TANÚSÍTVÁNY (E-MS07T-TAN.SW) MELLÉKLETE

Dokumentumazonosító	TAN.SW.ME-01	
Projektazonosító	E-MS07T	Microsec Kft. 2007
MATRIX tanúsítási igazgató	Dr. Szőke Sándor	
MATRIX tanúsító	Hornyák Gábor	
Kelt	Budapest, 2007. december 6.	
…… MATRIX tanúsítási igazgató	…… MATRIX tanúsító részéről	

TARTALOMJEGYZÉK

1 A TANÚSÍTÁS KÖRÜLMÉNYEI

A MICROSEC Kft. 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 Kft. a dokumentumok bevizsgálása után Tanúsítványokat állított ki (azonosító: E-MS03T-TAN.PP illetve E-MS05T-TAN.ST), amelyekben igazolta a megfelelést az alábbi normatíváknak:

Kötelező érvényű normatívák:

- 2001. évi XXXV. törvény az elektronikus aláírásról,
- 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.

A fejlesztő önként vállalt normatívái:

- MSZ ISO/IEC 15408:2002. 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.
- Az Európai Parlament és a Tanács 1999/93/EK Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről,
- CWA 14170:2001 E – Security Requirements for Signature Creation Applications,
- CWA 14171:2001 E – 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,
- RFC 3275: XML-Signature Syntax and Processing,
- ETSI TS 101 903 V1.2.2 (2004-04): XML Advanced Electronic Signatures (XAdES).

A MICROSEC a Biztonsági Előirányzat alapján kifejlesztette az e-Szignó 3.0 minősített aláírás létrehozó és kezelő alkalmazást, és annak részeként a XadesSigner.dll 1.0.23.0 minősített aláírás létrehozó és ellenőrző modult. MATRIX a MICROSEC megrendelése alapján 2005-ben megvizsgálta az e-Szignó 3.0 alkalmazást, és annak részeként a

XadesSigner.dll modult. A tanúsítási eljárás eredményeképp 2005. július 29-én kiállításra került az E-MS05T_TAN.SW azonosítójú tanúsítvány és az E-MS05T_TAN.SW.ME-01 melléklet.

A jogi szabályozás változása miatt 2005. szeptemberben a MATRIX kezdeményezte a tanúsítási eljárás felülvizsgálatát, a szükséges módosítások elvégzését és az eredeti tanúsítvány visszavonása mellett egy új tanúsítvány kiadását. A felülvizsgálat eredményeképp 2005. október 12-én MATRIX kiállította a jelenleg is érvényben lévő E-MS05T_TAN.SW_1 azonosítójú tanúsítványt és az E-MS05T_TAN.SW_1.ME-01 mellékletet.

2007-ben a MICROSEC továbbfejlesztette az aláírás létrehozó modult, és azt új funkciókkal bővítette ki. Az új funkciók megfelelőségének igazolására kiegészítő teszteket végzett, amelyet teszt jegyzőkönyvben dokumentált. MICROSEC megrendelése alapján MATRIX vállalkozott az új programverzió tanúsítási eljárásának lefolytatására. A tanúsítás az eredeti eljárás eredményeit felhasználva az új funkciók vizsgálatára fókuszált, de e mellett ellenőrizte a korábban vizsgált funkciók helyes működését is.

A tanúsítási eljárás eredményeképp MATRIX kiadta a vizsgált alkalmazás megfelelőséget igazoló E-MS07T-TAN.SW azonosítójú tanúsítványt és annak E-MS07T-TAN.SW.ME-01 azonosítójú mellékletét.

2 A VIZSGÁLAT TÁRGYA

Megnevezés: „MICROSEC e-Szignó 3.1 minősített aláírás létrehozó és kezelő alkalmazás XadesSigner megbízható aláírás létrehozó és ellenőrző modulja"

2.1 A tanúsításhoz a fejlesztő által átadott eszközök és dokumentációk

Típus	Tárgy	Verzió	Dátum	Adat-hordozó
Szoftver	e-Szigno_3_1_24_8_setup program, benne a vizsgálandó XadesSigner modul	1.1.10.13	2007.09.01.	elektronikus
Dokumentum	Változások az e-Szignó funkcionalitásában (3.1) a 2005. október 12-én tanúsított verzióhoz képest (3.0)	---	2007.09.01.	elektronikus
Dokumentum	Tesztjegyzőkönyv a XadesSigner megbízható aláírás-létrehozó modulhoz	Ver. 1.0. 2007.07.31.	2007.09.01.	elektronikus
Dokumentum	Kiegészítés a XadesSigner megbízható aláírás-létrehozó modulhoz készült tesztjegyzőkönyvhöz	Ver. 1.0, 2007.08.13.	2007.09.01.	elektronikus

