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
E-Group Magyarország Rt.
által kifejlesztett és forgalmazott

Signed Document eXpert (SDX) Professional

1.0-es verzió

aláíró alkalmazás

az 1. számú mellékletben áttekintett funkcionalitással, valamint

a 2. számú melléklet biztonságos felhasználásra vonatkozó feltételeinek figyelembe vételével

megfelel

a 2001. évi XXXV. törvényben szereplő
minősített elektronikus aláírás

létrehozásában és ellenőrzésében történő felhasználásra

Jelen tanúsítvány a HUNG-TJ-017-2004. számú tanúsítási jelentés alapján került kiadásra.
Készült az E-Group Magyarország Részvénytársaság megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-017/2004.**
A tanúsítás kelte: 2004. február 15.
A tanúsítvány érvényességi ideje: 2007. február 15.
Mellékletek: tulajdonságok, feltételek, követelmények, egyéb jellemzők, összesen 5 oldalon.

PH.

Tanúsítási igazgató: Ügyvezető igazgató

1. számú melléklet

A Signed Document eXpert (SDX) Professional legfontosabb tulajdonságainak összefoglalása

Az SDX Professional aláíró alkalmazás elektronikusan aláírt dokumentumok létrehozását és elektronikusan aláírt dokumentumok aláírásának ellenőrzését támogatja, szabványos formában (XAdES, XML Advanced Electronic Signatures, ETSI TS 101 903).
A Windows operációs rendszer erőforrásaira, eszközeire támaszkodik. A Crypto API függvényeit használja, amely Windows-os vagy más gyártó CSP-jét használja, ezek pedig magát a biztonságos aláírás-létrehozó eszközt (intelligens kártyát) megszólító, vele kommunikáló driver-eket hívnak meg.
Az SDX Professional az alkalmazási környezetek széles körében teszi lehetővé az elektronikus aláírás létrehozását, ellenőrzését. Az elektronikus aláíráshoz kapcsolódó feladatokat képes megoldani állomány szinten, levelező alkalmazásokban, browser-alapú alkalmazásokban, dokumentum kezelő és archiváló rendszerek környezetében, illetve egyedi és tömeges aláírás létrehozás/ellenőrzés esetén is.
Az SDX Professional szabványos interfészeken keresztül kapcsolódik a hitelesítés-szolgáltatókhoz (CRL lekérdezés) és szabványos függvényhívásokon keresztül éri el az aláíráshoz kapcsolódó alacsony szintű funkciókat (MS Crypto API).
Az SDX Professional mindkét alapfolyamata (aláírás létrehozása, aláírás ellenőrzése) az aláírás létrehozására és ellenőrzésére vonatkozó előírásokat definiáló Elektronikus Aláírási Szabályzaton (EASZ) alapul. Az SDX Professional EASZ független, az aláírásra és annak ellenőrzésére vonatokozó követelmények szabványos módon, formalizált nyelven (XML) leírhatók és az SDX Professional rendszerében szereplő eszközök ezen formális szabályzat alapján hozzák létre, illetve ellenőrzik a hiteles dokumentumokat.
A formalizált szabályzatokat elérhetővé kell tenni az aláíró és ellenőrző fél számára, és aláíráskor a használt szabályzat autentikus módon hozzákapcsolódik az aláírt dokumentumhoz. Ennek a megoldásnak a hatására ugyanazokkal az eszközökkel különböző felhasználási célra lehet dokumentumokat hitelesíteni a megfelelő EASZ kiválasztásával.

