TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005. (VII. 21.) IHM rendelet alapján, mint a Magyar Köztársaság Gazdasági és Közlekedési Miniszterének 113/2007 számú kijelölési okiratával kijelölt tanúsító szervezet

tanúsítja,

hogy a

Noreg Információvédelmi Kft.
által kifejlesztett

eSign Toolkit v2.1.0.2

fejlesztőkészlet 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
fokozott biztonságú és minősített elektronikus aláírás
létrehozására és ellenőrzésére alkalmazható
szabványos és biztonságos alkalmazások fejlesztéséhez.

Jelen tanúsítvány a HUNG-TJ-043-2008. számú tanúsítási jelentés alapján került kiadásra.
Készült a Noreg Információvédelmi Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-043-2008.**
A tanúsítás kelte: 2008. december 01.
A tanúsítvány érvényességi ideje: 2011. december 01.
Melléklet: tulajdonságok, feltételek, követelmények, egyéb jellemzők összesen 6 oldalon.

PH.

Endrődi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető igazgató

1. számú melléklet

Az eSign Toolkit v2.1.0 legfontosabb tulajdonságainak összefoglalása

Az eSign Toolkit v2.1.0 függvénygyűjtemény az alábbi tulajdonságokkal rendelkezik:

- képes szabványos formátumú (XAdES v1.2.2 és MELASZ-ready v1.0 szerinti XAdES-EPES, XAdES-T, XAdES-C és XAdES-XL, valamint RFC 3852 szerinti CMS) elektronikus aláírás létrehozására,
- képes szabványos formátumú (XAdES v1.2.2 és MELASZ-ready v1.0 szerinti XAdES-EPES, XAdES-T, XAdES-C, XAdES-XL és XAdES-A, valamint RFC 3852 szerinti CMS) elektronikus aláírás ellenőrzésére,
- képes X.509 v3 tanúsítványok és tanúsítványláncok kezelése (az RFC 5280 alapján),
- alkalmas időbélyegzés kérés készítésére és az időbélyeg válasz ellenőrzésére (az RFC 3161 szabványt követő időbélyegző-szolgáltatókkal együttműködve),
- képes visszavonási információk (CRL és OCSP) lekérdezésére a hitelesítés-szolgáltatóktól (a tanúsítványból kiolvasott elérési helyről),
- képes együttműködni különböző aláírás-létrehozó eszközökkel (ALE) és biztonságos aláírás-létrehozó eszközökkel (BALE).

Az eSign Toolkit v2.1.0 szoftverfejlesztők számára készült, zárt rendszerben felhasználásra kerülő, nyilvános kulcs szolgáltatásokat biztosító C nyelven írt függvénygyűjtemény, olyan funkcionalitással, mellyel elektronikus aláírások létrehozása, ellenőrzése, az ellenőrzéshez érvényesítő információk feldolgozása, tanúsítási útvonal felépítése, tanúsítványok érvényességének ellenőrzése, visszavonási információk érvényesség ellenőrzése, időbélyeg kérése és ellenőrzése, OCSP kérése és ellenőrzése valósítható meg.

Az eSign Toolkit v2.1.0 az OpenSSL funkcióira épít, azokat felhasználja működése során, ezen keresztül valósítja meg a legtöbb kriptográfiai funkcionalitást. A kriptográfiai token eszközök kezelése PKCS#11 felületen keresztül történik.

A DLL különféle programozási nyelvi környezetből hívható felülettel rendelkezik, szoftver fejlesztői csomagban kerül forgalomba.

2. számú melléklet

A biztonságos felhasználás feltételei

Az értékelés pozitív következtetése az alábbi feltétel csoportok teljesülésén múlik:

- a biztonsági előirányzatból adódó feltételek (az értékelés tárgyának biztonságához szükséges, az informatikai környezetre vonatkozó feltételezések),
- a CWA 14170 és a CWA 14171 követelményeinek való megfelelés érdekében teljesítendő feltételek
- a biztonságos felhasználás egyéb feltételei.

Feltételezések az eSign Toolkit v2.1.0 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 eSign Toolkit v2.1.0 fejlesztőkészletet megfelelően telepítik és konfigurálják (AE.Configuration).
3. Az eSign Toolkit v2.1.0 által meghívott kriptográfiai funkciók (például OpenSSL) megbízhatóan valósítják meg az eSign Toolkit v2.1.0 által hívott kriptográfiai funkciókat. Minősített elektronikus aláírás létrehozása esetén az eSign Toolkit v2.1.0 környezete tartalmaz egy (vagy több) NHH által nyilvántartott, tanúsított BALE-t, mely tárolja és védi az aláíró magánkulcsát, illetve végrehajtja a digitális aláírást. (AE.Crypto_Module)
4. A fejlesztői környezetben az eSign Toolkit v2.1.0 függvény-gyűjtemény védett a jogosulatlan fizikai hozzáféréssel szemben. (AE.Physical_Protection).
5. A tanúsítvány és tanúsítvány visszavonási információk az eSign Toolkit v2.1.0 rendelkezésére állnak (AE.PKI_Info).
6. A környezet GMT formában és a megkívánt pontossággal gondoskodik a pontos rendszeridőről (AE.Time).
7. Az eSign Toolkit v2.1.0 környezete biztosítja az időbélyegzés szolgáltatóhoz való hozzáférést (AE.TimeStamp).

