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 UI 1.6

aláíró alkalmazás

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 felhasználásra

Jelen tanúsítvány a HUNG-TJ-019-2004. számú tanúsítási jelentés alapján került kiadásra.
Készült a MÁV INFORMATIKA Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-019-2004.**
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

1. számú melléklet

A DSign UI 1.6 legfontosabb tulajdonságainak összefoglalása

A tanúsított termék a MÁV INFORMATIKA Kft. által fejlesztett és forgalmazott DSign UI 1.6 aláíró alkalmazás.

A DSign Ui 1.6 aláíró alkalmazás elektronikus dokumentumok elektronikus aláírással történő ellátását, és ezen aláírások kezdeti ellenőrzését támogatja. Az aláírt adat objektumot az ETSI TS 101 903 dokumentumában specifikált XAdES illetve XAdES-T (XML Advanced Electronic Signature) formátumban tárolja.

Az alkalmazás Microsoft Windows 2000/2003/XP operációs rendszeren és Microsoft . NET Framework környezetben működik. Az alkalmazás alapja a szintén a MÁV INFORMATIKA Kft. által fejlesztett DSign Library 1.6 programozói könyvtár. E könyvtárban lévő objektumokon keresztül éri el az operációs rendszer Crypto API-ját, amely az operációs rendszer részeként meg lévő, vagy más gyártó által írt CSP (Crypto Service Provider) segítségével tud kommunikálni aláíró eszközzel. Az aláírás folyamat során a megfelelő XML struktúrák legenerálódnak az aláírandó adatra az aláírás a CSP-n keresztül készül el.

A DSIgn UI 1.6 aláíró alkalmazás elektronikus dossziék hatékony kezelésére alkalmazható. Ezekhez a dossziékhoz dokumentumok adhatóak, vagy törölhetőek ki akár csoportosan is. Ezekhez a dokumentumokhoz egyenként vagy összevontan elektronikus aláírás készíthető. Az aláírások ideje időpecséttel hitelessé tehető.

Az aláírások azonnal ellenőrizhetőek. Aláírás ellenőrzésekor az érvényes aláírási szabályzat betartása a felhasználó felelőssége. Az ellenőrzés kiegészíthető offline (a Windows tanúsítványában tárolt) vagy online (a tanúsítvány CRL elérési hely mezőjében leírt URL-ről közvetlenül letöltött) visszavonási lista vizsgálattal is. Az aláírás eredménye érvényes vagy érvénytelen lehet. Érvénytelen esetben kijelzésre kerül a hiba oka.

Aláírás ellenőrzéshez költségmentesen elérhető alkalmazás létezik DSign Viewer 1.6 néven.

A DSign UI 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)

2. számú melléklet

A biztonságos felhasználás feltételei

Az alábbiakban összefoglaljuk azokat a kötelezően betartandó, a jelen tanúsítvány érvényességére kiható feltételeket, melyek hozzájárulnak a DSign UI 1.6 aláíró alkalmazás által kezelt aláírások biztonságához.

***1 számú feltétel**: Ha az aláírási szabályzat kiköti a CRL ellenőrzést, valamint az adott hitelesítés-szolgáltató a már lejárt tanúsítványokat törli a visszavonási listából, akkor - mivel a CRL érvényességét az ellenőrzés időpontjához viszonyítja a DSign UI 1.6 aláíró alkalmazás - CRL ellenőrzést csak akkor szabad kérni, ha az ellenőrzés időpontja korábbi, mint a tanúsítvány érvényesség lejárati dátuma. Ellenkező esetben a CRL ellenőrzés nem valós eredményt adhat.*

***2. számú feltétel:** A DSign UI 1.6 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírni kívánt dokumentumokhoz szükséges megjelenítő alkalmazások megfelelő módon telepítve és konfigurálva legyenek.*

***3. számú feltétel:** A DSign UI 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.*

***4. számú feltétel:** A DSign UI 1.6 aláíró alkalmazásban 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.*

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

6. számú feltétel: *A DSign UI 1.6 aláíró alkalmazás 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.*

7. számú feltétel: *A DSign UI 1.6 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék A DSign UI 1.6 aláíró alkalmazás funkcionális összetevőinek sértetlenségét megakadályozva, hogy behatolók elrontsák ezt.*

8. számú feltétel: *A DSign UI 1.6 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy a DSign UI 1.6 aláíró alkalmazást, 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

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/

4. számú melléklet

A tanúsítási eljárás egyéb jellemzői

A tanúsításhoz figyelembe vett, fejlesztői dokumentumok

- Kérelem a tanúsítás elvégzéséhez
- DSign UI 1.6 telepítési útmutató 2004. február 17.
- Funkció specifikáció DSign UI 1.6 2004. február 20.
- Magas szintű terv DSign UI 1.6 2004. február 25.
- DSign UI 1.6 használati útmutató 2004. február 17.
- Fejlesztői tesztjegyzőkönyv 1-24 2004. február 17.
- Fejlesztői teszt lefedettség elemzés 2004. február 25.

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

- Hung-TJ-018-2004 számú Tanúsítási jelentés a DSignLibrary 1.6 elektronikus aláíró alkalmazás fejlesztésére alkalmas programozói könyvtárról (készítette: HunGuard Kft)
- Értékelési jelentés a DSign UI 1.6 elektronikus aláíró alkalmazásról (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 14508 /Common Criteria/ **EAL 2**-es szintjéhez hasonló volt. /Az EAL2 a fejlesztőktől független garantált biztonság mérsékelt 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 érékelés az alábbi garanciaosztályokra terjedt ki:

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

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