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 006/2002 számú kijelölési okiratával kijelölt terméktanúsító szervezet

tanúsítja,

hogy a
Kopint-Datorg Részvénytársaság
által kifejlesztett és forgalmazott

MultiSigno Developer Professional
aláíró alkalmazás fejlesztő készlet (Pack.dll)

2.0-es verzió

elektronikus aláírási termék

a 2. számú melléklet biztonságos felhasználásra vonatkozó feltételeinek figyelembe vételével

megfelel

a 2001. évi XXXV. törvényben szereplő

minősített elektronikus aláírás

létrehozása és ellenőrzése céljából történő
szabványos és biztonságos alkalmazások fejlesztéséhez,
az 1. számú mellékletben áttekintett funkcionalitásra.

Jelen tanúsítvány a HUNG-TJ-010-2003. számú tanúsítási jelentés alapján került kiadásra.
Készült a Kopint-Datorg Részvénytársaság megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-010/2003.**
A tanúsítás kelte: 2003. július 10.
A tanúsítvány érvényességi ideje: 2006. július 10.
Mellékletek: tulajdonságok, feltételek, követelmények, egyéb jellemzők, összesen 6 oldalon.

PH.

Tanúsítási igazgató: Ügyvezető igazgató

1. számú melléklet

A MultiSigno Developer Professional legfontosabb tulajdonságainak összefoglalása

A **MultiSigno Developer Professional** egy olyan fejlesztői készlet, mely Windows 32-bites operációs rendszerhez biztosít DLL felületet (a későbbiekben a termékre **Pack.dll 2.0** néven is hivatkozni fogunk). Önmagában működésképtelen, megbízható aláíró alkalmazások fejlesztésére használható fel.
A MultiSigno Developer Professional által nyújtott felület lehetőséget nyújt XML csomagok nyitására, digitális aláírására, az aláírások ellenőrzésére, valamint objektumok és aláírások kezelésére.
A MultiSigno Developer Professional segítségével olyan aláíró (aláírás-létrehozó és aláírás-ellenőrző) alkalmazások fejleszthetők, melyek alkalmasak minősített elektronikus aláírások létrehozására és ellenőrzésére.

A MultiSigno Developer Professional az alábbi szabványos formátumokat és protokollokat támogatja:

- „XML Advanced Digital Signature” (XAdES) szabványos csomagok kezelése,
- X.509 v3 tanúsítványok kezelése,
- tanúsítvány visszavonási listák lekérdezése a hitelesítés-szolgáltatóktól (HTTP, HTTPS, LDAP protokollokkal, a tanúsítványból kiolvasott elérési helyről),
- az aláírás időpontjának aláírt biztonsági tulajdonságként való kezelése,
- időbélyegzés készíttetés és ellenőrzés,
- aláírás ellenőrzés.

A fenti aláírás létrehozó és ellenőrző funkciókon kívül a MultiSigno Developer Professional támogatja a csomagok titkosítását és dekódolását is, de ez a funkcionalitás kívül esik jelen tanúsítvány hatókörén.
Ugyancsak kívül esnek jelen tanúsítvány hatókörén a MultiSigno Developer Professional bázisán fejlesztett aláíró alkalmazások (bár a fejlesztő eszköz funkcionalitása, biztonságos és korrekt megvalósítása nyilván átöröklődik az ebből – szakszerűen és gondosan – fejlesztett alkalmazásokba).

A MultiSigno Developer Professional (Pack.dll 2.0) fejlesztő készlet a Windows operációs rendszerek erőforrásaira, eszközeire támaszkodik. DLL elemei a Microsoft Crypto API függvényeit hívják meg, s ezen keresztül (tetszőleges szabványos CSP-t használva, valamint a CSP-vel kommunikáló driver-eken keresztül) magát az aláírás-létrehozó eszközt (intelligens kártyát) szólítják meg, mely szintén igen sokféle lehet. Az aláírandó/ellenőrizendő XML struktúrára az MS Crypto API-n keresztül történik az aláírás létrehozásának/ ellenőrzésének aktivizálása.

A MultiSigno Developer Professional az alábbi algoritmusokat valósítja meg, illetve aktivizálja:

- a MultiSigno Developer Professional által megvalósított (egy csomagon belül kezelt dokumentumok integritásának ellenőrzésére használt) lenyomatoló függvény: **SHA-1**
- a MultiSigno Developer Professional által a CSP-n aktivizált (az XML struktúra digitális aláírására használt) lenyomatoló függvény: **SHA-1**
- a MultiSigno Developer Professional által a CSP-n aktivizált, az intelligens kártyával végrehajtott (XML struktúra aláírására használt) digitális aláíró algoritmus: **RSA (1024 bit)**

2. számú melléklet

A biztonságos felhasználás feltételei

Az alábbiakban összefoglaljuk azokat a feltételeket, melyek betartása hozzájárul a MultiSigno Developer Professional segítségével fejlesztett aláíró alkalmazások biztonságához.
Ezek a feltételek a fejlesztésekkel szembeni általános minőségbiztonsági (tervezési, tesztelési, dokumentálási stb.) követelményeken túlmutatóan az aláírás-specifikus elemek ellenőrzött védelmi szintjét szándékoznak garantálni.

