TANÚSÍTÁSI JELENTÉS

InfoSigno
(elektronikus aláírás alkalmazás fejlesztő készlet minősített elektronikus aláíráshoz)
v3.0.1

HUNG-TJ-55-2011

Verzió:	1.0
Fájl:	HUNG_TJ_55_2011_v10.pdf
Minősítés:	Nyilvános
Oldalak:	35

Változáskezelés

Verzió	Dátum	A változás leírása
v0.01	2011.02.11	A szerkezet felállítása
v0.02	2011.02.16	A tanúsítás eredményeit tartalmazó teljes változat
v0.03	2011.02.28	A tanúsítás eredményeit tartalmazó, az értékelővel egyeztetett teljes változat
v1.0	**2011.03.04**	**Végleges verzió**

A tanúsítási jelentést készítette:

Juhász Judit
HunGuard Kft
Tanúsítási divízió

Tartalomjegyzék

1 Összefoglaló

1.1 Az értékelés jellemzői

Az értékelt termék neve:	**InfoSigno (elektronikus aláírás alkalmazás fejlesztő készlet minősített elektronikus aláíráshoz)**
Verzió szám:	**v3.0.1 build 9**
Rövid elnevezés:	**InfoSigno v3.0.1 PKI SDK vagy InfoSigno**
Az értékelt termék típusa:	Fejlesztő készlet (könyvtár)
Értékelő szervezet:	HunGuard Kft.
Értékelés befejezése:	2011. január 14.
Az értékelés módszere:	MIBÉTS
Az értékelés garanciaszintje:	Kiemelt (EAL4)
Az értékelt termék funkcionalitása:	A fejlesztő készlet által támogatott nyilvános kulcsú szolgáltatások az alábbiak: • elektronikus aláírások létrehozása, • elektronikus aláírások ellenőrzése. Támogatja mind a fokozott biztonságú, mind a minősített elektronikus aláírásokat.
Konfigurációs követelmények:	Operációs rendszerek: • Windows XP SP2, • Windows Vista, • Windows 7, • Windows 2003 szerver Fejlesztő környezet: .NET Framework 3.5 Fokozott biztonságú elektronikus aláírás esetén: • Aladdin eToken 32k, Aladdin eToken 64k (CSP: eToken PKI Client v 5.0.0.65) Minősített elektronikus aláírás esetén: • StarCert (CSP: SmartSign CSP for StarCert v1.0.9.15) • Gemp 15-1 Classic v3 (CSP: Gemalto Classic Client v 6.0.0-002)
Megjegyzés:	A termék előző verziója a HUNG-T-031-2006 nyilvántartási számon tanúsított InfoSigno for Developers, mely azonban jelentős változáson ment át mind funkcionalitásban, technológiában, mind elnevezésben.

2 Azonosítás

Az értékelt termék neve:	**InfoSigno (elektronikus aláírás alkalmazás fejlesztő készlet minősített elektronikus aláíráshoz)**
Verzió szám:	**v3.0.1 build 9**
Az értékelt termék alkotó elemei (a felhasználókhoz, vagyis a fejlesztő készlet felhasználásával alkalmazást fejlesztőkhöz kiszállított tételek):	InfoSigno.dll (fejlesztő készlet dll) 3.0.1.9

3 Biztonsági szabályzat

Ez a fejezet azokat a szabályokat írja le, melyek alapján az InfoSigno v3.0.1 irányítja az erőforrásaihoz való hozzáférést, s ezen keresztül minden általa ellenőrzött információt és szolgáltatást.
Először az InfoSigno v3.0.1 üzemmódjait határozzuk meg. Ezt követően a szabályokat érvényre juttató biztonsági funkciókat tekintjük át.

3.1 Üzemmód

Fokozott biztonságú aláírás létrehozás esetén az InfoSigno v3.0.1 képes együttműködni, mint kriptográfiai hardver eszközzel, mint PKCS#12 szoftveres kulcstároló állománnyal.

Minősített elektronikus aláírás esetén az InfoSigno v3.0.1 képes együttműködni biztonságos aláírás létrehozó eszközzel (BALE).

3.2 Biztonsági funkciók

3.2.1 Elektronikus aláírás létrehozása

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

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

Az InfoSigno felhasználója egy program lehet, mely számára API interfészt biztosít. Az InfoSigno függvényei az létrehozó rendszer alábbi funkcionális összetevőit támogatják:

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

Az InfoSigno támogatja az aláírói dokumentumok megjelenítését, miszerint CWA üzemmódban mindig, normál üzemmódban pedig amennyiben a MimeTypeListEnabled konfigurációs paraméter értéke "true", a konfigurációban (a MimeTypeList beállításban) megadott kiterjesztések és programok alapján meghívja a megfelelő külső megjelenítő programot.

Az InfoSigno valósítja meg a dokumentumok szemantikai stabilitás ellenőrzését az alábbi módon:

- Egy konfigurációs paraméter értékétől függően (amennyiben MimeTypeNotTrustedWarning="true") kizárólag az alábbi kiterjesztésű formátumokat tekinti stabilnak: XML, TXT, TIFF, BMP, JPG.

- A kiterjesztése alapján nem stabilnak értékelt aláírandó fájlok esetén az alábbi figyelmeztető információs üzenetet jeleníti meg: „Az aláírandó adat típusa nem megbízható formátum”. Az aláíró ezt követően visszaléphet az aláírástól, de dönthet úgy is, hogy a figyelmeztetés ellenére aláírja a dokumentumot.
- A CWA üzemmód kikényszeríti a fenti stabilitás ellenőrzést (CWA üzemmódban MimeTypeNotTrustedWarning értéke "true").