Dokumentum	Nyilatkozat a biztonsági körülményekről	---	2007.11.14.	papír
Dokumentum	Nyilatkozat a műszaki normatíváknak való megfelelőségről	---	2007.11.14.	papír

2.2 Fejlesztő

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

3 AZ E-SZIGNÓ 3.1 BEMUTATÁSA

3.1 Működés leírása

A MICROSEC e-Szignó 3.1 egy minősített aláírás létrehozó és kezelő alkalmazás, amely biztosítja az elektronikus ügyvitelben az elektronikus dokumentumok kezeléséhez szükséges alábbi funkciókat:

- az elektronikus akták létrehozása,
- elektronikus dokumentumok beillesztése,
- elektronikus dokumentumok és akták aláírása,
- az elektronikus akta, a dokumentumok és az aláírások leíró adatokkal való ellátása,
- sértetlenségük és hitelességük ellenőrzése és
- nyugtázása.

Az elektronikus dokumentumokat és a leíró adatokat összefogó elektronikus aktát e-aktának nevezzük.

Az e-Szignó tipikus felhasználása, hogy az egyes, e-Szignóval rendelkező Windows munkaállomások a lokális 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 átvételi elismervénnyel nyugtázhatnak.

Az e-Szignó által létrehozott elektronikus aláírás állomány formátuma megfelel az RFC 3275 (XMLSignature) és az erre épülő ETSI TS 101 903 v1.2.2. (XAdES – XML Advanced Electronic Signatures) ajánlásoknak. Ezek lehetővé teszik, hogy az elektronikus dokumentumokat egy vagy több elektronikus aláírással lássuk el. Az elektronikus aláírások biztosítják az elektronikus dokumentumok hitelességét, valamint az ügyintézők azonosíthatóságát, azaz utólag is megállapítható, hogy ki, mikor és milyen

tartalommal írt alá egy dokumentumot. Egy dokumentum elektronikus aláírása rögzíti a dokumentum pillanatnyi állapotát és az aláírás ellenőrzésekor felfedhetővé tesz bármiféle utólagos módosítást, egyúttal biztosítja az aláírás letagadhatatlanságát is. Az elektronikus aláírás elkészítése egy személyhez rendelt chipkártya (smartcard) és az e-Szignó alkalmazás segítségével történik.

3.2 A VT ismertetése

A MICROSEC e-Szignó 3.1 minősített aláírás létrehozó és kezelő alkalmazás két fő komponensből áll:

- az Aláírás létrehozásához szükséges műveleteket végrehajtó Megbízható aláírás-létrehozó modulból (XadesSigner) és
- az aláírással kapcsolatos műveleteket a felhasználó számára elérhetővé tevő Felhasználói felületből.

A jelen vizsgálat tárgyát képező XadesSigner megbízható aláírás létrehozó és ellenőrző modul biztosítja az összes funkciót, amely az elektronikus aláírás megbízható módon történő létrehozásához és ellenőrzéséhez szükséges. Az aláírás-létrehozás folyamatát elemi műveletként teszi elérhetővé a Felhasználói felület számára.

A XadesSigner garantálja, hogy kívülről elérhető műveleteire – tetszőleges szekvenciában történő használat esetén is – teljesülnek a következők:

1. Egy e-akta megnyitása és lezárása között kizárólag a XadesSigner fér hozzá az e-aktához.
2. Az e-akta formátuma mindvégig megfelel az XMLSignature és a XAdES formátumoknak.
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) a XadesSigner által.
6. A Profilok adatainak módosítása az e-akta lezárását követően kimutatható, amennyiben az e-akta lezárásakor az Aláíró aláírást készített az e-aktára.

A XadesSigner az aláírási folyamat részeként a következő funkciókat végzi:

- az Aláírás-jellemzők meghatározása illetve összegyűjtése,
- az Aláírói Tanúsítvány kiválasztásának lehetővé tétele és a kiválasztott megjelenítése,
- az Aláírandó dokumentum megjelenítése a megfelelő – támogatott biztonságos formátum esetében a beépített biztonságos – megjelenítő programmal,

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

A minősített aláírás létrehozása egy Biztonságos Aláírás-Létrehozó 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.