A feltételek arra vonatkoznak, hogy a MultiSigno Developer Professional felhasználásával aláíró alkalmazásokat fejlesztők, hogyan használják ezt a terméket, saját fejlesztésükhöz. Így tulajdonképpen nem is a MultiSigno Developer Professional termékre, hanem az ebből fejlesztett (esetelegesen későbbi tanúsítási eljárás hatókörébe tartozó) aláíró alkalmazásra vonatkoznak.

a) Kötelezően betartandó feltételek:

1. A MultiSigno Developer Professional-t felhasználóihoz (akik aláíró alkalmazásokat fejlesztenek felhasználásukkal) CD-n szállítják. Használatba vétel előtt kötelező másolatot készíteni róla, hogy az eredetit mesterpéldányként lehessen felhasználni a későbbiekben végrehajtandó sértetlenség ellenőrzések során.

2. A MultiSigno Developer Professional-lal fejlesztett aláíró alkalmazások elkészülésekor a fejlesztők felelőssége a felhasznált és a mesterpéldányként elmentett MultiSigno Developer Professional függvényeinek sértetlenségének ellenőrzése /valóban a tanúsított fejlesztő készlet elemeit építették-e be/.

b) Ajánlások minősített aláírásokat kezelő alkalmazások fejlesztőinek:

A MultiSigno Developer Professional /"aláíró alkalmazást fejlesztő munkaállomásokon"/ alapvetően elszigetelt működtetési környezetben használandó, de kiegészítő feltételek garantálása esetén védett működtetési környezetben is lehet fejleszteni vele (sőt a teljes funkcionalitás végső tesztelése csak ilyen körülmények között valósítható meg).

Elszigetelt működtetési környezet (kisebb fejlesztéseknél ez a tipikus eset) esetén a fejlesztői készletet (és egyúttal a fejlesztés alatt álló aláíró alkalmazást) az védi, hogy nincs (sohasem) kapcsolódás kommunikációs hálózatokra (Internet, Intranet), és a működtetési környezetben olyan védelmi intézkedéseket valósítanak meg, melyek kivédik a jogosulatlan manuális hozzáférésen és adathordozóról történő adatbevitelen alapuló támadásokat is/. A Pack.dll 2-0 felhasználásával alapvetően ilyen környezetben ajánlott fejleszteni, tesztelni. Ugyanakkor az ebből fejlesztett, teljes funkcionalitást biztosító végterméket nem lehet teljeskörűen ebben a működtetési környezetben tesztelni, mivel a MultiSigno Developer Professional bázisán kifejlesztett aláíró alkalmazás:

- aláírás létrehozásánál nem képes tesztelni az időbélyegzés részét (hiszen nem kerülhet hálózati kapcsolatba egyetlen időbélyeg-szolgáltatóval sem),

- aláírás ellenőrzéséhez nem képes tesztelni azt a funkcióját, hogy amennyiben az adott munkaállomás nem rendelkezik érvényes visszavonási listával (amit elszigetelt környezetben adminisztratív úton, egy más munkaállomáson letöltött CRL adathordozóról történő betöltésével lehet biztosítani).

Védett működtetési környezet (kisebb fejlesztések esetén nem ez a tipikus eset) esetén a fejlesztői készletet (és egyúttal a fejlesztés alatt álló aláíró alkalmazást) a működtetési környezet nagy bizonyossággal megvédi a kommunikációs hálózatok (Internet, Intranet) irányából érkező, valamint a jogosulatlan manuális hozzáférésen és az adathordozóról történő adatbevitelen alapuló támadásoktól.

Általános működtetési feltételek

3. Eljárásrendi/szervezeti védelmi intézkedésekkel kell támogatni az aláíró alkalmazás fejlesztést megvalósító számítógép(ek)re irányuló olyan támadások kivédését, melyek manuális hozzáférésen, illetve adathordozóról történő adatbevitelen alapulnak. Garantálni kell, hogy a fejlesztés technikai környezete, valamint a fejlesztett programok és az ehhez felhasznált fejlesztő készlet funkcióit ne lehessen manipulálni, melyet különösen vírus és Trójai faló bejuttatása okozhat. Minden újonnan telepített szoftvernek manipulációtól mentesnek kell lennie.
   /A fenti intézkedések döntően ahhoz kellenek, hogy a fejlesztendő aláíró alkalmazás és az ennek bázisát képező fejlesztő készlet ne manipulálódjon./

