TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005. (VII. 21.) IHM rendelet alapján, mint a Magyar Köztársaság Informatikai és Hírközlési Miniszter 002/2006 számú kijelölési okiratával kijelölt tanúsító szervezet

tanúsítja,

hogy az

SDA Stúdió Kft.
által kifejlesztett

XadesMagic
elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz V1.0

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 létrehozására és ellenőrzésére alkalmazható szabványos és biztonságos alkalmazások fejlesztéséhez.

Jelen tanúsítvány a HUNG-TJ-034-2006. számú tanúsítási jelentés alapján került kiadásra. Készült az SDA Sútdió Kft.. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-034-2006.**
A tanúsítás kelte: 2006. november 20.
A tanúsítvány érvényességi ideje: 2009. november 20.
Melléklet: tulajdonságok, feltételek, követelmények, egyéb jellemzők összesen 6 oldalon.

PH.

Endrődi Zsolt	dr. Szabó István
Tanúsítási igazgató	Ügyvezető igazgató

1. számú melléklet

A XadesMagic v1.0 legfontosabb tulajdonságainak összefoglalása

Az értékelés tárgya egy olyan fejlesztő készlet, melynek segítségével szabványos (X.509 szabványon alapuló) nyilvános kulcsú szolgáltatásokat biztosító alkalmazások fejleszthetők. A fejlesztő készlet által támogatott nyilvános kulcsú szolgáltatások az alábbiak:

- Fokozott biztonságú elektronikus aláírás létrehozása a Crypto API által támogatott algoritmus paraméterekkel, Windows tanúsítványtárban vagy kriptográfiai hardver eszközben tárolt magánkulcs használatával.
- Elektronikus aláírás ellenőrzése, a kapcsolódó tanúsítvány útvonal felépítési és érvényesítési szolgáltatásokkal.
- Aláírás létrehozáshoz lenyomat készítése SHA-1, SHA-256, SHA-384, SHA-512, Ripemd-160 algoritmusokkal.
- Időbélyeg kérése és ellenőrzése.
- Visszavonási információ kérése és ellenőrzése (CRL, OCSP).

Ennek alapján a XadesMagic v1.0 fejlesztői készlet segítségével olyan alkalmazások fejleszthetők, melyek a nyilvános kulcsú technológia alapján bizalmasságot, sértetlenséget, hitelesítést és letagadhatatlanságot biztosító szolgáltatásokat képesek nyújtani.

A XadesMagic v1.0 fejlesztői függvénykönyvtár az alábbi nyilvános kulcs szolgáltatásokkal rendelkezik:

- biztonságosan kezel kulcsokat, megbízható pontokat és tanúsítványokat;
- elfogad és feldolgoz X.509 v3 nyilvános kulcs tanúsítványokat;
- képes a szükséges tanúsítványok és visszavonási adatok megszerzésére (a tanúsítványban szereplő CDP kiterjesztésben meghatározott helyről);
- ellenőrzi minden tanúsítvány érvényességét, az X.509 szabványban [ISO 9594-8] leírt eljárások felhasználásával, beleértve a visszavonás ellenőrzését is;
- hozzáfér pontos és megbízható időforráshoz a tanúsítványok, visszavonási adatok és alkalmazási adatok dátumának, idejének ellenőrzése érdekében;
- beszerzi, tárolja (beágyazza az aláírás struktúrába) a digitális aláírás jövőbeni ellenőrzéséhez szükséges adatokat;
- támogatja a Melasz-Ready XAdES elektronikus aláírás formátumot.

2. számú melléklet

A biztonságos felhasználás feltételei

Feltételezések a XadesMagic v1.0 informatikai környezetére

Az alábbi (a biztonsági előirányzatban is szereplő) feltételezések az informatikai környezetre vonatkoznak:

1. Az engedéllyel rendelkező felhasználók megbízhatók a tekintetben, hogy a számukra kijelölt funkciókat megfelelően hajtják végre (AE.Authorized_Users)
2. A XadesMagic v1.0 fejlesztő készletet megfelelően telepítik és konfigurálják. (AE.Configuration)
3. A XadesMagic v1.0 környezete tartalmaz egy megbízható kriptográfiai modult (CryptoAPI), mely modul a kriptográfiai műveleteket hajtja végre. (AE.Crypto_Module)
4. A XadesMagic v1.0 környezete fizikailag megvédi a XadesMagic v1.0–t a jogosulatlan fizikai hozzáféréssel szemben. (AE.Physical_Protection)
5. A tanúsítvány és tanúsítvány visszavonási információk a XadesMagic v1.0 rendelkezésére állnak. (AE.PKI_Info)
6. A XadesMagic v1.0 környezete GMT formában és a megkívánt pontossággal gondoskodik a pontos rendszeridőről. (AE.Time)
7. A XadesMagic v1.0 környezete biztosítja az időbélyegzés szolgáltatóhoz való hozzáférést. (AE.TimeStamp)

A biztonságos felhasználás egyéb feltételei

1. A XadesMagic v1.0 fejlesztő készlettel létrehozott aláíró alkalmazás csak olyan aláírási szabályzat szerint működhet, amely legfeljebb az alábbi X509v3 tanúsítvány kiterjesztéseket használja fel:
    - ExtendedKeyUsage
    - KeyUsage
    - BasicConstraints
    - CRLDistributionPoints
    - SubjectAlternativeName
    - IssuerAlternativeName
2. A XadesMagic v1.0 fejlesztő készlettel létrehozott aláíró alkalmazáshoz olyan CSP driver-t kell alkalmazni, amely képes megőrizni az aláírandó adat reprezentáns (DTBSR) és valamennyi protokoll adat sértetlenségét.
3. A XadesMagic v1.0 fejlesztő készlettel létrehozott aláíró alkalmazáshoz vagy olyan CSP driver-t kell alkalmazni, amely képes megőrizni az aláírót hitelesítő adatok bizalmasságát, vagy az aláíró alkalmazást olyan védett környezetben kell használni, ahol menedzsment, üzemeltetési és műszaki intézkedések garantálják az aláírót hitelesítő adatok bizalmasságát.
4. A XadesMagic v1.0 fejlesztő készletet használó aláíró alkalmazás működtetési környezetében menedzsment, üzemeltetési és műszaki intézkedésekkel biztosítani kell, 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.

