TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 15/2001. (VIII. 27.) MeHVM rendelet alapján, mint a Magyar Köztársaság Informatikai és Hírközlési Miniszter 002/2004 számú kijelölési okiratával kijelölt tanúsító szervezet

tanúsítja,

hogy a

NetLock Hálózatbiztonsági és Informatikai Szolgáltató Kft.
által kifejlesztetett

NLCAPI3 v3.2.0 kriptográfiai modul

elektronikus aláíró alkalmazás fejlesztésére alkalmas
programozói függvény könyvtár

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, valamint időbélyeg
kérelmezésére és ellenőrzésre alkalmazható
szabványos és biztonságos alkalmazások fejlesztéséhez**

Jelen tanúsítvány a HUNG-TJ-027-2005. számú tanúsítási jelentés alapján került kiadásra.
Készült a NetLock Hálózatbiztonsági és Informatikai Szolgáltató Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-027-2005.**
A tanúsítás kelte: 2005. június 20.
A tanúsítvány érvényességi ideje: 2008. június 20.
Melléklet: tulajdonságok, feltételek, követelmények, egyéb jellemzők összesen 5 oldalon.

PH.

Endrődi Zsolt

Tanúsítási igazgató
dr. Szabó István
Ügyvezető igazgató

1. számú melléklet

Az NLCAPI3 v3.2.0 legfontosabb tulajdonságainak összefoglalása

Az NLCAPI3 v3.2.0 egy programozói könyvtár, amely a rá épülő alkalmazás fejlesztői számára elektronikus aláírással kapcsolatos funkcionalitást nyújt.
Az NLCAPI3 v3.2.0 teljes mértékben a Windows operációs rendszer Crypto API-jára támaszkodik, használatát lényegesen leegyszerűsíti. A Crypto API-n keresztül a Microsoft vagy más gyártók CSP-jét használja az aláírás-létrehozó eszköz funkcionalitásának elérésére. A lenyomatoló eljárások szintén a Crypto API függvényei. A tanúsítványlánc ellenőrzésére az OpenSSL 0.9.7d verziójának függvényeit használja.
Az NLCAPI3 v3.2.0 kriptográfiai modul fejlesztők részére elektronikus aláírások készítésére azok ellenőrzésére, tanúsítványok, és időbélyegek kezelésére nyújt programozási felületet. Jellemző tulajdonságok:

- Használt aláírás formátumok:
  - PKCS7 (RFC2315);
  - XMLDSIG (RFC3275);
  - XADES-BES, XADES-T, XADES-C, XADES-XL, XAdES-A, többszörös XAdES-A (ETSI 101903)
  - Saját NetLock formátum (nem dokumentált)
- RFC3161 szerinti időbélyeg kezelés.
- MD5 és SHA1- lenyomatoló eljárások.
- X509 tanúsítványok és CRL-ek kezelése, Windows tanúsítványtárban vagy BASE64 kódolt PEM és DER formátumban.
- Tanúsítvány érvényesítés RFC3280 alapján.
- Támogatott tanúsítvány kiterjesztések:
  - Key Usage
  - Basic Constraints
  - CRL Distribution Points
  - Qualified Certificate Statement (ETSI TS 101 862)

2. számú melléklet

A biztonságos felhasználás feltételei

Az alábbiakban összefoglaljuk azokat a kötelezően betartandó, a jelen tanúsítvány érvényességére kiható feltételeket, melyek hozzájárulnak az NLCAPI3 v3.2.0 kriptográfiai modullal kifejlesztett elektronikus aláíró alkalmazások által kezelt aláírások biztonságához.