Az InfoSigno az alábbi aláírási tulajdonságok kezelését (beillesztését, lekérdezését) teszi lehetővé az InfoSigno-t meghívó aláírás létrehozó alkalmazások (köztük az InfoProve) számára:

- az aláírási szabályzatra való hivatkozás,
- az aláírás dátuma és időpontja,
- az aláíró tanúsítványa,
- tartalom-formátum (mime-type),
- kötelezettségvállalás típus (aláírás oka),
- az aláírás helyére vonatkozó állítás (ország, megye, város, irányítószám)

Az InfoSigno az alkalmazandó aláírási szabályzat alábbi részeinek beállítását teszi lehetővé az InfoSigno-t meghívó aláírás létrehozó alkalmazások (köztük az InfoProve) számára:

- a Cégbíróság részére külön séma szerint létrehozott XML-ek támogatása,
- alapértelmezett aláírói tanúsítvány megadása,
- támogatandó ETSI XAdES verzió (v1.2.2 vagy v1.3.2) megadása,
- időbélyeg szolgáltató elérési címe,
- az aláírásnál elvárt formátum (-EPES, -T),
- alkalmazandó lenyomatoló eljárás (hash algoritmus),
- az alkalmazott aláírási szabályzat explicit megadása (pl. MELASZ),
- az alkalmazott aláírási szabályzat elérési címe,
- mime típus alapú ellenőrzés bekapcsolása aláíráskor,
- mime típus alapú megjelenítő program hozzárendelés az aláírandó fájlokhoz.

Az InfoSigno a FIPS PUB 180-3 dokumentumban specifikált lenyomatoló algoritmusokat (SHA1, SHA256, SHA384, SHA512) támogatja.

Az InfoSigno az alábbi aláírás-létrehozó eszközök interfészének meghívását teszi lehetővé az InfoSigno-t meghívó aláírás létrehozó alkalmazások (köztük az InfoProve) számára:

- Windows tanúsítvány táron keresztül elérhető minden eszköz.

3.2.2 Elektronikus aláírás ellenőrzése

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

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

Az InfoSigno függvényei egy aláírás ellenőrző modul alábbi funkcionális összetevőit támogatják:

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

Az **InfoSigno** az alkalmazandó aláírási szabályzat alábbi részeinek beállítását teszi lehetővé az InfoSigno-t meghívó aláírás ellenőrző alkalmazások (köztük az InfoProve) számára:

- OCSP visszavonási információk használatának engedélyezése,
- OCSP visszavonási információk elérési címe,
- kivárási idő OCSP alkalmazása esetén,
- kivárási idő CRL alkalmazása esetén,
- időbélyeg szolgáltató elérési címe,
- az ellenőrzésnél elvárt formátum (-T, -C, -X, -XL, -A),
- az alkalmazott aláírási szabályzat explicit megadása (MELASZ),
- az alkalmazott aláírási szabályzat elérési címe,
- a tanúsítvány láncok felépítéséhez használható tanúsítványok megadása (az önaláírt gyökér tanúsítványok kivételével, melyeket a felhasználónak kell telepítenie),
- mime típus alapú ellenőrzés bekapcsolása ellenőrzéskor,
- mime típus alapú megjelenítő program hozzárendelés az ellenőrizendő fájlokhoz.

Az **InfoSigno** az alábbi támogatást biztosítja az InfoSigno-t meghívó aláírás ellenőrző alkalmazások (köztük az InfoProve) dokumentum megjelenítő alkalmazásokat végrehajtó összetevői számára:

- amennyiben a mime típus alapú ellenőrzés bekapcsolt állapotban van, az ellenőrizendő fájl alapú dokumentum mime típusához rendelt megjelenítő program meghívása.

Az **InfoSigno** az alábbi támogatást biztosítja az InfoSigno-t meghívó aláírás ellenőrző alkalmazások (köztük az InfoProve) érvényesítő adatokat összegyűjtő és feldolgozó összetevői számára:

- CRL letöltése,
- OCSP kérés összeállítása, elküldése,
- OCSP válasz fogadása, feldolgozása.

Az InfoSigno az érvényességi adatok összegyűjtésénél http/https hálózati protokollt használ.

Az InfoSigno az érvényesítő adatok feldolgozása során a következő funkciókat biztosítja:

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

Az **InfoSigno** az alábbi támogatást biztosítja az InfoSigno-t meghívó aláírás ellenőrző alkalmazások (köztük az InfoProve) digitális aláírásokat ellenőrző összetevői számára:

- XML aláírás létrehozása, betöltése, ellenőrzése,
- XML aláírások XMLDSIG, XAdES és MELASZ Ready 1-2 szerinti xml séma alapú szintaktikai és tartalmi ellenőrzése,
- Hiteles időbélyeg kérés küldése és válasz feldolgozása,
- PKI tanúsítvány láncok felépítése és kriptográfiai ellenőrzése (a hitelesség és a sértetlenség szempontjából),
- CRL visszavonási információk beszerzése és feldolgozása PKI tanúsítványhoz,
- OCSP visszavonási információk beszerzése és feldolgozása PKI tanúsítványhoz,
- Windows tanúsítványtárak kezelése és PKI tanúsítványok kezelése.

Az **InfoSigno** az alábbi támogatást biztosítja az InfoSigno-t meghívó aláírás ellenőrző alkalmazások (köztük az InfoProve) aláírási szabályzatokat adminisztráló összetevői számára:

- alkalmazott aláírási szabályzat explicit megadhatósága,
- belső InfoSigno aláírási szabályzat használata (MELASZ Ready 2).

4 Feltételezések és hatókör

Az értékelés következtetései a biztonsági előirányzatban megfogalmazott, az üzemeltetési környezetre vonatkozó feltételezések teljesülésén múlnak.

Ezek a feltételek (melyeket az InfoSigno nem kezel, nem kényszerít ki, hanem elvárja, hogy az informatikai és a nem informatikai környezete teljesítse) az alábbiak:

4.1 Elektronikus aláírás létrehozására és ellenőrzésére vonatkozó közös feltételek

OE.Host_Platform
Az a hoszt platform, melyre a TOE-t telepítették, vagy közvetlenül az aláíró/ellenőrző, vagy egy olyan szervezet felügyelete alatt álljon, amely garantálja az aláíró/ellenőrző számára, hogy az alábbi biztonsági intézkedéseket ténylegesen alkalmazzák.
A hosztgép operációs rendszerének elindításkor azonosítania kell az aláírót/ellenőrző felet.
A hoszt platform operációs rendszere elkülönített futási környezetet biztosítson az általa futtatott alkalmazások számára, továbbá:

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

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

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

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

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

OE.Signature_Policy_Origin
Az aláíró ellenőrizze az aláírási szabályzatok eredet hitelességét, mielőtt a TOE-ba importálná ezeket.