A Tanúsítványok megjelenítését a Microsoft Windows operációs rendszerek részeként szállított cryptui.dll végzi.

Az Időbélyeg elkészítését, a Tanúsítvány-lánc felépítéséhez szükséges Tanúsítványok, valamint a visszavonási információk (CRL-ek vagy OCSP válaszok) beszerzését a XadesSigner az Interneten HTTP, HTTPS és LDAP kapcsolatok segítségével bonyolítja le a Windows operációs rendszer részét képező ws2_32.dll segítségével.

A Dokumentumok – Aláírás létrehozás során szükséges – formátumoktól függő megjelenítését támogatott biztonságos formátum esetében a beépített biztonságos megjelenítő, a többi dokumentum esetében az operációs rendszerben az adott formátumhoz (kiterjesztéshez) tartozó megjelenítő program végzi.

E-akta aláírásakor az e-akta tartalmának megjelenítését a beépített biztonságos megjelenítő végzi.

A VT a korábban tanúsított XadesSigner 1.0.23.0 verziójú modul továbbfejlesztett változata. A főbb változások az előző verzióhoz képest:

Funkcionális változások:

- különálló aláírás létrehozása,
- felkínált aláírói tanúsítvány lista szűkítése,
- beillesztett dokumentumok formátumellenőrzésének módja,
- támogatott biztonságos formátumok megjelenése,
- dokumentum és e-akta titkosítása,
- explicit megadott aláírási szabályzatok real-time ellenőrzése.

Nem funkcionális változások:

- egyes profilokban új elemek jelentek meg illetve maradtak el,
- áttekinthetőbb felhasználói felület,
- átvételi elismervények kezelése felhasználóbarátabb lett,
- változtak a modulok fordítási egységei.

Platform változás:

- A korábbi program Microsoft Windows 2000 és Microsoft Windows XP operációs rendszereken futott,
- az új programverziót a Microsoft Windows XP SP2 és Microsoft Windows Vista operációs rendszerekre tervezték.

3.3 Felhasznált külső szoftver komponensek

Az e-Szignó program néhány külső forrásból származó kódot is felhasznál, amelyek külön modulban találhatóak, és az e-Szignó alkalmazással együtt szállításra kerülnek. Ezek a következők:

1. MS Visual Studio futtatókörnyezet
   - mfc71.dll (MS Foundation Classes funkciók)
   - msvcp71.dll (MS Visual C++ 7.1 futtatókörnyezet funkciók)
   - msvcr71.dll (MS Visual C 7.1 futtatókörnyezet funkciók)
   - atl71.dll (MS Active Template Library, 7.1, COM futtatókörnyezet funkciók)

2. Windows Image Helper (hibakereső modul)
   - dbghelp.dll

3. Netscape Mozilla komponensek
   - nsldap32v50.dll (Mozilla LDAP környezet)
   - libnspr4.dll (NSPR (Netscape Portable Runtime) környezet)
   - libplc4.dll (NSPR string funkciók)
   - libplds4.dll (NSPR memória funkciók)

Az e-Szignó működése során ezeken kívül közvetlenül meghívja és felhasználja a Windows operációs rendszer egyes funkcióit (pl. CryptoAPI, Windows shell funkciók, Windows filesystem funkciók stb.).

3.4 Hardver környezet

A VT működése során a következő külső hardver komponensek jelenlétét igényli:

- Minősített aláírás készítésekor az Aláírás-létrehozó adatok használatához:
  - Biztonságos Aláírás-Létrehozó Eszköz,
- Tanúsítványok beszerzéséhez; a Tanúsítványok visszavonási információinak beszerzéséhez; Időbélyeg készítéséhez:
  - TCP/IP hálózati összeköttetés a Hitelesítés szolgáltató, az Időbélyegzés szolgáltató és az OCSP szolgáltató eléréséhez.

3.5 Támogatott Aláírói dokumentum formátumok

Az e-Szignó a támogatott formátumok esetében saját maga ellenőrzi a formátumot; az ellenőrzés eredménye (sikeres vagy nem sikeres) eltárolásra kerül az e-aktában az Aláírói dokumentumhoz tartozó Profilban. A formátumok meghatározására a MIME-type-ot használja.

