TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005. (VII. 21.) IHM rendelet alapján, mint a Magyar Köztársaság Informatikai és Hírközlési Miniszter 002/2006 számú kijelölési okiratával kijelölt tanúsító szervezet

tanúsítja,

hogy az

Argeon Üzleti Szolgáltató Kft.
által kifejlesztett

InfoSigno for Developers v1.0.0 r119

fejlesztő készlet minősített elektronikus aláíráshoz

az 1.számú mellékletben áttekintett funkcionalitással, valamint

a 2. számú melléklet biztonságos felhasználásra vonatkozó feltételek figyelembe vételével

megfelel

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

Jelen tanúsítvány a HUNG-TJ-031-2006. számú tanúsítási jelentés alapján került kiadásra.
Készült az Argeon Üzleti Szolgáltató Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-031-2006.**
A tanúsítás kelte: 2006. május 29.
A tanúsítvány érvényességi ideje: 2009. május 29.
Melléklet: tulajdonságok, feltételek, követelmények, egyéb jellemzők összesen 6 oldalon.

PH.

Endrődi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető igazgató

1. számú melléklet

Az InfoSigno v1.0.0 legfontosabb tulajdonságainak összefoglalása

Az InfoSigno v1.0.0 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 X.509 v3 nyilvános kulcs tanúsítványokat.
- Képes a szükséges tanúsítványok és visszavonási adatok megszerzésére.
- Ellenőrzi minden tanúsítvány érvényességét, az RFC 3280-ban leírt eljárások felhasználásával a 2-es számú mellékletben leírt megkötések mellett, beleértve a visszavonás ellenőrzést is.
- RFC 3161 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.

2. számú melléklet

A biztonságos felhasználás feltételei

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).

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 tanúsítványláncban nem fordul elő, a CRL-t és a végfelhasználói tanúsítványt ugyanazzal a CA tanúsítvánnyal ellenőrizik, valamint a tanúsítványláncban a kibocsájtó-tulajdonos név egyezőség bináris.
2. Az InfoSigno v1.0.0 fejlesztő készletet 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 azt.
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.

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 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)

Szabványok

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

4. számú melléklet

A tanúsítási eljárás egyéb jellemzői

A tanúsításhoz figyelembe vett, fejlesztői dokumentumok

- Kérelem a tanúsítás elvégzéséhez
- Biztonsági előirányzat v1.0
- Funkcionális specifikáció v1.0
- Magas szintű terv v1.0
- Alacsony szintű terv v1.0
- Megfeleltetés elemzések v1.0
- Tesztelési dokumentáció v1.0
- Teszt lefedettség elemzés v1.0
- Teszt mélység elemzés v1.0
- Fejlesztői útmutató v1.0
- A konfiguráció menedzselés dokumentációja v1.0
- A fejlesztési biztonság dokumentációja v1.0
- Az életciklust meghatározó dokumentáció v1.0
- A fejlesztő eszközök dokumentációja v1.0
- Az útmutató helytelen használhatóságának elemzése v1.0
- Biztonsági funkcióerősség elemzés v1.0
- Sebezhetőség elemzés v1.0

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

Értékelési jelentés az InfoSigno for Developers fejlesztő készlet minősített elektronikus aláíráshoz v1.0 (Készítette HunGuard Kft.)

A követelményeknek való megfelelést ellenőrző független vizsgálat módszere

Az InfoSigno V1.0.0 értékelése az informatikai termékek technológia szempontú értékelésére szolgáló Magyar Informatikai Biztonsági és Értékelési Séma /MIBÉTS/ módszertanát követte. A MIBÉTS séma az informatikai termékek és rendszerek biztonsági értékelésére a Közös szempontrendszer (MSZ ISO/IEC 15408:2002) elveit, fogalmait és követelményrendszerét tekinti meghatározónak.

Az értékelés garanciaszintje

Kiemelt (EAL4)

Az értékeléshez felhasznált módszertani anyagok

- 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/.