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
Noreg Kft.
által kifejlesztett és forgalmazott

e-Sealer

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

létrehozására

Jelen tanúsítvány a HUNG-TJ-020-2004. számú tanúsítási jelentés alapján került kiadásra.
Készült a Noreg Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-020/2004.**
A tanúsítás kelte: 2004. május 10.
A tanúsítvány érvényességi ideje: 2007. május 10.
Mellékletek: tulajdonságok, feltételek, követelmények, egyéb jellemzők, összesen 7 oldalon.

PH.

Tanúsítási igazgató: Ügyvezető igazgató

1. számú melléklet

Az e-Sealer v1.0 legfontosabb tulajdonságainak összefoglalása

Az e-Sealer v1.0 speciális kiterjesztésű, tetszőleges tartalmú fájlok elektronikus aláírására szolgál. Két programból, egy adminisztrátori és egy aláírói alkalmazásból áll.

Az e-Sealer v1.0 digitális aláírással és annak automatikus ellenőrzésével kapcsolatos biztonsági funkciókat lát el Windows 2000, illetve XP operációs rendszer alapú célkörnyezetben.

Az aláírói alkalmazás egy megadott forráskönyvtárban (és annak alkönyvtáraiban) az aláírási funkció felhasználói interfésze elindításakor található valamennyi fájlt egyenként (az aláírási szabályzatban meghatározott szabályoknak megfelelően) digitálisan aláír, s az így előálló fájlokat egy megadott célkönyvtárba helyezi el (automatikusan ellenőrizve is az aláírásokat). Az alkalmazás szabványos formátumú (PKCS#7) minősített elektronikus aláírást hoz létre.

A célkönyvtár a forrás könyvtáréval hasonló fa szerkezetű lesz, ha valamelyik alkönyvtár hiányzik, akkor a program ezt automatikusan létrehozza.

A célkönyvtárban elhelyezett eredmény fájl neve (kiterjesztéssel együtt) ugyanaz lesz, mint az eredeti fájlé volt, csak a név második kiterjesztésként kiegészül a "sig" karakterhármassal, amennyiben a felhasználó „separate signature”-t nem kapcsolta be. Ez utóbbi esetben külön fájlként kerül a célkönyvtárba az aláírás.

A feldolgozás (elektronikus aláírás, a forráskönyvtárból a célkönyvtárba helyezéssel együtt) automatikusan történik, feldolgozás közben a feldolgozottság szintje folyamatosan követhető az aktuális feldolgozás alatt álló fájl nevének, valamint a feldolgozottság százalékos arányának a megjelenítésével.

A feldolgozás eredményéről riport készül, mely tartalmazza az alábbiakat:

- a feldolgozásra átadott fájlok száma,
- a sikeresen feldolgozott fájlok száma,
- a (valamilyen okból) nem feldolgozott fájlok száma,
- a forrás könyvtárban (s annak alkönyvtáraiban) található fájlok száma.

Az adminisztrátori alkalmazás segítségével az aláíró alkalmazás biztonsági tulajdonságainak kritikus részét (a megbízható pontokkal kapcsolatos adatokat) lehet felvinni, módosítani, illetve törölni, megfelelő (adminisztrátori) jogosultsággal.

Az e-Sealer v1.0 az alábbi biztonsági funkciókat valósítja meg:

- Azonosítás és hitelesítés
  Az e-Sealer v1.0 az aláírás létrehozási tevékenység előtt felhasználó hitelesítési kérelmet jelenít meg a felhasználói felületen (PIN kód bekérés), a hitelesítő adatot továbbítja a BALE felé.
- Hozzáférés ellenőrzés
  Az e-Sealer v1.0 csak az általa elért könyvtárban található állományokra végzi el az aláírás létrehozási és az automatikus aláírás ellenőrzési folyamatot.
- Naplózás
  Az alkalmazás szempontjából fontosnak ítélt napló események előállítását végző funkció.
  /A naplózási követelmények döntő részét az e-Sealer v1.0 környezete teljesíti: az operációs rendszer naplózza az alkalmazás jogos felhasználóinak bejelentkezésével kapcsolatos események bejegyzését, s a napló adatok megtekintését is (a környezethez tartozó) külön alkalmazás teszi lehetővé. A saját maga által generált naplóállományok védelmét annyiban vállalja fel az e-Sealer v1.0, hogy az elkészült napló-riport állományokat lezárás után „csak olvasható” attribútummal látja el, mely a véletlen törlés ellen véd./
- Aláírás létrehozási funkció (az egyik alapvető biztonsági funkció)
  Az aláíró magánkulcsot használja az aláírás generálására, és lehetővé teszi az aláírási információk generálását is. Az aláírás létrehozásával a sértetlenség, hitelesség és letagadhatatlanság biztonsági szolgáltatásokat valósítja meg az e-Sealer v1.0. Opcionálisan időbélyeg is kérhető.
- Aláírás ellenőrzési funkció (a másik alapvető biztonsági funkció)
  Ez dolgozza fel az aláírási információkat, például a PKCS#7 blob-ot, és a nyilvános kulcsot használja az aláírás ellenőrzéséhez. Ez a funkció-csomag függ a tanúsítási útvonal érvényességének ellenőrzése biztonsági funkciótól. Az aláírás ellenőrzési funkció a tanúsítási útvonal érvényesség ellenőrzés eredményét bemenetként használja fel.
- Tanúsítási útvonal érvényesség ellenőrzése
  Ez a funkció a tanúsítási útvonal érvényességét ellenőrzi. A megvalósítás az útvonal felépítéséből, majd a tanúsítási útvonal érvényességének ellenőrzéséből áll. A tanúsítási útvonal érvényességének ellenőrzése a tanúsítványok érvényességének ellenőrzéséből áll, oly módon, hogy ez az ellenőrzés egy megbízható pont által tanúsítottal kezdődik, és az aláírónak kibocsátottal fejeződik be.
  A tanúsítási útvonal érvényesség ellenőrzése az aktuális idő szerint történik (szemben például a vitás esetekben felmerülő régi aláírások ellenőrzésével).
- CRL érvényesség ellenőrzése funkció
  Ez a funkció a CRL érvényességének ellenőrzésére szolgál. Olyan teljes CRL feldolgozására használható, amelyre egy CRL szétosztó pont kiterjesztés mutat egy tanúsítványban.
- Aláírandó fájlok listájának megjelenítése
  Az aláírás létrehozási funkció aktivizálásakor megjelenő hitelesítő ablakban látható gomb (Show files) megnyomása után az aláírásra összeállított fájlok listáját mutatja be a felhasználónak. A könyvtár időközbeni módosítását figyelmen kívül hagyja ezen aláírás létrehozási szakaszban.

2. számú melléklet

A biztonságos felhasználás feltételei

Az alábbiakban összefoglaljuk azokat a kötelezően betartandó, a jelen tanúsítvány érvényességére kiható feltételeket, melyek hozzájárulnak az e-Sealer v1.0 aláíró alkalmazás által kezelt aláírások biztonságához.

A feltételek nem a megvalósított aláíró alkalmazásra, hanem annak telepítésére, környezetére és működtetésére vonatkoznak.

1. számú feltétel
Az e-Sealer v1.0 aláíró alkalmazást olyan biztonságos aláírás-létrehozó eszköz felhasználása mellett alkalmazzák, mely szerepel a Nemzeti Hírközlési Hatóság BALE nyilvántartásában.

2. számú feltétel
Az e-Sealer v1.0 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.
/Mivel az e-Sealer v1.0 aláíró alkalmazás egy szoftver, ezért a futtató környezetnek kell biztosítania, hogy magát az e-Sealer v1.0 alkalmazást ne lehessen lecserélni./

3. számú feltétel
Az aláírási szabályzat által engedélyezett .pdf és .xml fájlok megjelenítéséhez olyan megjelenítő összetevőt kell használni (az operációs rendszerben az alapértelmezett megjelenítő kijelölésével), amely nem engedi megváltoztatni az aláírandó dokumentumot (tehát csak nézegetőt szabad alapértelmezett megjelenítőként telepíteni a gazdagépre, szerkesztőt nem).

4. számú feltétel
Az e-Sealer v1.0 adminisztrátora jól képzett, megbízható és betartja az "e-Sealer v1.0 Adminisztrátori kézikönyv" által leírt, a biztonságos telepítésre és adminisztrálásra vonatkozó kötelező tevékenységeket.

5. számú feltétel
Az e-Sealer v1.0 felhasználói jól képzettek, megbízhatóak és betartják az "e-Sealer v1.0 Használati útmutató" által leírt, a biztonságos használatra vonatkozó kötelező tevékenységeket.