Az e-Szignó a következő formátumú állományokat támogatja:

Formátum	Specifikáció
text/plain	RFC2646, ISO 8859-2
text/xml	RFC 3023, W3C XML V1.0
application/pdf	Adobe PDF V1.5
text/rtf	\rtf\ansi\ansicpg1250\uc1\deff0\stshfd
text/html	RFC2854, HTML V4.0
application/msword	Microsoft Word 97 V8.0
image/jpeg	JFIF V1.02 1992
image/tiff	RFC2302 , TIFF V6.0
image/png	PNG V1.0 1996
image/gif	GIF 89a
application/zip	PKWARE 98
application/eszigno	Microsec e-Szignó 2.0
application/eszigno3	Microsec e-Szignó 3.0

A támogatott formátumok közül azokat, amelyek biztosan nem tartalmazhatnak aktív elemet, valamint amelyekhez a VT tartalmaz biztonságos (beépített) megjelenítő programot, *támogatott biztonságos formátumnak* nevezi. A támogatott biztonságos formátumok a következők:

Formátum	Specifikáció
text/plain	RFC2646, ISO 8859-2
text/rtf	\rtf\ansi\ansicpg1250\uc1\deff0\stshfd
application/eszigno3	Microsec e-Szignó 3.0

Egy Aláíráshoz kapcsolódóan az e-aktában eltárolásra kerül az a körülmény is, hogy az Aláíró az aláírási folyamat során megtekintette-e az Aláírói dokumentumot a beépített biztonságos megjelenítő segítségével.

A (támogatott biztonságos formátumokon kívüli) többi formátum megjelenítése mindig az operációs rendszerben az adott formátumhoz (kiterjesztéshez) rendelt megjelenítő program segítségével történik.

4 MEGFELELŐSÉG

4.1 Megfelelőség a normatív dokumentumok alapján

A "XadesSigner megbízható aláírás létrehozó és ellenőrző modul" megfelel az alábbi követelményeknek:

- Kötelezően betartandó normatívák MATRIX által bevizsgálva:

- 2001. évi XXXV. törvény az elektronikus aláírásról,
- 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről,

– Megfelelés az önként vállalt normatíváknak:

- MATRIX által bevizsgált normatívák:
  - MSZ ISO/IEC 15408:2002 Az informatikai biztonság értékelésének közös szempontrendszere,
    - MSZ ISO/IEC 15408-1: Bevezetés és általános modell,
    - MSZ ISO/IEC 15408-2: A biztonság funkcionális követelményei,
    - MSZ ISO/IEC 15408-3: A biztonság garanciális követelményei,
  - Az Európai Parlament és a Tanács 1999/93/EK Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről,
  - 2/2002. (IV. 26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről,
  - CEN CWA 14170:2001 E – Security Requirements for Signature Creation Applications,
  - CEN CWA 14171:2001 E – Procedures for Electronic Signature Verification,
  - a megrendelő által készített Biztonsági Előirányzat (ST-MS-05/001(ver. 1.0)).
- Fejlesztő, vagy más szervezetek által igazolt megfelelések:
  - MMM 001:2005. Egységes MELASZ formátum elektronikus aláírásokra. Verzió:1.0.
  - RFC 3275: XML-Signature Syntax and Processing,
  - ETSI TS 101 903 V1.2.2 (2004-04): XML Advanced Electronic Signatures (XAdES),
  - ETSI TR 102 038 V1.1.1 (2002-04): XML format for Signature Policies,
  - 20/2004. (IV. 21.) PM rendelet az elektronikus számláról,
  - 7/2005. (VII. 18.) IHM rendelet a digitális archiválás szabályairól, valamint az információs társadalommal összefüggő szolgáltatásokkal kapcsolatos elektronikus archiválás szabályairól,
  - 12/2005. (X. 27.) IHM rendelet az elektronikus ügyintézési eljárásban alkalmazható dokumentumok részletes technikai szabályairól,
  - 13/2005. (X. 27.) IHM rendelet a papíralapú dokumentumokról elektronikus úton történő másolat készítésének szabályairól,

- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható időbélyegzés formátum műszaki specifikációjára, 2005. november 1.

- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára, 2005. november 1.

- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára, 2005. november 22.

- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírási szabályzatok készítésére, 2005. november 22.