4.2 Kizárólag az elektronikus aláírás létrehozására vonatkozó feltételek

OE.SCDev
Az SCDev-nek képesnek kell lennie a TOE-tól kapott adatokból digitális aláírást létrehozni.
Az SCDev-nek hitelesítenie kell az aláírót, lehetővé téve számára a kiválasztott tanúsítványnak megfelelő magánkulcs aktivizálását.
Az SCDev felelős az aláíró adatainak megvédéséért. Az SCDev-nek az alábbi adatokat biztonságos módon kell tárolnia és használnia:

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

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

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

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

4.3 Kizárólag az elektronikus aláírás ellenőrzésére vonatkozó feltételek

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

4.4 A CWA 14170 és CWA 14171 követelményeknek való megfelelésből adódó feltétel

Az InfoSigno PKI SDK-t csak olyan környezetben szabad alkalmazni, amelyben a CRL-t és a végfelhasználói tanúsítványt ugyanazzal a CA tanúsítvánnyal kell ellenőrizni, illetve csak olyan aláírási szabályzat szerint működhet, amely legfeljebb a következő X509v3 tanúsítvány kiterjesztéseket használja fel:

- ExtendedKeyUsage,
- KeyUsage,
- BasicConstraints,
- CRLDistributionPoints,
- SubjectAlternativeName,
- IssuerAlternativeName,
- OCSP No check - id-pkix-ocsp-nocheck,
- OCSP AuthorityInfoAccess,
- QC statement.

5 A InfoSigno v3.0.1 szerkezeti leírása

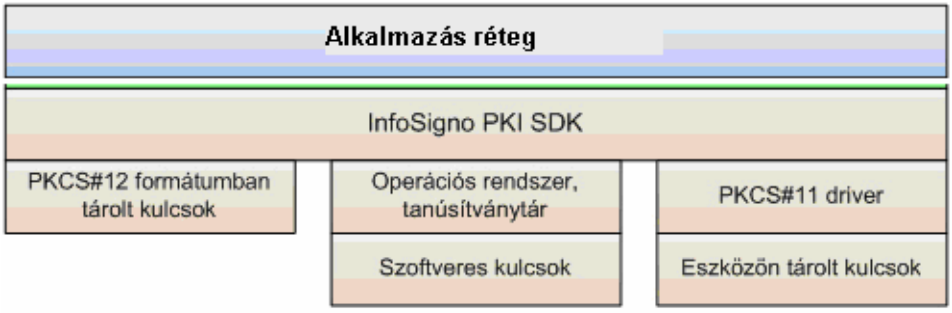
Az InfoProve + InfoSigno egy olyan speciális elektronikus aláírás termék, melynek fő funkciója elektronikus aláírások biztonságos létrehozása és ellenőrzése. A fokozott biztonságú és a minősített elektronikus aláírásokat egyaránt támogatják. Az InfoProve egy Windows alkalmazás, az InfoSigno pedig az ennek alapját képező szoftver fejlesztőkészlet. Az InfoSigno számos más aláíró alkalmazásnak is alapja lehet.

Az InfoProve + InfoSigno az alábbi szabványoknak, illetve ajánlásoknak megfelelő működést biztosít:

- RFC 2560 OCSP kérés előállítás, valamint OCSP és OCSP válasz ellenőrzés
- RFC 3161 Időbélyeg kérés, valamint az időbélyeg és időbélyeg válasz ellenőrzés
- RFC 5280 Tanúsítványok és CRL-ek ellenőrzése, tanúsítási útvonal felépítése és érvényesítése. A tanúsítványlánc felépítésénél az alábbi kiterjesztéseket támogatja:
  - ExtendedKeyUsage,
  - KeyUsage,
  - BasicConstraints,
  - CRLDistributionPoints,
  - SubjectAlternativeName,
  - IssuerAlternativeName,
  - OCSP No check - id-pkix-ocsp-nocheck,
  - OCSP AuthorityInfoAccess,
  - QC statement.
- Egységes MELASZ formátum elektronikus aláírásokra v2.0 (MELASZ Ready, MMM-001: 2008, v2.0)

5.1 Az értékelés tárgya biztonsági környezete és határai

Az (InfoProve + InfoSigno)-t alkotó fizikai összetevőket és környezetét szemlélteti az 1. ábra.



1. ábra Az InfoProve + InfoSigno fizikai elemei

Az értékelés tárgyának összetevői:

- InfoProve aláíró alkalmazás (az 1. ábrán az Alkalmazás réteg),
- InfoSigno PKI SDK (önállóan is meghívható fejlesztő készlet),
- Felhasználói dokumentáció (InfoProve),
- Fejlesztői dokumentáció (InfoSigno).

Az értékelés tárgya az alábbi informatikai elemekből álló környezetben működőképes:

- Windows operációs rendszerek (Windows 32 bites: XP Professional SP2, Windows Vista, Windows 7, Windows 2003 Server),
- Windows API (benne CryptoAPI),
- fejlesztő környezet (.NET Framework 3.5),
- minősített elektronikus aláírás létrehozásához: biztonságos aláírás-létrehozó eszköz a hozzátartozó middleware-rel,
- fokozott biztonságú elektronikus aláírás létrehozásához: aláírás-létrehozó eszköz a hozzátartozó middleware-rel, vagy Microsoft CryptoAPI (külön hardver eszköz nélkül).

