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

Grepton Informatikai Részvénytársaság
által kifejlesztett

MultiSigno V3 SDK /3.0.1 r249/

aláíró alkalmazás fejlesztő készlet

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-033-2006. számú tanúsítási jelentés alapján került kiadásra.
Készült a Grepton Informatikai Részvénytársaság. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-033-2006.**
A tanúsítás kelte: 2006. június 09.
A tanúsítvány érvényességi ideje: 2009. június 09.
Melléklet: tulajdonságok, feltételek, követelmények, egyéb jellemzők összesen 6 oldalon.

PH.

Endrődi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető igazgató

1. számú melléklet

A MultiSigno v3.0.1 legfontosabb tulajdonságainak összefoglalása

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 elektronikus aláírás létrehozása RSA/1024 algoritmus paraméterekkel, PKCS#12 formátumú fájlban, saját tanúsítványtárban vagy kriptográfiai hardver eszközben tárolt magánkulcs használatával;
- minősített elektronikus aláírás létrehozása RSA/1024 algoritmus paraméterekkel BALE használatával;
- elektronikus aláírás ellenőrzése, a kapcsolódó tanúsítvány útvonal felépítési és érvényesítési szolgáltatásokkal;
- aláírás létrehozáshoz lenyomat készítése SHA-1, SHA-256, SHA-384, SHA-512 algoritmusokkal;
- szimmetrikus AES ECB és CBC, 3DES-CBC, RC2 -CBC és aszimmetrikus (RSA, PKCS#1 v1.5) titkosítás és megoldás;
- időbélyegzés (kérése és ellenőrzése).

Ennek alapján a MultiSigno 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 MultiSigno v3.0.1 fejlesztői függvénykönyvtár az alábbi nyilvános kulcs szolgáltatásokkal rendelkezik:

- 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 X.509 szabványban [ISO 9594-8] 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 aláírás létrehozása esetén együttműködik a magyar jogszabályok által megkövetelt módon minősített aláírás létrehozásához szükséges tanúsított BALE eszközzel, vagy fokozott biztonságú aláírások esetén képes szabványos szoftveres kulcstároló állományok vagy Kriptográfiai hardver eszköz (KHE) 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.
- Elektronikus aláírás formátum: Melasz-Ready XAdES.

2. számú melléklet

A biztonságos felhasználás feltételei

Feltételezések a MultiSigno v3.0.1 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. A MultiSigno v3.0.1-t megfelelően telepítik és konfigurálják (AE.Configuration).
3. Fokozott biztonságú elektronikus aláírás létrehozása esetén a MultiSigno v3.0.1 által meghívott kriptográfiai funkciók (OpenSSL v0.9.8) megbízhatónak tekinthetők az elvárt kriptográfiai funkciók megvalósítása terén. Minősített elektronikus aláírás létrehozása esetén a MultiSigno v3.0.1 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).
4. A MultiSigno v3.0.1-mal szembeni támadási potenciált alacsonynak tételezzük fel. (AE.Low).
5. A MultiSigno v3.0.1 környezete fizikailag biztonságos (AE.Physical_Protection).
6. A tanúsítvány és tanúsítvány visszavonási információk a MultiSigno v3.0.1 rendelkezésére állnak (AE.PKI_Info)
7. A MultiSigno v3.0.1 környezete GMT formában és a megkívánt pontossággal gondoskodik a pontos rendszeridőről (AE.Time).
8. A MultiSigno v3.0.1 környezete biztosítja az időbélyegzés szolgáltatóhoz való hozzáférést (AE.TimeStamp).

A biztonságos felhasználás egyéb feltételei

1. A MultiSigno v3.0.1 programozói könyvtár az önkibocsátott (self issued) tanúsítványokat nem támogatja. Nem támogatja az automatikus Policy kezelést és az LDAP alapú CRL kibocsátást, valamint a delta CRL-t. Ezért csak olyan környezetben szabad alkalmazni, ahol önkibocsátott (self issued) tanúsítvány a tanúsítványláncban nem fordul elő. Nem használható olyan rendszerben, ahol a Policy-t automatikusan kell kezelni, LDAP alapú a CRL kibocsátás, vagy delta CRL-t használnak.
2. A MultiSigno v3.0.1 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. A MultiSigno v3.0.1 programozói könyvtár működtetési környezetében biztosítani kell a használt PKCS#12 fájl és token eszköz jelszavának lecserélhetőségét.

4. A MultiSigno v3.0.1 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. A MultiSigno v3.0.1 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék a MultiSigno v3.0.1 programozói könyvtár funkcionális összetevőinek sértetlenségét, megakadályozva, hogy behatolók elrontsák azt.
6. A MultiSigno v3.0.1 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy a MultiSigno v3.0.1 programozói könyvtárat, valamint az aláírás-létrehozás és aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő valamennyi 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 for 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

- Biztonsági előirányzat v1.0
- Funkcionális specifikáció v1.0
- Magas szintű terv v1.0
- Alacsony szintű terv (MultiSigno SDK Dokumentáció) v3.0.1
- megvalósítás v3.0.1
- Megfeleltetés elemzések v1.0
- Tesztelési dokumentáció v1.0
- Teszt lefedettség elemzés v1.0
- Teszt mélység elemzés v1.0
- Útmutatók (MultiSigno 3.0 Manual) 2006.04.28
- 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
- Sebezhetőség elemzés v1.0
- Folyamatábrák v.1.0.0
- MultiSigno 3 - Rendszerterv - Implementációs modell 2006.01.06
- MultiSigno 3 - Rendszerterv - Felhasználási esetek megvalósításai 2006.01.06
- Logikai architektúra a MultiSigno 3 rendszertervhez 2006.01.06
- MultiSigno 3.0 Specifikáció v2.0
- MultiSigno 3.0 Manual 2006.04.28

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

Értékelési jelentés a MultiSigno V3 SDK aláíró alkalmazás fejlesztő készlet v3.0.1 /r249/ v1.0 (Készítette HunGuard Kft.)

A követelményeknek való megfelelést ellenőrző független vizsgálat módszere

A MultiSigno v3.0.1 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/.