TANÚSÍTVÁNY (E-MS03T_TAN.SW) MELLÉKLETE

Dokumentumazonosító:	**TAN.SW.ME-01**	
Projektazonosító:	**E-MS03T**	**Microsec Kft. 2003**
MATRIX tanúsítási igazgató:	**Dr. Szőke Sándor**	
MATRIX tanúsító:	**Gyányi Sándor** **Hornyák Gábor**	
Kelt:	Budapest, 2004. október 12.	
……. MATRIX tanúsítási igazgató	……. MATRIX tanúsító részéről	

1. A TANÚSÍTÁS KÖRÜLMÉNYEI

A Microsec az MSZ ISO/IEC 15408 (Az informatikai biztonság értékelésének közös szempontrendszere) alapján kifejlesztette a „Biztonsági Specifikáció Minősített elektronikus aláírás létrehozó és kezelő alkalmazáshoz” dokumentumot, majd erre alapozva az ennek megfelelő „Biztonsági Előirányzat Minősített elektronikus aláírás létrehozó és kezelő alkalmazáshoz” dokumentumot. A MATRIX a dokumentumok bevizsgálása után Tanúsítványokat állított ki (azonosító: PP-MS-03/001 illetve ST-MS-03/001)), amelyekben igazolta a megfelelést az alábbi normatíváknak:

Kötelező érvényű normatívák:

- 2001. évi XXXV. törvény Az elektronikus aláírásról
- 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

A fejlesztő önként vállalt normatívái:

- MSZ ISO/IEC 15408: Az informatikai biztonság értékelésének közös szempontrendszere
  - 15408-1: 1. rész: Bevezetés és általános modell
  - 15408-2: 2. rész: A biztonság funkcionális követelményei
  - 15408-2: 3. rész: A biztonság garanciális követelményei

- EU Directive 1999/93/EC of the European Parliament and the council of 13 December 1999 on a Community framework for electronic signatures;
- CWA 14170 – Security Requirements for Signature Creation Applications
- CWA 14171 – Procedures for Electronic Signature Verification
- A Miniszterelnöki Hivatalt vezető miniszter 2/2002. (IV. 26.) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről

A Microsec a Biztonsági Előirányzat alapján kifejlesztette az e-Szignó 2.0 minősített aláírás létrehozó és kezelő alkalmazást, és annak részeként a vizsgálat tárgyát képező XmlSigner.dll aláírást létrehozó modult. Részletes tesztelést hajtott végre, a tesztekről jegyzőkönyvet készített. A Tesztjegyzőkönyv célja annak bizonyítása, hogy az e-Szignó megfelel a Biztonsági Előirányzatban (továbbiakban: BE) meghatározott követelményeknek. Ennek érdekében a teszteket a BE-ben azonosított követelmények szerinti csoportosításban végezte el.

A tanúsítási folyamat során ellenőrzésképpen elvégeztük a teszt jegyzőkönyvben leírt valamennyi tesztet, s azt vizsgáltuk, hogy az átadott eszközök és dokumentumok alapján az e-Szignó program magját képező aláírás létrehozó modul maradéktalanul megfelel-e a Biztonsági Előirányzatban megfogalmazott célkitűzéseknek, s így közvetve az annak alapját képező fentebb felsorolt normatíváknak.

2. A VIZSGÁLAT TÁRGYA

2.1. A tanúsításhoz a gyártó által átadott eszközök és dokumentációk

Megnevezés: „XmlSigner.dll megbízható aláírás létrehozó modul"

Típus	Tárgy	Verzió	Dátum	Adat-hordozó
Szoftver	XmlSigner.dll	2.0.0.437	2004.09.22.	CD
Hardver	GemPC 410 kártyaolvasó		2004.09.22.	-
Hardver	GemSafe GPK16k chipkártya		2004.09.22.	-
Dokumentáció	Tesztjegyzőkönyv az XmlSigner.dll megbízható aláírás létrehozó modulhoz		2004.09.22.	CD + papír
Dokumentáció	Nyilatkozat		2004.08.03.	Papír

Fejlesztő:

Microsec Számítástechnikai Fejlesztő Kft.
1022 Budapest,
Marczibányi tér 9.

3. FUNKCIONÁLIS LEÍRÁS

A Microsec e-Szignó minősített aláírás létrehozó és kezelő alkalmazás biztosítja az elektronikus ügyvitelben az elektronikus dokumentumok kezeléséhez szükséges funkciókat, amelyek:

- *elektronikus akták létrehozása,*
- *elektronikus dokumentumok beillesztése,*
- *elektronikus dokumentumok aláírása,*
- *az e-akta, a dokumentumok és az aláírások leíró adatokkal való ellátás,*
- *sértetlenség és hitelesség ellenőrzése,*
- *nyugtázás*.