4. A fejlesztő környezetben konfiguráció menedzselési eljárások kidolgozásával és betartásával kell garantálni a fejlesztett termék sértetlenségét azzal, hogy fegyelmet és ellenőrzést követelnek meg a fejlesztendő termék és más ezzel összefüggő információ pontosításában és módosításában.
   /A konfiguráció menedzselése akadályozza a fejlesztés alatt álló alkalmazások egyes verzióinak jogosulatlan módosítását, bővítését vagy törlését, illetve hozzájárul a mégis bekövetkező felhatalmazás nélküli változtatások észleléséhez (a verziónként elkülönítetten is letárolt példányok időszakos összehasonlításával)./

A védett működtetési környezetben történő felhasználás járulékos feltételei

5. Amennyiben a fejlesztő környezetnek hálózati kapcsolatai is vannak a 4. feltételben elvárt konfiguráció menedzselési eljárásokon kívül rendszeres időnként ellenőrizni kell a fejlesztő készlet és a fejlesztett aláíró alkalmazás verziók sértetlenségét (az elkülönítetten is letárolt (mester) példányok időszakos összehasonlításával).

Az elszigetelt működtetési környezetben történő felhasználás feltételei

Az elszigetelés számos fenyegetést eleve kizár (hálózati támadások), a fenyegetések más részét pedig az általános működtetési feltételek lefedik. (Nincs járulékos feltétel).

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 munkacsoport egyezmény: Security Requirements for Signature Creation Systems

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

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

ETSI TS 101 733 Electronic Signature Formats

ETSI TS 101 903 XML Advanced Electronic Signatures (XadES)

Szabványok

CAPI	Microsoft Cryptographic Application Programming Interface
PKCS #1	RSA Cryptography Standard /RFC 2313/
RSA	Rivest-Shamir-Adleman (public key cryptosystem) /ANSI X9.31/
SHA-1	Secure Hash Algorithm /FIPS PUB 180-1/

4. számú melléklet

A tanúsítási eljárás egyéb jellemzői

A tanúsításhoz figyelembe vett egyéb fejlesztői dokumentumok

- Kérelem a tanúsítás elvégzésére
- Kérdőív a tanúsítás kérelmezéséhez
- MultiSigno koncepcionális terv
- Pack._dll 2.0 áttekintés /magas szintű fejlesztői leírás a DLL könyvtárról/
- A függvények részletes leírása, paraméterezése és a paraméterek leírása
- Pack.dll /a függvény könyvtár/
- Pack.cpp, xmlHandleWrapper.cpp, MyByteArray.cpp, KDLDAP.cpp /forráskódok/

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

- Értékelési jelentés a MultiSigno Developer Professional vizsgálatáról

A követelményeknek való megfelelést ellenőrző független vizsgálat módszere

A független vizsgálatok a forráskódok ellenőrzésre és a tesztelésre helyezte a hangsúlyt, ezért az egyéb (a biztonságos tervezésre, megvalósításra és működésre indirekt úton bizalmat erősítő) értékelési megközelítések kisebb szerephez jutottak.
Az ellenőrző vizsgálat a MultiSigno Developer Professional biztonsági viselkedésének megértése érdekében elemezte a biztonsági funkciókat, ehhez felhasználta a fejlesztők által készített dokumentációkat.
Az ellenőrző vizsgálat kitért a következők elemzésére:

- a minősített aláírásokra is alkalmazható aláíró alkalmazások mely funkcionális és biztonsági követelményeit kell, illetve célszerű kielégítenie a DLL-nek, s mely maradhat az aláíró alkalmazás feladata,
- a DLL felvállalja-e a szükséges követelmények kielégítését,
- a DLL teljesíti-e a felvállalt követelményeket.

a MultiSigno Developer Professional forráskódjainak elemzésével hangsúlyosan vizsgálta az alábbiakat:

- nincs-e hiba a programban,
- hibás paramétereket lekezeli-e a program,
- a kritikus részek tényleg azt végzik-e, amit kell,
- a belső függvények meghívása, visszaadott hibaüzenetek lekezelése megfelelő-e.

Az ellenőrző vizsgálat ezen kívül:

- funkcionális teszteket végzett (a DLL egyes függvényeire, külön erre a célra kifejlesztett speciális tesztprogram felhasználásával),
- áttekintette a fejlesztők által végzett tesztelést, elemezte ennek teljeskörűségét,
- a fejlesztőktől független minta tesztelést végzett /minta felhívó programokkal/,
- értékelte a biztonsági funkciók erősségét, a termék sebezhetőségét.

A MultiSigno Developer biztonsági funkciók értékelt erőssége: **magas szintű**