6 Dokumentáció

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

Telepítési kézikönyv:	InfoSigno_Telepitesi_kezikonyv_v1.1.doc	1.1
Fejlesztői dokumentáció:	InfoSigno_Fejlesztoi_v1.4.doc	1.4
	InfoSigno.chm	3.0.1
Üzemeltetési kézikönyv:	InfoSigno_PKI_SDK_Uzemeltetesi_kezikonyv_v1.2.doc	1.2

7 Tesztelés

7.1 A fejlesztők tesztelése

Teszt környezet:
A tesztelést a következő környezetekben végezte el a fejlesztő:

- Windows XP SP2,
- Windows Vista,
- Windows 7,
- Windows 2003 szerver

A fejlesztői teszt felépítése:

A fejlesztő az InfoSigno PKI SDK tesztelését 34 darab beépített automata tesztesetek készítésével végezte. A TOE moduljai tartalmaznak egy SelfTest nevű interfészt, ami egy előre meghatározott tesztet futtat az adott modulon, és egy kimeneti fájlba információkat ír a tesztek kimeneteléről. Az InfoSigno SelfTest interfésze a többi modul SelfTest-jét is meghívja így annak meghívása az InfoSigno egy átfogó tesztelését jelenti.

A tesztesetek eredménye minden esetben megfeleltek az elvárt eredményeknek.

7.2 Az értékelők tesztelése

Teszt környezet:
Az értékelés során a következő környezetben került tesztelésre az InfoSigno PKI SDK v3.0.1:

- Windows XP SP3, .Net Framework 3.5

Tesztesetek
A független tesztelés

- a fejlesztői tesztek Windows XP SP3-on történő megismétléséből,
- az InfoSigno v3.0.1 fejlesztő készlet RFC 5280-nak való megfelelésének vizsgálatából (PKITS-tesztkészlet), valamint
- az aláírás formátum kezelést ellenőrző Melasz Ready2 tesztesetek végrehajtásából állt.

A fejlesztői tesztek megismétlése sikeresen, hiba nélkül lefutottak. A tesztesetek eredménye minden esetben megfelelt az elvárt eredménynek.

A PKITS tesztekből az InfoSigno v3.0.1 az alábbi tesztcsoportokat vállalta fel:
PKITS Tesztesetek:

- Alap tesztesetek
- Érvényességi idő tesztesetek
- Név lánc tesztestetek
- Visszavonással kapcsolatos tesztesetek
- Alapvető típusmegkötések tesztesetek
- Kulcshasználat tesztesetek
- Ismeretlen tanúsítvány kiterjesztés tesztestek

A felvállalt tanúsítvány kiterjesztések kezelése megfelelt a PKITS tesztkörnyezet elvárásainak.

Melasz Ready2 tesztesetek:

- EPES aláírások
- EPES aláírás kiterjesztése T-re
- T aláírás kiterjesztése C-re CRL-el
- T aláírás kiterjesztése C-re OCSP-vel
- C aláírás kiterjesztése XL-re RefsOnly Timestamp használatával
- C aláírás kiterjesztése XL-re SignAndRefs Timestamp használatával
- XL aláírás kiterjesztése A-ra (RefsOnly)
- XL aláírás kiterjesztése A-ra (SignAndRefs)
- C aláírás kiterjesztése A-ra (CRL)
- C aláírás kiterjesztése A-ra (OCSP)
- A aláírás ellátása új archív időbélyeggel.
- Negatív tesztesetek

A tesztelés megállapította az InfoSigno 3.0.1 Melasz Ready2 kompatibilitását.

8 Az értékelt konfiguráció

Értékelt InfoProve verzió: 3.0.1.81

Értékelt InfoSigno verzió: 3.0.1 (build 9), mely az alábbi dll:

InfoSigno.dll v3.0.1.9
```
SHA1:   20B8385B3C84B0FE2242724A245B6EAAF805FD1D
SHA256: 1f779e13f57175eeea665ee2f5cb1ea49a1ccc93d126199559c30b1e52d0b70f
```

Az értékelt konfiguráció elemei:

Operációs rendszerek:
- Windows XP SP2,
- Windows Vista,
- Windows 7,
- Windows 2003 szerver

Fejlesztő környezet: .NET Framework 3.5

Fokozott biztonságú elektronikus aláírás esetén:
- Aladdin eToken 32k, Aladdin eToken 64k (CSP: eToken PKI Client v 5.0.0.65)

Minősített elektronikus aláírás esetén:
- StarCert (CSP: SmartSign CSP for StarCert v1.0.9.15)
- Gemp 15-1 Classic v3 (CSP: Gemalto Classic Client v 6.0.0-002)

9 Az értékelés eredményei

Az InfoSigno elektronikus aláírás alkalmazás fejlesztő készlet minősített elektronikus aláíráshoz termék értékelése az InfoPove elektronikus aláírás alkalmazással együtt történt. Az InfoPove alkalmazás az InfoSigno fejlesztői könyvtár szolgáltatásaira épülve végez elektronikus aláírást és ellenőrzést.

Az InfoProve + InfoSigno értékelés az informatikai termékek technológia szempontú biztonsági értékelésére kidolgozott MIBÉTS (Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma) módszertant használta.

A MIBÉTS értékelési módszertana a KIB (Közigazgatási Informatikai Bizottság) 28. számú ajánlásának (Az E-közigazgatási Keretrendszer követelménytár, 2009) részét képezi az alábbi címen: „Termékekre vonatkozó értékelési módszertan”.

Az értékelés garanciaszintje MIBÉTS kiemelt, mely a CC (Common Criteria, MSZ ISO/IEC 15408) szerinti EAL4-es szintnek felel meg.

Az értékelés fő következtetése az alábbi:

Az InfoProve (elektronikus aláírás alkalmazás) v3.0.1 + InfoSigno (elektronikus aláírás alkalmazás fejlesztő készlet minősített elektronikus aláíráshoz) v3.0.1 megfelel biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket.

9.1 A biztonsági előirányzat értékelése

Ez az alfejezet az InfoProve + InfoSigno biztonsági előirányzata értékelési eredményeit foglalja össze.