Az elektronikus dokumentumokat és a leíró adataikat az e-Szignó *elektronikus aktákban* (e-aktákban) fogja össze.

Az e-Szignó tipikus felhasználása, hogy az egyes, e-Szignóval rendelkező munkaállomások a számítógépes hálózaton keresztül kapcsolódnak az ügyviteli hálózat többi munkaállomásához, valamint annak központi szerveréhez. A számítógépes hálózat tagjai egymás között elektronikus levelekkel kommunikálnak. Az összeállított, elektronikus dokumentumokat tartalmazó e-aktákat elektronikus levelek csatolt állományaiként továbbítják az ügyvitel résztvevői, amelyeket elektronikus tértivevényekkel nyugtázhatnak.

Az e-Szignó által létrehozott állományok formátuma megfelel az RFC 3275 (XMLSignature) ajánlásnak, lehetővé téve a tartalmazott elektronikus dokumentumok egy vagy több elektronikus aláírással történő ellátását. Az elektronikus aláírások biztosítják az elektronikus dokumentumok hitelességét, valamint az ügyintézők azonosíthatóságát, azaz utólag is megállapítható, hogy ki, mikor és milyen tartalommal láttamozott egy dokumentumot. Egy dokumentum elektronikus aláírása rögzíti a dokumentum pillanatnyi állapotát és az aláírás ellenőrzésekor felfedhetővé tesz bármiféle utólagos módosítást, egyúttal biztosítva az aláírás letagadhatatlanságát is. Az elektronikus aláírás elkészítése egy személyhez rendelt chipkártya (smartcard) és a VT segítségével történik.

Az e-Szignó 2.0 minősített aláírás létrehozó és kezelő alkalmazás két fő komponensből áll: az Aláírás létrehozásához szükséges műveleteket végrehajtó *Megbízható aláírás-létrehozó modulból* (XmlSigner.dll) és az aláírással kapcsolatos műveleteket a felhasználó számára elérhetővé tevő *Felhasználói felületből* (EsignoNav.exe).

A jelen vizsgálat tárgyát konkrétan képező *XmlSigner.dll* megbízható *Aláírás-létrehozó modul* biztosítja az összes funkciót, amely az Aláírás megbízható módon történő létrehozásához szükséges. Az Aláírás-létrehozás folyamatát elemi műveletként teszi elérhetővé a Felhasználói felület számára.

Az XmlSigner garantálja, hogy kívülről elérhető műveleteinekre – tetszőleges szekvenciában történő használata esetén is – teljesülnek a következők:

1. Egy e-akta megnyitása és lezárása között kizárólag az XmlSigner fér hozzá az e-aktához.

2. Az e-akta formátuma mindvégig megfelel az RFC3275-ben definiált XMLSignature formátumnak.

3. Aláírás kizárólag az Aláíró tudtával és jóváhagyásával készül, pontosan az általa jóváhagyott Aláírói dokumentumon és Aláírás-jellemzőkön.

4. Az e-akta formátuma mindvégig megfelel az e-Szignó e-akta formátumnak.

5. Az Aláírásokhoz és Aláírói dokumentumokhoz kapcsolódó leíró adatok közül csak az arra külön kijelöltek módosíthatóak (a biztonsági szempontból jelentősek nem módosíthatóak) az XmlSigner által.

6. A Profilok adatainak módosítása az e-akta lezárását követően kimutatható az e-akta lezárásakor, az Aláíró által elhelyezett aláírásnak köszönhetően.

Az XmlSigner az aláírási folyamat részeként a következő funkciókat végzi:

- az Aláírandó dokumentum megjelenítése,
- az Aláírás-jellemzők meghatározása,
- az Aláírás-jellemzők megjelenítése,
- az Aláírói Tanúsítvány megjelenítése,
- az Aláírói Tanúsítvány érvényességének ellenőrzése,
- a Formázott aláírandó adathalmaz elkészítése,
- az Aláírandó adathalmaz lenyomatának elkészíttetése,
- az Aláírás elkészíttetése,
- az Aláírt adathalmaz összeállítása.

Maga a Minősített elektronikus aláírás létrehozása egy *Biztonságos Aláírást Előállító Eszköz* (BALE) segítségével történik. A BALE irányába történő adatküldés illetve a BALE irányából érkező adatok fogadása a Microsoft Windows operációs rendszer részeként szállított Microsoft Crypto API csatolón keresztül történik.

Az Időpecsét elkészítéséhez illetve a Tanúsítvány Hitelesítés-szolgáltatóval történő ellenőriztetéséhez az összeállított kérést az XmlSigner az Interneten keresztül, HTTPS kapcsolat létesítésével juttatja el a Hitelesítés-szolgáltatóhoz illetve Időbélyegző szolgáltatóhoz, amelyhez a *wininet.dll* modul segítségével valósul meg.