Az SDX Professional jellemző tulajdonságai:

- XML Advanced Electronic Signatures szabvány szerinti hiteles dokumentum formátum.
- Az alkalmazás és az alkalmazási környezet integritásvédelmének biztosítása digitális aláírással és annak ellenőrzésével.
- Windows (Explorer) integráció.
- Szabványos, X.509 tanúsítványok kezelése.
- Egymásba ágyazott, többszörös elektronikus aláírás kezelésének támogatása.
- Az RFC 3161 szabvány szerinti időbélyeg szolgáltatás támogatása.
- Felhasználó azonosítás támogatása időbélyeg szolgáltatás használatához.
- Tanúsítvány érvényességi állapotának teljes körű ellenőrzése.
- BALE kezelése.
- Szabványos XML elektronikus aláírási szabályzat kezelése.
- Elektronikus Aláírási Szabályzat végrehajtás (dokumentum formátum, tanúsítvány tartalom ellenőrzés, zárt hálózati működés, preferált időbélyeg szerver)

2. számú melléklet

A biztonságos felhasználás feltételei

Az alábbiakban összefoglaljuk azokat a kötelezően betartandó, a jelen tanúsítvány érvényességére kiható feltételeket, melyek hozzájárulnak az SDX Professional aláíró alkalmazás által kezelt aláírások biztonságához.

A feltételek nem a megvalósított aláíró alkalmazásra, hanem annak telepítésére, környezetére, illetve az alkalmazható Elektronikus Aláírási Szabályzatra vonatkoznak.

1. számú feltétel

Az SDX Professional aláíró alkalmazást olyan biztonságos aláírás-létrehozó eszköz felhasználása mellett alkalmazzák, mely szerepel a Nemzeti Hírközlési Hatóság BALE nyilvántartásában.

2. számú feltétel

Az SDX Professional aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláíró alkalmazást, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy **biztonságos területen** valósítsák meg.
/Az SDX alkalmazás az alkalmazási környezet komponenseinek integritását ellenőrizni tudja, egy beállítható komponens lista alapján. Mivel az SDX alkalmazás egy szoftver, ezért a futtató környezetnek kell biztosítania, hogy magát az SDX alkalmazást (teljes egészében) ne lehessen lecserélni./

3. számú feltétel

Az SDX Professional aláíró alkalmazást olyan Elektronikus Aláírási Szabályzattal együtt kell használni, amely az elektronikus aláírás során használt algoritmusokra és input formátumokra az alábbi követelményeket fogalmazza meg:

- aláíró algoritmus: **RSA** (legalább **1024** kulcsméret mellett).
- lenyomatoló algoritmus: **SHA-1**.
- aláírás formátum: **emsa-pkcs1-v1_5**,

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: EESSI Conformity Assessment Guidance - Part 4: Signature Creation Application and Procedures for Electronic Signature Verification

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
- SDX Professional 1.0 - Konfigurációmenedzsment eljárások
- Alkalmazások tervezése, fejlesztése - Minőségirányítási eljárás
- SDX Professional 1.0 - Funkcionális specifikáció
- SDX Professional 1.0 - Magas szintű terv
- SDX Professional 1.0 - Felhasználói kézikönyv
- SDX Professional 1.0 - Telepítési útmutató
- E-Group Magyarország Rt. Informatikai szabályzat v1.0
- Alkalmazások tesztelése - Minőségirányítási eljárás
- SDX Professional Functional Tests
- SDX Professional 1.0 - A vizsgálat kiterjedtsége
- SDX Professional 1.0 - A vizsgálat mélysége
- SDX Professional 1.0 - Sebezhetőség vizsgálat

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

- Értékelési jelentés a Signed Document eXpert (SDX) professional 1.0 elektronikus aláíró alkalmazásról

A követelményeknek való megfelelést ellenőrző független vizsgálat módszere

A jelen tanúsításhoz figyelembe vett, a fejlesztőktől független értékelés garancia szintje az ISO 14508 /Common Criteria/ **EAL 3**-as szintjéhez hasonló volt. /Az EAL3 a fejlesztőktől függetlenül garantált biztonság közepes szintjét biztosítja./

A fejlesztőktől független értékelés összefoglalásaként egy értékelési jelentés készült.
Az ebben megfogalmazott és dokumentált eredményekre épül az a tanúsítási jelentés, mely jelen tanúsítvány alapját képezi.

Az értékelés az alábbi garanciaosztályokra terjedt ki:
- konfiguráció menedzselés
- kiszállítás és működtetés
- fejlesztés
- útmutató dokumentumok
- életciklus támogatás
- tesztek
- sebezhetőség felmérése

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