Az értékelés alapja az alábbi dokumentum:

Biztonsági előirányzat	InfoSigno_biztonsagi_eloiranyzat_v1.00.doc	1.00

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Biztonsági előirányzat	ASE_INT.1 Bevezetés	A követelményeknek **megfelelt**.
	ASE_CCL.1 Megfelelőségi nyilatkozatok	A követelményeknek **megfelelt**.
	ASE_SPD.1 Biztonsági probléma meghatározás	A követelményeknek **megfelelt**.
	ASE_OBJ.2 Biztonsági célok	A követelményeknek **megfelelt**.
	ASE_ECD.1 Kiterjesztett biztonsági követelmények	A követelményeknek **megfelelt**.
	ASE_REQ.2 Biztonsági követelmények	A követelményeknek **megfelelt**.
	ASE_TSS.1 Az értékelés tárgya összefoglaló előírása	A követelményeknek **megfelelt**.

9.2 A fejlesztés értékelése

Ez az alfejezet az InfoProve + InfoSigno tervezési dokumentációit értékeli a biztonsági funkcióik megfelelő leírása és magyarázata szempontjából.

Az értékelés alapját az alábbi fejlesztői bizonyítékok képezték:

Biztonsági előirányzat	InfoSigno_biztonsagi_eloiranyzat_v1.00.doc	1.00
Biztonsági szerkezet leírás	InfoSigno_biztonsagi_szerkezet_v1.00.doc	1.00
Funkcionális specifikáció	InfoSigno_funkcionalis_specifikacio_v1.00	1.00
TOE terv	InfoSigno_TOE_terv_v1.00.doc	1.00
Megvalósítási reprezentáció	InfoSigno_megvalositas_reprezentacio_v1.00.doc	1.00
Saját fejlesztésű forráskódok	--- (argeon\InfoSigno\2010\ Deliverables\TOE\TOE_Final\InfoSigno alkönyvtár)	3.0.1
Fejlesztői dokumentáció	InfoSigno_Fejlesztoi_v1.4.doc InfoSigno.chm	1.4 3.0.1
Üzemeltetési kézikönyv	InfoSigno_PKI_SDK_Uzemeltetesi_kezikonyv_v1.2.doc	1.2

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Fejlesztés	ADV_ARC.1 A biztonsági szerkezet leírás	A követelményeknek **megfelelt**.
	ADV_FSP.4 Teljes funkcionális specifikáció	A követelményeknek **megfelelt**.
	ADV_TDS.3 Alap moduláris terv	A követelményeknek **megfelelt**.
	ADV_IMP.1 A TSP megvalósítási reprezentációja	A követelményeknek **megfelelt**.

9.3 Az útmutatók értékelése

Ez az alfejezet az InfoProve + InfoSigno útmutató dokumentációját értékeli.

Az értékelés alapját az alábbi fejlesztői bizonyítékok képezték:

Biztonsági előirányzat	InfoSigno_biztonsagi_eloiranyzat_v1.00.doc	1.00
Funkcionális specifikáció	InfoSigno_funkcionalis_specifikacio_v1.00	1.00
TOE terv	InfoSigno_TOE_terv_v1.00.doc	1.00
A szállítási eljárások leírása	Lásd: „Telepítési kézikönyv” 1 fejezete	1.1
Telepítési kézikönyv	InfoSigno_Telepitesi_kezikonyv_v1.1.doc	1.1
Fejlesztői dokumentáció	InfoSigno_Fejlesztoi_v1.4.doc InfoSigno.chm	1.4 3.0.1
Üzemeltetési kézikönyv	InfoSigno_PKI_SDK_Uzemeltetesi_kezikonyv_v1.2.doc	1.2

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Útmutató dokumentumok	AGD_PRE.1 Az előkészítő eljárások	A követelményeknek **megfelelt**.
	AGD_USR.1 Az üzemeltetési felhasználói útmutató	A követelményeknek **megfelelt**.

9.4 Az életciklus támogatás értékelése

Ez az alfejezet az InfoProve + InfoSigno fejlesztése során a fejlesztői környezetben betartott biztonsági intézkedéseket értékeli.

Az értékelés alapját az alábbi fejlesztői bizonyítékok képezték:

Biztonsági előirányzat	InfoSigno_biztonsagi_eloiranyzat_v1.00.doc	1.00
A tesztelésre alkalmas TOE	InfoSigno.dll SimpleTester.exe MMMEAA_ARG.exe InfoProveProfessional.exe	3.0.1.9 1.0.0 1.0.0 3.0.1
Konfiguráció lista	InfoSigno_konfiguracio_lista_v1.00.doc	1.00
A konfiguráció kezelés dokumentációja	InfoSigno_konfiguracio_kezeles_v1.00	1.00
A fejlesztés biztonság dokumentációja	InfoSigno_fejlesztes_biztonsag_v1.00.doc	1.00
Az életciklus meghatározás dokumentációja	InfoSigno_eletciklus_meghatarozas_v1.00	1.00
A fejlesztő eszközök dokumentációja	InfoSigno_fejlesztesi_eszkozok_v1.00	1.00
A szállítási eljárások leírása	A „Telepítési kézikönyv” 1 fejezetében	1.1

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Életciklus támogatás	ALC_CMC.4 A TOE előállítás támogatása, átvételi eljárások és automatizálás	A követelményeknek **megfelelt**.
	ALC_CMS.4 A probléma követés CM lefedettsége	A követelményeknek **megfelelt**.
	ALC_DEL.1 A szállítási eljárások	A követelményeknek **megfelelt**.
	ALC_DVS.1 A biztonsági intézkedések azonosítása	A követelményeknek **megfelelt**.
	ALC_LCD.1 A fejlesztő által meghatározott életciklus modell	A követelményeknek **megfelelt**.
	ALC_TAT.1 Jól meghatározott fejlesztő eszközök	A követelményeknek **megfelelt**.

9.5 A tesztelés értékelése

Ez az alfejezet azt vizsgálja és értékeli, hogy az InfoProve + InfoSigno a tervdokumentációkban megadottaknak megfelelően működik-e, valamint összhangban van-e a biztonsági előirányzatában megfogalmazott funkcionális biztonsági követelményeivel.