A Dokumentumok – Aláírás létrehozás során szükséges – formátumoktól függő megjelenítése néhány kiválasztott megjelenítőprogram segítségével történik.

A VT a következő külső hardver komponensek jelenlétét igényli:

- Aláírás-létrehozó adatok használatához:

  - BALE

- Tanúsítványok beszerzéséhez; a Tanúsítványok visszavonási állapotáról szóló információk beszerzéséhez; a Tanúsítvány-ellenőr szolgáltatás igénybevételéhez; Időpecsét készítéshez:

  - TCP/IP hálózati összeköttetés a Hitelesítés-szolgáltató illetve az Időbélyegző szolgáltató eléréséhez.

A VT a következő szoftver komponensek jelenlétét igényli:

- Aláírói dokumentumok megjelenítéséhez, Tanúsítványok megjelenítéséhez, egyéb

alap illetve kriptográfiai rendszerfunkció ellátásához:

- Windows XP (vagy azzal kompatibilis Windows verzió)
- MS Word
- Adobe Acrobat Reader

4. MEGFELELŐSÉG A NORMATÍV DOKUMENTUMOK ALAPJÁN

4.1. Megfelelőség

Az "XmlSigner.dll megbízható aláírás létrehozó modul" megfelel az alábbi követelményeknek:

- 2001 évi XXXV. törvény Az elektronikus aláírásról
- 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- MSZ ISO/IEC 15408:Az informatikai biztonság értékelésének közös szempontrendszere
    - 15408-1: 1. rész: Bevezetés és általános modell
    - 15408-2: 2. rész: A biztonság funkcionális követelményei
    - 15408-3: 3. rész: A biztonság garanciális követelményei
- EU Directive 1999/93/EC of the European Parliament and the council of 13 December 1999 on a Community framework for electronic signatures;
- CWA 14170 – Security Requirements for Signature Creation Applications
- CWA 14171 – Procedures for Electronic Signature Verification
- A Miniszterelnöki Hivatalt vezető miniszter 2/2002. (IV. 26.) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről
- ST-MS-03/001 azonosító jelű Biztonsági Előirányzat (v6.0)

Az aláírás létrehozó modul megfelel a fenti követelményeknek a 4.2 pontban leírt működési környezetben az alábbi feltételek teljesülése mellett:

A tanúsítás kizárólag az XmlSigner.dll 2.0.0.437 verziószámú program modulra vonatkozik, bárminemű változtatás ismételt vizsgálatok és a tanúsítás megújítása nélkül nem engedélyezett (MD5 hash: 554ce9e66920306d191b1fc9e5633d98)

4.2. Működési környezet

A fenti megfelelőség feltétele az alábbi működési környezetre vonatkozó követelményrendszer teljesülése.

4.2.1. Hardver és szoftver környezet

A VT csak olyan környezetben használható minősített aláírások létrehozására, amelynek minden eleme kielégíti az alapvető biztonsági követelményeket, és együttesen egy megfelelően biztonságos informatikai rendszert hoznak létre. A vizsgálatnak nem tárgya a környezet egyes elemeinek vizsgálata, az itt megfogalmazott követelmények iránymutató jellegűek az eszköz megfelelő használatához.

4.2.1.1. Operációs rendszer

A VT Windows XP Professional operációs rendszeren fut, az alapfunkciók mellett az operációs rendszer részét képező Crypto API végzi a kriptográfiai műveleteket. A VT biztonságos használatának előfeltétele, hogy az operációs rendszert megfelelően biztonságos konfigurációban használjuk. A Windows XP Professional jelenleg biztonsági tanúsítás alatt áll. A tanúsítás elkészülte után a rendszert a tanúsításban megfogalmazott feltételek betartásával kell üzemeltetni.

A fentiektől eltérő Windows operációs rendszer is használható, azonban használatának alapfeltétele, hogy az operációs rendszer protected módban fusson.

4.2.1.2. BALE eszköz

Az XmlSigner modul minősített aláírás létrehozására csak olyan biztonságos aláírás létrehozó eszközzel (BALE) használható, amely szerepel a Nemzeti Hírközlési Hatóság (NHH) vagy más Európai Uniós tagállam megfelelő hatósága által hivatalosan közzétett nyilvántartásában.

A BALE kiválasztása során különös figyelmet kell fordítani a BALE-t az operációs rendszer kriptográfiai szolgáltatásaihoz illesztő CSP modul megbízhatóságára. A BALE csak olyan CSP-vel használható, amelyet a BALE gyártója szállít, vagy amelynek fejlesztője garantálja a CSP biztonságos működését.

