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
aláíró alkalmazás fejlesztő készlet

1.2-es verzió

elektronikus aláírási termék

a 2. számú melléklet biztonságos felhasználásra vonatkozó feltételeinek figyelembe vételével

megfelel

a 2001. évi XXXV. törvényben szereplő

fokozott biztonságú elektronikus aláírás

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

Jelen tanúsítvány a HUNG-TJ-003-2003. számú tanúsítási jelentés alapján került kiadásra.
A tanúsítványt a Kopint-Datorg Részvénytársaság kérésére állítottuk ki.

A tanúsítvány regisztrációs száma: **HUNG-T-003/2003.**
A tanúsítás kelte: 2003. január 22.
A tanúsítvány érvényességi ideje: 2006. január 22.
Mellékletek: tulajdonságok, feltételek, követelmények, egyéb jellemzők, összesen: 5 oldalon.

PH.

Tanúsítási igazgató: Ügyvezető igazgató

1. számú melléklet

A MultiSigno Developer legfontosabb tulajdonságainak összefoglalása

A MultiSigno Developer egy olyan fejlesztői készlet, mely Windows 32-bites operációs rendszerhez biztosít DLL felületet. Önmagában működésképtelen, megbízható aláíró alkalmazások fejlesztésére használható fel.
A MultiSigno Developer által nyújtott felület lehetőséget nyújt XML csomagok nyitására, dokumentumok és megjegyzések kezelésére, digitális aláírására és aláírások ellenőrzésére. Segítségével XML digitális aláírás szabványon alapuló aláíró (aláírás-létrehozó és aláírás-ellenőrző) alkalmazások fejleszthetők.
Az alábbi szabványos formátumokat és protokollokat támogatja:

- „XML Signature" szabványos csomagok kezelése, közte:
  - együttes aláírások kezelése (több dokumentumot összefogó csomag aláírása),
  - többszörös aláírások kezelése (több személy aláírása ugyanazon a csomagon),
- X.509 v3 tanúsítványok kezelése,
- tanúsítvány visszavonási listák lekérdezése a hitelesítés-szolgáltatóktól (HTTP, HTTPS, LDAP protokollokkal, a tanúsítványból kiolvasott elérési helyről),
- aláírás ellenőrzés (ahol mindig a rendszer idő az ellenőrzés alapja),
- időbélyegzés készíttetés és ellenőrzés (az RFC 3161 szabványt követő időbélyegző-szolgáltatókkal együttműködve).

A fenti aláírás létrehozó és ellenőrző funkciókon kívül a MultiSigno Developer 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 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 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 az alábbi algoritmusokat valósítja meg, illetve aktivizálja:

- a MultiSigno Developer által megvalósított (egy csomagon belül kezelt dokumentumok integritásának ellenőrzésére használt) lenyomatoló függvény: **SHA-1**
- a MultiSigno Developer által a CSP-n aktivizált (az XML struktúra digitális aláírására használt) lenyomatoló függvény: **MD5**
- a MultiSigno Developer 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 segítségével fejlesztett aláíró alkalmazások fokozott 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 között vannak kötelezően betartandó, a tanúsítvány érvényességére kiható feltételek, és vannak olyan feltételek, amelyek az aláírások biztonságára jelentős befolyással bírnak, ezért fokozott (nem minősített) aláíráshoz, ahol a lehetőség adott, ezen feltételek betartása erősen ajánlott.

a) Kötelezően betartandó feltételek:

1. A MultiSigno Developer-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-rel fejlesztett aláíró alkalmazások elkészülésekor a fejlesztők felelőssége a felhasznált és a mesterpéldányként elmentett MultiSigno Developer függvényei sértetlenségének ellenőrzése /valóban a tanúsított fejlesztő készlet elemeit építették-e be/.

b) Ajánlások a fokozott biztonságú aláírás-alkalmazásokhoz:

A MultiSigno Developer /”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 MultiSigno Developerrel 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 bázisán kifejlesztett aláíró alkalmazás:

- aláírás létrehozásánál nem képes tesztelni időbélyegzés opcióját (hisz 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 2. 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)

ISO/IEC 14508-3 Information Technology. Security technique. Evaluation criteria for IT security. Part 3: Security assurance requirements

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
- Pack._dll_interface.doc /felső-szintű fejlesztői leírás a DLL könyvtárról/
- Pack.h /a függvények részletesebb leírása, paraméterezése és a paraméterek leírása/
- Pack.dll /maga a függvény könyvtár/

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

- Értékelési jelentés a MultiSigno Developer (1.2) vizsgálatáról

A követelményeknek való megfelelést ellenőrző független vizsgálat garancia szintje

A tanúsításhoz figyelembe vett, a fejlesztőktől független ellenőrző vizsgálat garancia szintje az ISO 14508 /Common Criteria/ **EAL 2**-es szintjéhez hasonló volt. /Az EAL2 a fejlesztőktől függetlenül garantált biztonság mérsékelt szintjét biztosítja./ Ez az alábbi vizsgálatokat jelentette:

Az ellenőrző vizsgálat a MultiSigno Developer biztonsági viselkedésének megértése érdekében elemezte a biztonsági funkciókat, ehhez felhasználta az alábbi fejlesztői dokumentációkat:

- a MultiSigno Developer konfigurációs tételei,
- a szállítás eljárásai,
- a szoftver telepítésének, elindításának eljárásai,
- felső-szintű tervek,
- felhasználásra vonatkozó útmutatók,

Ezeken kívül:

- funkcionális teszteket végzett (a MultiSigno Standard felhasználásával) /lásd az erről készült HUNG-T-003/2003. regisztrációs számú tanúsítvány/
- 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

A biztonsági funkciók erőssége: **középszintű**