Az értékelés alapját az alábbi fejlesztői és értékelői bizonyítékok képezték:

Biztonsági előirányzat	InfoSigno_biztonsagi_eloiranyzat_v1.00.doc	1.00
Biztonsági szerkezet leírás	InfoSigno_biztonsagi_szerkezet_v1.00.doc	1.00
Funkcionális specifikáció	InfoSigno_funkcionalis_specifikacio_v1.00	1.00
TOE terv	InfoSigno_TOE_terv_v1.00.doc	1.00
Telepítési kézikönyv	InfoSigno_Telepitesi_kezikonyv_v1.1.doc	1.1
Fejlesztői dokumentáció	InfoSigno_Fejlesztoi_v1.4.doc InfoSigno.chm	1.4 3.0.1
Üzemeltetési kézikönyv	InfoSigno_PKI_SDK_Uzemeltetesi_kezikonyv_v1.2.doc	1.2
A konfiguráció kezelés dokumentációja	InfoSigno_konfiguracio_kezeles_v1.00	1.00
A tesztelésre alkalmas TOE	InfoSigno.dll SimpleTester.exe MMMEAA_ARG.exe InfoProveProfessional.exe	3.0.1.9 1.0.0 1.0.0 3.0.1
Tesztelési dokumentáció	Lásd a teszt lefedettség elemzés 3. fejezete	1.00
Teszt lefedettség elemzés	InfoSigno_teszt_lefedettseg_v1.00.doc	1.00
Teszt mélység elemzés	InfoSigno_teszt_melyseg_v1.00.doc	1.00

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Tesztelés	ATE_FUN.1 A funkcionális tesztelés	A követelményeknek **megfelelt**.
	ATE_COV.2 A teszt lefedettség elemzés	A követelményeknek **megfelelt**.
	ATE_DPT.2 A biztonságot érvényre juttató modulok tesztelése	A követelményeknek **megfelelt**.
	ATE_IND.2 A független tesztelés	A követelményeknek **megfelelt**.

9.6 A sebezhetőség értékelése

Ez az alfejezet az InfoProve + InfoSigno -ban lévő hibák, gyengeségek meglétét és a velük való visszaélések lehetőségét kívánja meghatározni vagy kizárni. Mindez a fejlesztő és az értékelő elemzésén alapul, valamint értékelői tesztelés egészíti ki.

Az értékelés alapját az összes fejlesztői bizonyíték képeztek (lásd 14.2)

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
A sebezhetőség felmérése	AVA_VAN.3 Célirányos sebezhetőség vizsgálat	A követelményeknek **megfelelt**.

10 Értékelői megjegyzések és javaslatok

Az értékelő nem adott a tanúsítási jelentésbe megjelenítendő 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.

A InfoSigno v3.0.1 fejlesztő készletre (mint elektronikus aláírás létrehozásának és ellenőrzésének megvalósítására felhasználható elektronikus aláírási termékre) ugyanakkor az alábbi két nemzetközi követelményrendszer is vonatkozik:

- CEN CWA 14170:2004 munkacsoport egyezmény: Security requirements for signature creation applications /May 2004/
- CEN CWA 14171:2004 munkacsoport egyezmény: 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 felel meg" 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.

A fent leírt külön vizsgálatnak a következtetése az alábbi:

Az InfoSigno v3.0.1 fejlesztő készlet (A 4. 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.**

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

11.1 Az InfoSigno v3.0.1 megfelelése a funkcionális követelményeknek

Funkcionális követelmény	Teljesülés	Teljesülés módja
F_SCA_1	Megfelel	megvalósít
F_SDP_1	Megfelel	kezel, tárol
F_SDP_2	Megfelel	kezel, tárol
F_SDP_3	Megfelel	kezel, tárol
F_SAV_1	Megfelel	kezel, tárol
F_SAV_2	Megfelel	kezel, tárol
F_SAV_3	Megfelel	megvalósít
F_SIC_1	Nem vonatkozik rá a követelmény	-
F_SIC_2	Nem vonatkozik rá a követelmény	-

Funkcionális követelmény	Teljesülés	Teljesülés módja
F_SIC_3	Nem vonatkozik rá a követelmény	-
F_DTBSF_1	Megfelel	megvalósít
F_DTBSF_2	Megfelel	megvalósít
F_DHC_1	Megfelel	megvalósít
F_DHC_2	Nem vonatkozik rá a követelmény	-
F_SSC_1	Nem vonatkozik rá a követelmény	-
F_SSC_2	Nem vonatkozik rá a követelmény	-
F_SSC_3	Nem vonatkozik rá a követelmény	-
F_SSC_4	Nem vonatkozik rá a követelmény	-
F_SSC_5	Nem vonatkozik rá a követelmény	-
F_SSC_6	Nem vonatkozik rá a követelmény	-
F_SSC_7	Nem vonatkozik rá a követelmény	-
F_SSC_8	Nem vonatkozik rá a követelmény	-
F_SSA_1	Nem vonatkozik rá a követelmény	-
F_SDC_1	Nem vonatkozik rá a követelmény	-
F_SDOC_1	Megfelel	megvalósít
F_I/O-1	Nem vonatkozik rá a követelmény	
F_I/O-2	Megfelel	megvalósít
F_I/O-3	Megfelel	megvalósít
F_ISV-1	Megfelel	megvalósít
F_ISV-2	Megfelel	megvalósít
F_ISV-3	Feltétellel megfelel (1. számú CWA feltétel)	megvalósít
F_USV-1	Megfelel	megvalósít
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	Nem vonatkozik rá a követelmény	-
F_human_5	Nem vonatkozik rá a követelmény	-

Funkcionális követelmény	Teljesülés	Teljesülés módja
F_human_6	Nem vonatkozik rá a követelmény	-
F_human_7	Megfelel	megvalósít, támogat
F_machine_1	Megfelel	megvalósít, támogat
F_machine_2	Megfelel	megvalósít, támogat
F_general_1	Nem vonatkozik rá a követelmény	-
F_protocol	Megfelel	megvalósít
F_format	Megfelel	megvalósít
F_principles	Nem vonatkozik rá a követelmény	-

