
Biztonsági előirányzat	v1.0.0	InfoSigno_ST_v10_final.pdf
Funkcionális specifikáció	v1.0.0	InfoSigno_FS_v100.doc
Magas szintű terv	v1.0.0	InfoSigno_HLD_v100.doc
Alacsony szintű terv	v1.0.0	man.chm
Megfeleltetés elemzések	v1.0.0	InfoSigno_Repr_Corresp_v100.doc
Tesztelési dokumentáció	v1.0.0	InfoSigno_Test_Documentation.doc
Teszt lefedettség elemzés	v1.0.0	InfoSigno_Test_Cov_v100.doc
Teszt mélység elemzés	v1.0.0	InfoSigno_Test_Depth_v100.doc
Fejlesztői útmutató	v1.0.0	refman.rtf
A konfiguráció menedzselés dokumentációja	v1.0.0	InfoSigno_Conf_Mgmt_v100.doc
A fejlesztési biztonság dokumentációja	v1.0.0	InfoSigno_Development_Security
Az életciklust meghatározó dokumentáció	v1.0.0	InfoSigno_Life_Cycle_Def_v100.doc
A fejlesztő eszközök dokumentációja	v1.0.0	InfoSigno_Tools_v100.doc
Az útmutató helytelen használhatóságának elemzése	v1.0.0	InfoSigno _Misuse_v100.doc
Sebezhetőség elemzés	v1.0.0	InfoSigno_Vulnerability_Analysis.doc

14.3 Az értékeléshez felhasznált módszertani anyagok

Az értékelés az alábbi dokumentumokban leírt módszertant és eljárásrendet követte:

- 1. számú MIBÉTS kiadvány: A MIBÉTS nemzeti séma általános modellezése /0.95 verzió, 2005 február/,
- 2. számú MIBÉTS kiadvány: Az értékelés és a tanúsítás folyamatai /0.95 verzió, 2005 február/,
- 3. számú MIBÉTS kiadvány: Az értékelés módszertana 1 - A biztonsági előirányzat értékelésének módszertana /0.95 verzió, 2005 február/,
- 3. számú MIBÉTS kiadvány: Az értékelés módszertana 4 - A kiemelt garanciaszint értékelésének módszertana /0.95 verzió, 2005 február/

14.4 Az értékeléshez felhasznált egyéb dokumentumok

Az értékelés figyelembe vette az alábbi mértékadó követelményrendszereket is:

Az elektronikus aláírásról szóló 2001. Évi XXXV.törvény

CEN CWA 14170:2004 munkacsoport egyezmény: Security Requirements fro Signature Creation System

CEN CWA 14171:2004 munkacsoport egyezmény: General guidelines for electronic signature verification

CEN CWA 14172-4:2001 munkacsoport egyezmény: Signature-creation application and general gudelines for electronic signature verification

ETSI TS 101 733 v1.6.3 CMS Advanced Electronic Signatures (CAdES)

ETSI TS 101 862 v1.3.3 Qualified Certificate profile

ETSI SR 002 176-1 v1.2.1 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms

ETSI TS 101 903 v1.2.2 XML Advanced Electronic Signatures (XAdES)

RSA Rivest-Shamir-Adleman (public key cryptosystem) /ANSI X9.31/

SHA-1 Secure Hash Algorithm /FIPS PUB 180-1/

RFC3161 Time-Stamp Protocol (TSP)

RFC3275 XML Digital Signatures (XMLDSig)

RFC3280 Certificate and Certificate Revocation List (CRL) Profile

PKCS#1 RSA Cryptographic Standard /RFC2313/

PKCS #11 v2.11: Cryptographic Token Interface Standard

PKCS #12 v1.0 Personal Information Exchange Information Standard