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

Szabványok

PKCS #7	Cryptographic Message Syntax Standard /version 1.5, November 1993/
PKCS #11	Cryptographic Token Interface Standard /version 2.10, December 1999/
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
- Az e-Sealer v1.0 elektronikus aláíró program **biztonsági előirányzat**a v1.2
- Erste Bank Hungary Rt. - Elektronikus egyenleg aláíró program - Elektronikus **aláírási szabályzat**a v1.0
- **Konfigurációmenedzselési terv**, e-Sealer 1.0
- Összefoglaló az 1. **helyszíni szemlé**n végzett interjúról
- e-Sealer v1.0 **Adminisztrátori kézikönyv**
- e-Sealer v1.0 **Használati útmutató**
- Technikai specifikáció az Erste Bank Rt. részére fejlesztendő elektronikus egyenleg aláíró program server-oldali moduljára (**Funkcionális specifikáció**) v1.0
- Az e-Sealer V1.0 aláíró alkalmazás alrendszerei, biztonsági funkciói és mechanizmusai (**magas szintű terv**) v1.3
- Erste Bank, Elektronikus egyenleg aláíró program, **Fejlesztői teszt terv** v1.0
- Erste Bank, Elektronikus egyenleg aláíró program, **Fejlesztői tesztelés eredménye** v1.01

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

- **Értékelési jelentés** az e-Sealer v1.0 elektronikus aláíró programról
- e-Sealer V1.0, A fejlesztői tesztelés **lefedettségi elemzés**e v1.1
- e-Sealer V1.0, A fejlesztői tesztelés **mélységi elemzés**e v1.0
- ERSTE Bank, Elektronikus egyenleg aláíró program, e-Sealer V1.0, **Sebezhetőségi elemzés** v1.0
- **Telephely látogatás** Jegyzőkönyve
- **Független Tesztelés** Jegyzőkönyve
- 2. számú **Független Tesztelés** Jegyzőkönyve
- e-Sealer V1.0, Az **áthatolás tesztelés** eredménye

A követelményeknek való megfelelést ellenőrző független vizsgálat módszere

A jelen tanúsításhoz figyelembe vett, a fejlesztőktől független értékelés az informatikai termékek technológia szempontú értékelésére szolgáló, kialakítás alatt álló nemzeti séma, a **Magyar Informatikai Biztonsági és Értékelési Séma** /MIBÉTS/ módszertanát követte.
Ennek a fejlesztőktől független értékelés garancia szintje az ISO 15408 /Common Criteria/ **EAL 3**-as szintjéhez hasonló volt. /megfelelt a MIBÉT Séma **fokozott értékelési garanciaszint**jének, mely a fejlesztőktől függetlenül garantált biztonság közepes szintjét biztosítja./

A fejlesztőktől független értékelés összefoglalásaként egy értékelési jelentés készült.

Az értékelési jelentésnek a fő megállapításai az alábbiak voltak:

Az értékelés tárgya, az e-Sealer v1.0 elektronikus aláíró program, megfelel biztonsági előirányzatának (kielégíti az "e-Sealer v1.0 elektronikus aláíró program biztonsági előirányzata, verzió 1.2, 2004-04-05" dokumentumban megfogalmazott funkcionális és garanciális biztonsági követelményeket).

Az értékelés tárgya, az e-Sealer v1.0 elektronikus aláíró program, megfelel aláírási szabályzatának (kielégíti az "Erste Bank Hungary Rt. - Elektronikus egyenleg aláíró program - Elektronikus aláírási szabályzata - verzió 1.0, 2004-04-30" dokumentumban megfogalmazott szabályokat és elvárásokat).

Az értékelés tárgya, az e-Sealer v1.0 elektronikus aláíró program, megfelel a minősített aláírások létrehozását és ellenőrzését végző alkalmazásokra vonatkozó (CEN/ISSS CWA 14170 és CEN/ISSS CWA 14171 dokumentumokban meghatározott) **mértékadó funkcionális és biztonsági követelményeknek.**

Az e-Sealer v1.0 biztonsági funkciónak megvalósításában jelentős szerepet játszó **beépített függvények** /Utimaco SafeGuard Toolkit, vizsgált API verziószám: UMB/CW/V02.50.02/W (Feb 9 2004 / 15:56:42)/ **helyesen, a leírásuknak megfelelően működnek**.

Az értékelési jelentésben 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.