TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005. (VII.21.) IHM rendelet alapján, mint a Magyar Köztársaság Miniszterelnöki Hivatalt Vezető Miniszterének 001/2010 számú Kijelölési okiratával kijelölt tanúsító szervezet

tanúsítja,
hogy az

ARGEON Informatikai Szolgáltató Kft.
által kifejlesztett

InfoSigno PKI SDK
elektronikus aláírás alkalmazás fejlesztő készlet minősített elektronikus aláíráshoz
v3.0.1 (build 9)

az 1.számú mellékletben áttekintett funkcionalitással, valamint

a 2. számú melléklet biztonságos felhasználásra vonatkozó feltételek figyelembe vételével

megfelel

a 2001. évi XXXV törvényben szereplő
fokozott biztonságú és minősített elektronikus aláírás
létrehozására és ellenőrzésére alkalmazható
szabványos és biztonságos alkalmazások fejlesztéséhez.

Jelen tanúsítvány a HUNG-TJ-055-2011. számú tanúsítási jelentés alapján került kiadásra.
Készült az ARGEON Informatikai Szolgáltató Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-055-2011**
A tanúsítás kelte: 2011. március 04.
A tanúsítvány érvényességi ideje: 2014. március 04.
Melléklet: tulajdonságok, feltételek, követelmények, egyéb jellemzők összesen 6 oldalon.

PH.

Endrődi Zsolt	dr. Szabó István
Tanúsítási igazgató	Ügyvezető igazgató

1. számú melléklet

Az InfoSigno v3.0.1 legfontosabb tulajdonságainak összefoglalása

Az InfoSigno v3.0.1 egy olyan fejlesztő készlet, melynek segítségével szabványos (X.509 szabványon alapuló) nyilvános kulcsú szolgáltatásokat biztosító alkalmazások fejleszthetők. 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. 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-224, SHA-256, SHA-384, SHA-512 algoritmusokkal.
- Időbélyeg kérése és ellenőrzése.
- Visszavonási információ kérése és ellenőrzése (CRL, OCSP).

Ennek alapján a 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.

A InfoSigno v3.0.1 fejlesztői függvénykönyvtár az alábbi nyilvános kulcs szolgáltatásokkal rendelkezik:

- biztonságosan kezel kulcsokat, megbízható pontokat és tanúsítványokat;
- elfogad és feldolgoz X.509 v3 nyilvános kulcs tanúsítványokat;
- képes a szükséges tanúsítványok és visszavonási adatok megszerzésére;
- ellenőrzi minden tanúsítvány érvényességét, az RFC 5280 dokumentumban leírt eljárások felhasználásával, beleértve a visszavonás ellenőrzését is;
- hozzáfér pontos és megbízható időforráshoz a tanúsítványok, visszavonási adatok és alkalmazási adatok dátumának, idejének ellenőrzése érdekében;
- beszerzi, tárolja (beágyazza az aláírás struktúrába) a digitális aláírás jövőbeni ellenőrzéséhez szükséges adatokat;
- támogatja a XAdES-EPES, -T, -C, -X, -X-L és -A elektronikus aláírás formátumokat.

2. számú melléklet

A biztonságos felhasználás feltételei

A tanúsítvány érvényessége a biztonsági előirányzatban megfogalmazott, az üzemeltetési környezetre vonatkozó feltételezések teljesülésén múlik.
Az alábbi (a biztonsági előirányzatban is szereplő) feltételezések az informatikai környezetre vonatkoznak:

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 aláíró/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.

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.

Kizárólag az elektronikus aláírás ellenőrzésére vonatkozó feltételek

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

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 X.509 v3 tanúsítvány kiterjesztéseket használja fel:

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

3. számú melléklet

Termékmegfelelőségi követelmények

Követelményeket és szabványokat tartalmazó dokumentumok

Követelmények

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

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

CEN CWA 14171:2004 munkacsoport egyezmény: 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)

Szabványok

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

4. számú melléklet

A tanúsítási eljárás egyéb jellemzői

A tanúsításhoz figyelembe vett, fejlesztői dokumentumok

- Biztonsági előirányzat InfoSigno_biztonsagi_eloiranyzat_v1.00.doc v1.00
- Telepítési kézikönyv InfoSigno_Telepitesi_kezikonyv_v1.1.doc v1.1
- Fejlesztői dokumentáció InfoSigno_Fejlesztoi_v1.4.doc v1.4, InfoSigno.chm v3.0.1
- Üzemeltetési kézikönyv InfoSigno_PKI_SDK_Uzemeltetesi_kezikonyv_v1.2.doc v1.2
- Biztonsági szerkezet leírás InfoSigno_biztonsagi_szerkezet_v1.00.doc v1.00
- Funkcionális specifikáció InfoSigno_funkcionalis_specifikacio_v1.00 v1.00
- TOE terv InfoSigno_TOE_terv_v1.00.doc v1.00
- Megvalósítási reprezentáció InfoSigno_megvalositas_reprezentacio_v1.00.doc v1.00
- Saját fejlesztésű forráskódok
- Konfiguráció lista InfoSigno_konfiguracio_lista_v1.00.doc v1.00
- A konfiguráció kezelés dokumentációja InfoSigno_konfiguracio_kezeles_v1.00 v1.00
- A fejlesztés biztonság dokumentációja InfoSigno_fejlesztes_biztonsag_v1.00.doc v1.00
- Az életciklus meghatározás dokumentációja InfoSigno_eletciklus_meghatarozas_v1.00 v1.00
- A fejlesztő eszközök dokumentációja InfoSigno_fejlesztesi_eszkozok_v1.00 v1.00
- A szállítási eljárások leírása Lásd: „Telepítési kézikönyv” 1 fejezete 1.1
- A tesztelésre alkalmas TOE InfoSigno.dll v3.0.1.9
- Tesztelési dokumentáció Lásd a teszt lefedettség elemzés 3. fejezete
- Teszt lefedettség elemzés InfoSigno_teszt_lefedettseg_v1.00.doc v1.00
- Teszt mélység elemzés InfoSigno_teszt_melyseg_v1.00.doc v1.00

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

Értékelési jelentés az Infoprove v3.0.1 elektronikus aláíró alkalmazás + InfoSigno v3.0.1 elektronikus aláírás alkalmazás fejlesztő készlet minősített elektronikus aláíráshoz v1.0 (Készítette HunGuard Kft.)

A követelményeknek való megfelelést ellenőrző független vizsgálat módszere

Az InfoSigno v3.0.1 fejlesztő készlet a MIBÉTS módszertana szerint került független értékelésre és tanúsításra.

Az értékelés garanciaszintje

MIBÉTS kiemelt (mely megfelel a CC EAL4 garanciaszintjének)

Az értékeléshez felhasznált módszertani anyagok

- 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”