5. A XadesMagic v1.0 fejlesztő készletet használó aláíró alkalmazáshoz:
    a. vagy olyan CSP driver-t kell alkalmazni, amely képes egy időkorlátot megadni arra az időtartamra, ami az aláírót hitelesítő adatok megadásától az aláírás kiváltásáig eltelhet,
    b. vagy az alkalmazásnak kell biztosítania az elvárást azáltal, hogy az aláírás kiváltása után kéri be a hitelesítő adatot.
6. A XadesMagic v1.0 fejlesztő készletet használó aláíró alkalmazáshoz:
    a. vagy olyan CSP driver-t kell alkalmazni, amely képes egy időkorlát letelte után az aláírási folyamatot félbeszakítani, az aláírót hitelesítő adatok újra megadását megkövetelve a folyamatot újrakezdeni, és az újraindítás szükségességéről az aláírót tájékoztatni,
    b. vagy az alkalmazásnak kell biztosítania az elvárást azáltal, hogy az aláírás kiváltása után kéri be a hitelesítő adatot.
7. A XadesMagic v1.0 működtetési környezetében menedzsment, üzemeltetési és műszaki intézkedéseket kell tenni az alábbiak biztosítására:
    a. vírusok ne ronthassák el az aláíró alkalmazást és az általa meghívott egyéb aláíró összetevőket, valamint
    b. az esetlegesen vírussal fertőzött aláíró összetevőket megfelelően helyre lehessen állítani.
8. A XadesMagic v1.0 működtetési környezetében menedzsment, üzemeltetési és műszaki intézkedésekkel kell megvédeni a XadesMagic v1.0 funkcionális összetevőinek sértetlenségét, megakadályozva, hogy behatolók elrontsák ezt.
9. A XadesMagic v1.0 működtetési környezetében menedzsment, üzemeltetési és műszaki intézkedésekkel biztosítani kell, hogy magát a XadesMagic v1.0-t, valamint az aláírás-létrehozás és aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összes összetevőt egy biztonságos területen valósítsák meg.

3. számú melléklet

Termékmegfelelőségi követelmények

Követelményeket és szabványokat tartalmazó dokumentumok

Követelmények

Az elektronikus aláírásról szóló 2001. Évi XXXV. törvény

CEN CWA 14170:2004 munkacsoport egyezmény: Security Requirements fro Signature Creation System

CEN CWA 14171:2004 munkacsoport egyezmény: General guidelines for electronic signature verification

CEN CWA 14172-4:2001 munkacsoport egyezmény: Signature-creation application and general gudelines for electronic signature verification

ETSI SR 102 176-1 v1.2.1 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms

ETSI TS 101 733 v1.6.3 CMS Advanced Electronic Signatures (CAdES)

ETSI TS 101 903 v1.2.2 XML Advanced Electronic Signatures (XAdES)

Szabványok

RSA	Rivest-Shamir-Adleman (public key cryptosystem) /ANSI X9.31/
SHA-1	Secure Hash Algorithm /FIPS PUB 180-1/
RFC 2560:	PKIX - Online Certificate Status Protocol – OCSP
RFC3161	Time-Stamp Protocol (TSP)
RFC3275	XML Digital Signatures (XMLDSig)
RFC3280	Certificate and Certificate Revocation List (CRL) Profile
PKCS#1	RSA Cryptographic Standard /RFC2313/

4. számú melléklet

A tanúsítási eljárás egyéb jellemzői

A tanúsításhoz figyelembe vett, fejlesztői dokumentumok

- Biztonsági előirányzat v1.0
- Funkcionális specifikáció v1.0
- Magas szintű terv v1.0
- Megfeleltetés elemzések v1.0
- Adminisztrátori útmutató v1.0
- Tesztelési dokumentáció 2006.09.26.
- Teszt lefedettség elemzés v1.0
- Teszt mélység elemzés v1.0
- A konfiguráció menedzselés dokumentációja v1.0
- A fejlesztési biztonság dokumentációja v1.0
- Fejlesztői sebezhetőség elemzés v1.0
- A tesztelésre alkalmas értékelés tárgya (az SDA.E-Magic program segítségével tesztelhető fejlesztő készlet)

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

Értékelési jelentés a XadesMagic v1.0 XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz 1.0 (Készítette HunGuard Kft.)

A követelményeknek való megfelelést ellenőrző független vizsgálat módszere

A XadesMagic v1.0 fejlesztő készlet a CEM (Common Evaluation Methodology) v2.3 módszertana szerint került független értékelésre és tanúsításra.

Az értékelés garanciaszintje

EAL3

Az értékeléshez felhasznált módszertani anyagok

- MSZ/ISO/IEC 15408:2003 Informatika – Biztonságtechnika - Az informatikai biztonságértékelés közös szempontjai
- Common Criteria for Information Technology Security Evaluation (CC) Part 1: Introduction and general model - Version 2.3, August 2005
- Common Criteria for Information Technology Security Evaluation (CC) Part 2: Security functional requirements - Version 2.3, August 2005
- Common Criteria for Information Technology Security Evaluation (CC) Part 3: Security assurance requirements - Version 2.3, August 2005
- Common Methodology for Information Security Evaluation (CEM), Version 2.3, August 2005