A CWA 14170 és 14171 követelményeknek való megfelelés feltételei

1. számú CWA feltétel (az F_ISV_3 funkcionális követelmény teljesítéséhez)
Az eSign Toolkit v2.1.0 függvény-gyűjtemény a tanúsítványlánc ellenőrzésekor a kagylóhéj modellt követi, azaz minden tanúsítvány érvényességi időintervallumának benne kell lennie az őt kibocsátó tanúsítvány érvényességi időintervallumában. Nem támogatja azon tanúsítványláncok ellenőrzését sem, ahol a kibocsátott CRL nem teljes. Ezért csak olyan környezetben szabad alkalmazni, ahol egy kibocsátott tanúsítvány nem érvényes tovább, mint az őt kibocsátó tanúsítvány, valamint a tanúsítványokhoz kiadott CRL teljes.

2. számú CWA feltétel (az S_SCA_9 biztonsági követelmény teljesítéséhez)
Az eSign Toolkit v2.1.0 függvény-gyűjteménnyel fejlesztett 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. számú CWA feltétel (az S_SCA_12 biztonsági követelmény teljesítéséhez)
Az eSign Toolkit v2.1.0 függvény-gyűjtemény tartalom típusként a text/xml típust tárolja el. Ezért kizárólag e típusnak megfelelő adatok aláírására használható.

4. számú CWA feltétel (az S_I/O_1 biztonsági követelmény teljesítéséhez)

Az eSign Toolkit v2.1.0 függvény-gyűjtemény nem rendelkezik önvédelmi funkcióval, ezért működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:

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

5. számú CWA feltétel (az S_I/O_2 biztonsági követelmény teljesítéséhez)
Az eSign Toolkit v2.1.0 működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék az eSign Toolkit v2.1.0 függvény-gyűjtemény funkcionális összetevőinek sértetlenségét, megakadályozva, hogy behatolók elrontsák ezt.

6. számú CWA feltétel (az S_VER_1 biztonsági követelmény teljesítéséhez)
Az eSign Toolkit v2.1.0 működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az eSign Toolkit v2.1.0 függvény-gyűjtemény valamennyi aláírás-létrehozás vagy aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.

A biztonságos felhasználás egyéb feltételei

Az eSign Toolkit v2.1.0 az alábbi üzemmódokat különbözteti meg:

- minősített elektronikus aláírást létrehozó üzemmód (a „QualifiedSignature” környezeti változó értéke nem 0)
- fokozott biztonságú elektronikus aláírást létrehozó üzemmód (a „QualifiedSignature” környezeti változó értéke 0)

1. számú egyéb feltétel
Minősített elektronikus aláírás létrehozása esetén a „minősített elektronikus aláírást létrehozó üzemmód”-ot kell beállítani a „QualifiedSignature” környezeti változó értékének helyes beállításával.

3. számú melléklet

Termék-megfelelőségi 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

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 2.0.0 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/
RFC 2560	X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 1999
RFC3161	Time-Stamp Protocol (TSP)
RFC3275	XML Digital Signatures (XMLDSig)
RFC3852	Cryptographic Message Syntax (CMS)
RFC5280	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
MELASZ-ready v1.0	Egységes MELASZ formátum elektronikus aláírásokra v1.0, 2006 február

4. számú melléklet

A tanúsítási eljárás egyéb jellemzői

A tanúsításhoz figyelembe vett fejlesztői dokumentumok

- Kérelem a tanúsítás elvégzéséhez
- Biztonsági Előirányzat 1.0
- A Konfiguráció Kezelés Dokumentációja 1.0
- A Fejlesztés Biztonság Dokumentációja 1.0
- Noregpki2.Dll - Fejlesztői Dokumentáció 2.1.0.2
- Tesztelési Dokumentáció 1.0
- Teszt Lefedettség Elemzés 1.0
- Teszt Mélység Elemzés 1.0
- Magas Szintű Terv 1.0
- Megfelelés Elemzés 1.0
- Sebezhetőség Elemzés 1.0
- NoregPKI2.dll, NoregPKI2.h 2.1.0.2

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

Értékelési jelentés az „eSign Toolkit minősített elektronikus aláíráshoz v2.1.0” v1.0 (Készítette HunGuard Kft.)

A követelményeknek való megfelelést ellenőrző független vizsgálat módszere

Az eSign Toolkit v2.1.0 fejlesztőkészlet 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 15408:2005) elveit, fogalmait és követelményrendszerét tekinti meghatározónak.

Az értékelés garanciaszintje

Fokozott (EAL3)

Az értékeléshez felhasznált módszertani anyagok

- ISO/IEC 15408:2005 Information technology — Security techniques — Evaluation criteria for IT security (Part 1,2,3)
- ISO/IEC 18045:2005 Information technology — Security techniques — Methodology for IT security evaluation
- KIB 25. ajánlás A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (v1.0, 2008 június) - 5. számú segédlet: ÉRTÉKELÉSI MÓDSZERTAN