1. számú feltétel: *Az NLCAPI3 v3.2.0 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. Ezért csak olyan környezetben szabad alkalmazni, amelyben önkibocsátott (self issued) tanúsítvány a tanúsítványláncban nem fordul elő, valamint amelyben a CRL-t és a végfelhasználói tanúsítványt ugyanazzal a CA tanúsítvánnyal kell ellenőrizni.*

2. számú feltétel *Az NLCAPI3 v3.2.0 kriptográfiai modullal 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 feltétel: *Fokozott vagy minősített elektronikus aláírások létrehozásánál az MD5 lenyomatoló algoritmus nem használható.*

4. számú feltétel: *Bár az NLCAPI3 v3.2.0 kriptográfiai modul rendelkezik önvédelmi funkcióval, 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 feltétel: *Az NLCAPI3 v3.2.0 kriptográfiai modul működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék az NLCAPI3 v3.2.0 kriptográfiai modul funkcionális összetevőinek sértetlenségét megakadályozva, hogy behatolók elrontsák ezt.*

6. számú feltétel: *Az NLCAPI3 v3.2.0 kriptográfiai modul működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az NLCAPI3 v3.2.0 kriptográfiai modul, 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/ISSS/E-Sign; Area G1 14170:2004 munkacsoport egyezmény: Security Requirements fro Signature Creation System

CEN/ISSS/E-Sign; Area G2 14171:2004 munkacsoport egyezmény: Procedures for Elecronic Signature Verification

CEN/ISSS/E-Sign; Area V 14172-4:2001 munkacsoport egyezmény: Signature Creation Application and Procedures for Electronic Signature Verification

ETSI TS 101 733 v1.4.0 Electronic Signature Formats

ETSI TS 101 862 v1.3.2 Qualified Certificate profile

ETSI SR 002 176 v1.1.1 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures

ETSI TS 101 903 v1.2.2 XML Advanced Electronic Signatures (XAdES)

Szabványok

CAPI	Microsoft Cryptographic Application Interface
PKCS#1	RSA Cryptographic Standard /RFC2313/
RSA	Rivest-Shamir-Adleman (public key cryptosystem) /ANSI X9.31/
SHA-1	Secure Hash Algorithm /FIPS PUB 180-1/

RFC3061 Time-Stamp Protocol (TSP)

RFC3275 XML Digital Signatures (XMLDSig)

RFC3280 Certificate and Certificate Revocation List (CRL) Profile

PKCS #7: Cryptographic Message Syntax Standard

4. számú melléklet

A tanúsítási eljárás egyéb jellemzői

A tanúsításhoz figyelembe vett, fejlesztői dokumentumok

- Kérelem a tanúsítás elvégzéséhez
- NLCAPI 3 funkcióspecifikáció v1.0
- NLCAPI 3 magas szintű terv v1.0
- NLCAPI 3 felhasználói dokumentáció
- NLCAPI 3 tesztelési dokumentáció v1.0

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

- Értékelési jelentés az NLCAPI3 V3.2.0 kriptográfiai modulról, mint elektronikus aláíró és ellenőrző alkalmazás kifejlesztésére alkalmas programozói könyvtárról (Készítette HunGuard Kft.)

A követelményeknek való megfelelést ellenőrző vizsgálat garancia szintje

A jelen tanúsítási jelentéshez figyelembe vett, a fejlesztőktől független ellenőrző vizsgálat garancia szintje az ISO 15408 /Common Criteria/ **EAL 3**-as szintjéhez hasonló volt. /Az EAL3 a fejlesztőktől független garantált biztonság közepes szintjét biztosítja./

A fejlesztőktől független ellenőrző vizsgálat összefoglalásaként egy értékelési jelentés készült.
Jelen tanúsítási jelentés alapvetően a fejlesztői bizonyítékokra, valamint az értékelési jelentésben megfogalmazott és dokumentált eredményekre épül.

Az értékelés az alábbi garancia osztályokra terjedt ki:

- fejlesztés
- útmutató dokumentumok
- tesztek

Az értékelés során, a fentieken kívül a fejlesztőktől független minta tesztelésre, illetve áthatolás tesztelésre is sor került.