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

- A tanúsítás kizárólag a bevizsgált XadesSigner 1.1.10.13. verziószámú program modulra vonatkozik, bárminemű változtatás ismételt vizsgálatok és a tanúsítás megújítása nélkül nem engedélyezett

- Nem képezi a tanúsítás részét a program működési környezete, így az

  - operációs rendszer,

  - a felhasznált külső szoftver modulok illetve programok,

  - a működéshez szükséges hardver elemek sem.

4.2 A bevizsgált program komponensek azonosítása

No.	Program modul	Dátum	Verzió	Méret	Leírás	Szerzői jog	SHA-1 lenyomat	SHA-256 lenyomat
01	XadesSigner.dll	2007.11.01. 14:56	1.1.10.13	4 943 872	Az e-Szignó 3.1 minősített aláírás létrehozó és kezelő parancssori alkalmazás megbízható aláírás létrehozó modulja.	Microsec Kft.	8bebec6fcc6a3b03 02242e3f60a64dad fcb62cbd	2669b885b4b36ccc 10918a1e236068ae 311a15a77db06057 9dc2d9657b2e7539
02	XadesSignerLocale ENG .dll	2007.10.30 10:04	---	49 152	Üzenetek, helyi kódolás angolul.	Microsec Kft.	c0fe9bb3b2035716 06803caf76872b23 5654a9c3	24dd3ce407cab54b af198c5336a75630 7d3cec47e6e4cf5e 155c594d0cf58094
03	XadesSignerLocale GER .dll	2007.10.30 10:05	---	53 248	Üzenetek, helyi kódolás németül.	Microsec Kft.	7819bcba8b0f7636 2751d6c89f78a58b 2dd63100	839ec00cca63cb77 331ea102dd08246d d2dafcbb1f7933d7 e923a380033d5752
04	XadesSignerLocale HUN .dll	2007.11.01 14:32	---	53 248	Üzenetek, helyi kódolás magyarul.	Microsec Kft.	67b5119a8bd3b310 f3008831b03853e0 67f84cba	0262cba41cf892a5 1f722e1ec8031c63 5cee01c2ceb1f1f5 72f00cf6e28dc475

05	eszigno3.exe	2007.11.01. 15:09	3.1.24.8	2 828 704	Az elektronikus aláírással kapcsolatos műveleteket a felhasználó számára grafikus felületen elérhetővé tevő komponens.	Microsec Kft.	dcd8bcffdf0342dbe563585af1e758fb663b26ef	9b4edffd8bf1169d4562746fb35dd9ef76741769488d7809126aa59450f8add4
06	CrashReporter.exe	2007.11.01 15:09	1.0.0.33	28˙576	Hibajelentéseket készítő komponens.	Microsec Kft.	f874e1520309cf3b8c093a8598cb9eb71958e4e9	a4b8a0a73698f7e8b402764096e4c75906885d059e04652c5493a64635fd0d6f
07	EszignoScanner.exe	2007.11.01 15:09	1.0.4.47	1˙460˙640	Szkennerkezelő komponens.	Microsec Kft.	a69f5b677402e928065b1d1b01a0175270a8f924	b74eaf9f38b4e59897418d3a0f90770fb1ea233bd039232d2715b6479f61d2a6
08	ESzignoUpdater.exe	2007.11.01 15:09	1.1.0.35	72˙096	Az e-Szignó aláírás-létrehozó alkalmazás frissítését végző komponens.	Microsec Kft.	51ebbf34b9126185aa0a1574909e264d0294e750	84353253dc7e72a2ffbc71d25a5142693dcf3254521d426a5c802dd5199b3ecb
09	EszignoBar.dll	2007.11.01 15:09	1.0.1.36	104˙864	Az Internet Explorer alá beépülő e-Szignó toolbar komponens.	Microsec Kft.	92876092282de0bce82f84333af953b47fffa2ad	b522629467c6695606d4b4e62cf14acdaee62103148215ad8539c500d0b5f61f
10	MIMEChecker.dll	2007.11.01 14:57	1.0.3.51	1˙232˙896	A MIME-típus ellenőrzését végző komponens.	Microsec Kft.	084634f0f69232700e4dc57307226fa94a996410	1a158cb518f60574422634869b3b0ca0428888976cdb9639d608495fb24930e6
11	MIMECheckerLocale_ENG.dll	2007.11.01 14:57	1.0.0.36	12˙288	A MIMEChecker nyelvi modulja.	Microsec Kft.	a7433b950898be993026b6d0d0ae8daa552b65d3	6d3d88bc5368b96474089f1a75c916e11b5ed28ff14fd19e3c65288e8fd948d8