11.2 A InfoSigno v3.0.1 megfelelése a biztonsági követelményeknek

Biztonsági követelmény	Teljesülés	Teljesülés módja
S_SCA_1	Feltétellel megfelel (OE.TOE/SCDev_ Communications)	részben megvalósít
S_SCA_2	Feltétellel megfelel (OE.Signatory_Authentication_ Data_Protection)	részben megvalósít + külső környezeti elvárás
S_SCA_3	Nem vonatkozik rá a követelmény	-
S_SCA_4	Nem vonatkozik rá a követelmény	-
S_SCA_5	Megfelel	támogat
S_SCA_6	Megfelel	támogat
S_SCA_7	Nem vonatkozik rá a követelmény	-
S_SCA_8	Nem vonatkozik rá a követelmény	-
S_SCA_9	Feltétellel megfelel (OE.Host_Platform)	részben megvalósít + külső környezeti elvárás
S_SCA_10	Megfelel	megvalósít
S_SCA_11	Megfelel	megvalósít
S_SCA_12	Megfelel	megvalósít
S_SDP_1	Megfelel	támogat
S_SDP_2	Megfelel	megvalósít -
S_SDP_3	Nem vonatkozik rá a követelmény	-
S_SDP_4	Nem vonatkozik rá a követelmény	-
S_SDP_5	Megfelel	megvalósít
S_SDP_6	Megfelel	támogat
S_SDP_7	Nem vonatkozik rá a követelmény	-

Biztonsági követelmény	Teljesülés	Teljesülés módja
S_SDP_8	Nem vonatkozik rá a követelmény	-
S_SDP_9	Nem vonatkozik rá a követelmény	-
S_SDP_10	Megfelel	megvalósít
S_SDP_11	Megfelel	megvalósít
S_SDP_12	Nem vonatkozik rá a követelmény	-
S_SAV_1	Megfelel	megvalósít
S_SAV_2	Megfelel	megvalósít
S_SAV_3	Megfelel	megvalósít
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	megvalósít
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	Nem vonatkozik rá a követelmény	-
S_SAC_2	Nem vonatkozik rá a követelmény	-
S_SAC_3	Nem vonatkozik rá a követelmény	-
S_SAC_4	Nem vonatkozik rá a követelmény	-
S_SAC_5	Nem vonatkozik rá a követelmény	-
S_SAC_6	Nem vonatkozik rá a követelmény	-
S_SAC_7	Nem vonatkozik rá a követelmény	-
S_SAC_8	Nem vonatkozik rá a követelmény	-
S_SAC_9	Nem vonatkozik rá a	-

Biztonsági követelmény	Teljesülés	Teljesülés módja
	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	megvalósít
S_DHC_1	Megfelel	megvalósít
S_DHC_2	Nem vonatkozik rá a követelmény	-
S_DHC_3	Megfelel	megvalósít
S_SSC_1	Nem vonatkozik rá a követelmény	-
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 (OE.Host_Platform)	részben megvalósít + külső környezeti elvárás
S_I/O_2	Feltétellel megfelel (OE.Host_Platform)	részben megvalósít + külső környezeti elvárás
S_I/O_3	Nem vonatkozik rá a követelmény	-
S_VER_1	Feltétellel megfelel (OE.Host_Platform)	részben megvalósít + külső környezeti elvárás

11.3 A tanúsított termékek listájába javasolt szöveg

Jelenleg Magyarországon 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. A fejlesztő készlet által támogatott nyilvános kulcsú szolgáltatások az alábbiak:

- *Fokozott biztonságú és minősített elektronikus aláírás létrehozása a Crypto API által támogatott algoritmus paraméterekkel, Windows tanúsítványtárban, szoftver tokenben vagy kriptográfiai hardver eszközben tárolt magánkulcs használatával.*
- *Elektronikus aláírás ellenőrzése a kapcsolódó tanúsítvány útvonal felépítési és érvényesítési szolgáltatásokkal, RSA algoritmus támogatással.*
- *Aláírás létrehozáshoz lenyomat készítése SHA-1, SHA-256, SHA-384, SHA-512, algoritmusokkal.*
- *Időbélyeg kérése és ellenőrzése.*
- *Visszavonási információ kérése és ellenőrzése (CRL, OCSP).*

Ennek alapján az InfoSigno v3.0.1 fejlesztői készlet segítségével olyan alkalmazások fejleszthetők, melyek a nyilvános kulcsú technológia alapján bizalmasságot, sértetlenséget, hitelesítést és letagadhatatlanságot biztosító szolgáltatásokat képesek nyújtani."

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

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

értékelés tárgya
Az az informatikai termék vagy rendszer, valamint a hozzá kapcsolódó adminisztrátori és használati útmutatók, amelyre az értékelés irányul.

értékelési garanciaszint
A CC. 3 rész olyan garancia összetevőiből 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 a TOE fejlesztőkészletet, vagy az erre épülő aláíró alkalmazásokat használja, azaz a TOE szolgáltatásait igénybe veszi.

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

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

tanúsítási útvonal érvényesítése
A tanúsítási útvonalat 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 tanúsítványláncban az első helyen szerepel.

tanúsítvány, közbenső tanúsítvány
Olyan, hitelesítés szolgáltató számára kiadott tanúsítvány, amely a tanúsítványláncban 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 tanúsítványláncban 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.

tanúsítványlánc
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.

13.2 Rövidítések

Az alábbiakban meghatározzuk a jelen értékelési jelentésben használt betűszavak jelentését.