Az alkalmazott összeállításnak garantálnia kell a megfelelően biztonságos csatorna kialakítását a BALE és az aláíró alkalmazás között az aláírandó adatok átadásához.

Az alkalmazott összeállításnak garantálnia kell a megfelelően biztonságos útvonal kialakítását a BALE és az aláíró között az aláírás aktiváló adatok bevitelére és továbbítására a BALE felé.

Smartcard alkalmazás esetén előnyben kell részesíteni az olyan CSP használatát, amely a BALE-t képes Pinpad-dal rendelkező (Class 2) olvasóval használni, ezzel kizárva az esetleg hozzáférhető billentyűzet használatát.

4.2.1.3. Hálózati működés

Mivel az alkalmazás az ellátandó feladatok jellegéből adódóan nyilvános hálózatra kapcsolódik, kiemelt figyelmet kell fordítani az egész számítógép védelmére a hálózaton terjedő rosszindulatú programok támadásainak detektálása, kivédése érdekében.

4.2.2. Személyi védelem

Az üzemeltetés során a személyi védelem tekintetében az alábbi intézkedések betartásáról kell gondoskodni:

- Hozzáértő adminisztrátorokat és felhasználókat kell a VT és a VT által tartalmazott titkos adatok kezelésére alkalmazni.
- Az összes adminisztrátor és felhasználó magas szinten ismerje a biztonsági szabályzatot, amely szerint a VT működik.
- A hozzáférés megszüntetése (pl. a felhasználó munkaviszonya megszűnik) során megfelelő eljárások fussanak le a hozzáférés megszüntetése és egyéb jogosultsági komponensek eltávolítása érdekében.
- Az adminisztrátorokat és felhasználókat időben és megfelelő módon kell tájékoztatni azokról a biztonsági közleményekről, amelyekben leírják a VT üzemeltetését veszélyeztető tényezőket, így minimalizálva a bizalmas információk elvesztésének, illegális felhasználásának, illegális módosításának kockázatát.
- Az adminisztrátorokat és felhasználókat ki kell oktatni a szociális hírszerzés elleni védekezés módszereiről (pl. nem megbízhatóan hitelesített – telefonon érdeklődő – személyek felé adatszolgáltatás tiltása stb.).
- Az adminisztrátorok és felhasználók felvétele során ügyelni kell a megbízható személyek kiválasztására (pl. erkölcsi bizonyítvány stb.).

4.2.3. A fizikai védelem

Az üzemeltetés során a fizikai védelem tekintetében az alábbi intézkedések betartásáról kell gondoskodni:

- A VT által tartalmazott hardver, szoftver és firmware elemeket megfelelően kell védeni az illetéktelen fizikai módosítások ellen.
- A VT által használt kommunikációs csatornákat megfelelően védeni kell az illetéktelen fizikai módosítások ellen.
- A VT által használt kommunikációs csatornákat megfelelő módon védeni kell az illetéktelen lehallgatás ellen. Lehallgatás alatt logikai (pl. kémprogramok) és fizikai (EMC) módszerekkel végzett adatgyűjtés értendő.

4.2.4. Szállítás és telepítés

A program telepítő készletét nem módosítható, biztonságos adathordozón kell a felhasználónak átadni. Az átadás-átvételt hitelt érdemlő módon igazolni kell az átadás pontos időpontjának rögzítésével.

A telepítést csak a megfelelően előkészített, biztonságos környezetben szabad megkezdeni az átadott adathordozó segítségével, a telepítési útmutatóban rögzített lépések pontos betartásával.

Az adathordozó felhasználásával rendszeresen ellenőrizni kell a számítógépre telepített program integritását.

4.2.5. Felhasználói felület

Az XmlSigner.dll modul biztonságos üzemeltetéséhez a szoftver felhasználói felületének biztosítania kell a Biztonsági Előirányzatban rögzített körülményeket.

4.3. Algoritmusok és kapcsolódó paraméterek

Az aláírandó adathalmaz lenyomatának létrehozása (hash), a kitöltő adatok hozzáadása és az aláírás elvégzése a VT határain kívül történik, így az erre vonatkozó megfelelést nem kell igazolni.

4.4. Biztonsági szint

Az "XmlSigner.dll megbízható aláírás létrehozó modul" kiértékelése a CC előírásainak megfelelően a MATRIX ez irányú módszertan használatával sikeresen megtörtént a **Common Criteria EAL3** biztonsági szinten.

5. RÖVIDÍTÉSEK

CC MSZ ISO/IEC 15408 Az informatikai biztonság értékelésének közös szempontrendszere

EAT 2001. évi XXXV. törvény az elektronikus aláírásról

PP Protection Profile, Biztonsági Specifikáció

ST Security Target, Biztonsági Előirányzat

TOE Target Of Evaluation, a Vizsgálat Tárgya

Dokumentum vége