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 006/2002/2004 számú kijelölési okiratával kijelölt tanúsító szervezet

tanúsítja,

hogy a

MÁV INFORMATIKA Kft.
által kifejlesztett és forgalmazott

DSign Library 1.6

elektronikus aláíró alkalmazás fejlesztésére alkalmas
programozói 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 elektronikus aláírás

létrehozásában és ellenőrzésében történő
szabványos és biztonságos alkalmazások fejlesztéséhez

Jelen tanúsítvány a HUNG-TJ-018-2004. számú tanúsítási jelentés alapján került kiadásra.
Készült a MÁV INFORMATIKA Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-018-2004.**
A tanúsítás kelte: 2004. április 26.
A tanúsítvány érvényességi ideje: 2007. április 26.
Melléklet: tulajdonságok, feltételek, követelmények, egyéb jellemzők összesen 6 oldalon.

PH.

Tanúsítási igazgató

Ügyvezető igazgató

A DSign Library 1.6 legfontosabb tulajdonságainak összefoglalása

A DSign Library 1.6 egy programozói könyvtár, amely a rá épülő alkalmazás fejlesztői számára elektronikus aláírással kapcsolatos funkcionalitást nyújt.
Mindezt szabványos formában (XAdES XML Advanced Electronic Signatures ETSI TS 101 903) teszi.
A DSign Library teljes mértékben a Windows operációs rendszer erőforrásaira, eszközeire támaszkodik. A Crypto API-n keresztül a Microsoft vagy más gyártók CSP-jét használja. Ezen keresztül szólítja meg akár az aláírás-létrehozó eszközt. Az aláírás során legenerálható vele a megfelelő XML struktúra, majd az aláírandó XML elemre a Microsoft Crypto API-ján keresztül elkészíthető az aláírás.
A DSign Library 1.6 fejlesztő készlet elektronikus aláírással és az aláírás ellenőrzésével kapcsolatos funkcionalitást valósít meg a Microsoft Crypto API-jára és azon keresztül különböző CSP-kre épülve. A Library képes különböző aláírási szabályzatoknak megfelelni, de azokat szabványos elektronikus aláírási szabályzatként automatikusan nem képes kezelni. A tág keretek közti variálhatósága miatt azonban számos aláírási szabályzat megvalósítható a Library segítségével.

A DSign Library 1.6 jellemző tulajdonságai:

- XAdES és XAdES-T szabvány szerinti hiteles dokumentum formátum
- Szabványos X.509 tanúsítványok kezelése (Windows tanúsítványtárban)
- Az RFC 3161 szabvány szerinti időbélyeg szolgáltatás támogatása
- Felhasználó azonosítás támogatása időbélyeg szolgáltatás használatához
- Tanúsítvány érvényességi állapot teljes körű ellenőrzése.
- Aláíró eszköz kezelése (CSP-n keresztül)

A biztonságos használat feltételei

Az alábbiakban összefoglaljuk azokat a kötelezően betartandó, a jelen tanúsítvány érvényességére kiható feltételeket, melyek hozzájárulnak a DSign Library 1.6 programozói könyvtárral kifejlesztett elektronikus aláíró alkalmazások által kezelt aláírások biztonságához.

1. számú feltétel: *A DSign Library 1.6 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.*

2. számú feltétel: *A DSign Library 1.6 programozói könyvtárban a dokumentumhoz illetve magához a dossziéhoz kapcsolt megjegyzések nem minősülnek aláírási tulajdonságnak. Az alkalmazandó Aláírási Szabályzatnak tiltania kell jogi következménnyel járó adatok írását a megjegyzésekbe.*

3. számú feltétel: *A DSign Library 1.6 programozói könyvtárat olyan Elektronikus Aláírási Szabályzattal együtt kell használni, amely az elektronikus aláírás során használt algoritmusokra és input formátumokra az alábbi, megfelelő követelményeket fogalmazza meg:*

- *aláíró algoritmus: RSA*
- *lenyomatoló algoritmus: SHA-1*
- *aláírás formátum: emsa-pkcs1-v1_5*

4. számú feltétel: *A DSign Library 1.6 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírás-létrehozó eszközzel kommunikáló összetevőt (CSP) ne lehessen jogosulatlanul módosítani.*

5. számú feltétel: *A DSign Library 1.6 programozói könyvtár 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.*

6. számú feltétel: *A DSign Library 1.6 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék A DSign Library 1.6 programozói könyvtár funkcionális összetevőinek sértetlenségét megakadályozva, hogy behatolók elrontsák ezt.*

7. számú feltétel: *A DSign Library 1.6 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy a DSign Library 1.6 programozói könyvtárat, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.*

TERMÉKMEGFELELŐSÉGI KÖVETELMÉNYEK

Követelményeket és szabályokat tartalmazó dokumentumok

Követelmények

Az elektronikus aláírásról szóló 2001. évi XXXV.törvény

CEN/ISSS/E-Sign; Area G1 14170 munkacsoport egyezmény: Security Requirements fro Signature Creation System

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 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/

A tanúsítási eljárás egyéb jellemzői

A tanúsításhoz figyelembe vett fejlesztői dokumentumok

- Kérelem a tanúsítás elvégzéséhez
- DSign Library 1.6 Telepítési útmutató – 2004.02.17
- Funkció specifikáció - A DSign Library programozói könyvtárhoz 1.6 verzió – 2004.02.20
- Magas szintű terv - - A DSign Library programozói könyvtárhoz 1.6 verzió – 2004.02.27
- DSign Library 1.6 Adminisztrátori útmutató – 2004.02.17
- DSign Library 1.6 Felhasználói útmutató – 2004.02.17
- DSign Library 1.6 Teszt jegyzőkönyvek – 2004.02.17
- DSign Library 1.6 Tesztlefedettség elemzés – 2004.02.25

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

- Értékelési jelentés a DSignLibrary 1.6 elektronikus aláíró alkalmazás fejlesztésére alkalmas programozói könyvtárról (Készítette HunGuard Kft.)

A követelményeknek való megfelelést ellenőrző független vizsgálat módszere

Jelen tanúsítási jelentéshez figyelembe vett, a fejlesztőktől független ellenőrző vizsgálat garancia szintje az ISO 14508 /Common Criteria/ **EAL 2**-es szintjéhez hasonló volt. / Az EAL 2 a fejlesztőktől függetlenül garantált biztonság mérsékelt szintjét biztosítja, mely elegendő a fokozott biztonságú elektronikus aláíráshoz használható aláírási termékekre. /
A fejlesztőktől függetlenül ellenőrző vizsgálatról összefoglalásként egy értékelési jelenté 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:

- Konfiguráció menedzselés
- kiszállítás és működtetés
- fejlesztés
- útmutató dokumentumok
- tesztek

Az értékelés során a fejlesztőktől független minta tesztelésre is sor került.