API	**A**pplication **P**rogramming **I**nterface
BALE	**B**iztonságos **a**láírás **l**étrehozó **e**szköz
CC	**C**ommon **C**riteria (Közös szempontok)
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)
DTBS	**D**ata **t**o **b**e **S**igned (aláírandó adat)
DTBSR	**D**ata **t**o **b**e **S**igned Representation (aláírandó adat reprezentáció)
EAL	**E**valuation **A**ssurance **L**evel (értékelési garanciaszint)
ETSI	**E**uropean **T**elecommunication **S**tandard **I**nstitute
ETSI TS	**ETSI T**echnical **S**pecification
MIBÉTS	**M**agyar **I**nformatikai **B**iztonsági **É**rtékelési és **T**anúsítási **S**éma
OCSP	**O**nline **C**ertificate **S**tatus **P**rotocol (valósidejű tanúsítvány állapot protokoll)
PKI	**P**ublic **K**ey **I**nfrastructure
PKITS	**P**ublic **K**ey **I**nteroperability **T**est **S**uite
PKIX	Internet **X**509 **PKI**
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)
SCDev	**S**ignature-**C**reation **Dev**ice (aláírás-létrehozó eszköz)
SDC	**S**igner's **D**ocument **C**omposer (aláírói dokumentum szerkesztő)
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	**S**ecure **H**ash **A**lgorithm
SIC	**S**igner's **I**nteraction **C**omponent (aláíróval kölcsönható összetevő)
SSA	**S**CDev - **S**CA **A**uthenticator (az aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás közötti hitelesítés összetevője)
SSCD	**S**ecure **S**ignature-**C**reation **Dev**ice (biztonságos aláírás-létrehozó eszköz)
TOE	**T**arget **o**f **E**valuation (az értékelés tárgya)

XML E**x**tensible **M**arkup **L**anguage

XAdES **X**ML **Ad**vanced **E**lectronic **S**ignature (XML formátumú elektronikus aláírás)

14 Felhasznált dokumentumok

14.1 A tanúsításhoz felhasznált kiinduló dokumentumok

- Kérdőív a tanúsítás kérelmezéséhez
- InfoSigno v3.0.1 Biztonsági előirányzat v1.00
- InfoSigno v3.0.1 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:

fejlesztői bizonyíték	Cím	verzió
Megvalósítás		
futtatható saját szoftver elemek	InfoSigno.dll (fejlesztő készlet dll) SimpleTester.exe (az InfoSigno.dll egy tesztprogramja) MMMEAA_ARG.exe (az InfoSigno.dll egy másik tesztprogramja) InfoProveProfessional.exe (InfoSigno.dll-re épülő minta alkalmazás)	3.0.1.9 1.0.0 1.0.0 3.0.1
forráskódok	Áttekintő leírás: Lásd „Megvalósítási reprezentáció” Forráskódok: Lásd az alábbi alkönvtár: Hungserver\argeon\ InfoSigno\2010\Deliverables\TOE\TOE_Final\InfoSigno\InfoSigno. NET_20110123	1.00
harmadik fél által fejlesztett szoftver komponensek	pkcs12_crypto.dll ICSharpCode.SharpZipLib.dll nunit.core.dll, nunit.core.interfaces.dll, nunit.framework.dll	1.5.0 0.844.0 2.4.8
Fejlesztői dokumentációk		
Biztonsági előirányzat	InfoSigno_biztonsagi_eloiranyzat_v1.00.doc	1.00
Telepítési kézikönyv	InfoSigno_Telepitesi_kezikonyv_v1.1.doc	1.1
Fejlesztői dokumentáció	InfoSigno_Fejlesztoi_v1.4.doc InfoSigno.chm	1.4 3.0.1
Üzemeltetési kézikönyv	InfoSigno_PKI_SDK_Uzemeltetesi_kezikonyv_v1.2.doc	1.2
Biztonsági szerkezet leírás	InfoSigno_biztonsagi_szerkezet_v1.00.doc	1.00
Funkcionális specifikáció	InfoSigno_funkcionalis_specifikacio_v1.00	1.00
TOE terv	InfoSigno_TOE_terv_v1.00.doc	1.00
Megvalósítási reprezentáció	InfoSigno_megvalositas_reprezentacio_v1.00.doc	1.00
Saját fejlesztésű forráskódok	--- (\argeon\InfoSigno\2010\Deliverables \TOE\TOE_Final\InfoSigno alkönyvtár)	3.0.1
Konfiguráció lista	InfoSigno_konfiguracio_lista_v1.00.doc	1.00
A konfiguráció kezelés dokumentációja	InfoSigno_konfiguracio_kezeles_v1.00	1.00
A fejlesztés biztonság dokumentációja	InfoSigno_fejlesztes_biztonsag_v1.00.doc	1.00
Az életciklus meghatározás dokumentációja	InfoSigno_eletciklus_meghatarozas_v1.00	1.00
A fejlesztő eszközök dokumentációja	InfoSigno_fejlesztesi_eszkozok_v1.00	1.00
A szállítási eljárások leírása	Lásd: „Telepítési kézikönyv” 1 fejezete	1.1
A tesztelésre alkalmas TOE	InfoSigno.dll SimpleTester.exe MMMEAA_ARG.exe InfoProveProfessional.exe	3.0.1.9 1.0.0 1.0.0 3.0.1
Tesztelési dokumentáció	Lásd a teszt lefedettség elemzés 3. fejezete	1.00
Teszt lefedettség elemzés	InfoSigno_teszt_lefedettseg_v1.00.doc	1.00
Teszt mélység elemzés	InfoSigno_teszt_melyseg_v1.00.doc	1.00

14.3 Az értékeléshez felhasznált módszertani anyagok

Az értékelés az alábbi dokumentumokban leírt módszertant és eljárásrendet követte:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Revision 1, September 2006.
- [Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Revision 2, September 2007.
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, Revision 2, September 2007.
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, Revision 2, September 2007.
- KIB (Közigazgatási Informatikai Bizottság) 28. számú ajánlás „Termékekre vonatkozó értékelési módszertan”

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 - Security requirements for signature creation applications
- CEN CWA 14171:2004 - General guidelines for electronic signature verification
- Protection Profile - Electronic Signature Creation Application (DCSSI-PP-2008/05)
- Protection Profile - Electronic Signature Verification Module (DCSSI-PP-2008/06)
- ETSI TS 102 176-1 v2.0.0 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms
- Egységes MELASZ formátum elektronikus aláírásokra v2.0 (MELASZ Ready2, MMM-001: 2008, v2.0)
- RFC 2560: PKIX - Online Certificate Status Protocol – OCSP
- RFC 3161 PKIX - Time-Stamp Protocol
- RFC 5280 PKIX - Certificate and Certificate Revocation List (CRL) Profile
- SHS Secure Hash Standard /FIPS PUB 180-3/
- PKCS#1 RSA Cryptography Standard v2.1, June 2002