12	MIMECheckerLocale_GER.dll	2007.11.01 14:57	1.0.0.36	13˙312	A MIMEChecker nyelvi modulja.	Microsec Kft.	a967b2e7fe142b6fa6a7915e2a922119e9401981	610d8ff88ab3d20b9323eb6ed047e133efeafb4b9ac4cd2f99ef712a038c2091
13	MIMECheckerLocale_HUN.dll	2007.11.01 14:57	1.0.0.36	12˙288	A MIMEChecker nyelvi modulja.	Microsec Kft.	26b3ba1ac8b9fd5884fadbc22544d5cb14fecd2c	37047725cb33d8cc4660f3cdfba4190ebaa4e63b9b018cf0726c7777e34fdb56
14	atl71.dll	2007.06.08 11:03	7.10.3077.0	89˙088	MS Active Template Library funkciók	Microsoft Corporation	86476819229f4bf00f32e5f0969e19c5b61d1b2a	3f25e7b097b65eaf82a6d5b58646dff38ca19347664f40c2b8a409b9d6939457
15	dbghelp.dll	2004.08.17. 16:46	5.1.2600.2180	640˙000	DbgHelp (hibajelentést segítő) funkciók	Microsoft Corporation	d531e4b814c375c4ab121815dde32ae596684412	d9df4472ca6d7908b64794dcc37c110a6f399119688372ba6db465658140ffc5
16	libnspr4.dll	2007.06.08. 12:05	4.4.1.0	204 800	NSPR környezet	Netscape Communications Corporation	ca06c10ce209e61ab71122dc22088855659137dc	2a38c4858f7c504bc7a9428136ea3f266eb4c0571a142eb183affbd18b7d93ee
17	libplc4.dll	2007.06.08. 12:05	4.4.1.0	13 312	NSPR string funkciók	Netscape Communications Corporation	5a33229aa0a8dbcb2804920a3917dd33863033a3	19486278dda77bcaa1a340a7280a21f9a1cadf3005310b557f5b0fcc7371b8b4
18	libplds4.dll	2007.06.08. 12:05	4.4.1.0	9 216	NSPR memória funkciók	Netscape Communications Corporation	2ac17e059552b83fd75af41bac061dc0df29da0b	81c2539b195a3fa8dd4912b20562b21ce5762b1b9974dcc432230b469ad0a9b7
19	MFC71.dll	2007.06.08. 11:03	7.10.3077.0	1 060 864	MS Foundation Classes funkciók	Microsoft Corporation	664dc99e78261a43d876311931694b6ef87cc8b9	4da5efdc46d126b45daeee8bc69c0ba2aa243589046b7dfd12a7e21b9bee6a32
20	msvcp71.dll	2007.06.08. 11:03	7.10.3077.0	499 712	MS Visual C++ 7.1 futtatókörnyezet funkciók	Microsoft Corporation	c8ccb04eedac821a13fae314a2435192860c72b8	df96156f6a548fd6fe5672918de5ae4509d3c810a57bffd2a91de45a3ed5b23b

21	msvcr71.dll	2007.06.08. 11:03	7.10.3052.4	348 160	MS Visual C 7.1 futtatókörnyezet funkciók	Microsoft Corporation	d5502a1d00787d68f548ddeebbde1eca5e2b38ca	8094af5ee310714caebccaeee7769ffb08048503ba478b879edfef5f1a24fefe
22	nsldap32v50.dll	2007.06.08. 12:05	---	143 360	Mozilla LDAP környezet	Netscape Communications Corporation	9f409e9b8c90aba0bac4e433f372539778e34ccd	48a092caa48388918ff82a79ce0a74d80b0175e5eab2786f0262a412c2da398c
23	customui\ CUI_Post.dll	2007.11.01 14:58	1.0.0.37	28˙672	HTTP POST e-Szignó toolbar	Microsec Kft.	e8d1b4c5e2766bd7cd5c2682b858d81aa2c1b34a	11076e520bd7d72332849ed4e5c0782054f380dc2779c861389cb3b70fe782ca
24	customui\ CUI_Xades.dll	2007.11.01 14:59	1.0.0.37	22˙528	Aláírás e-Szignó toolbar	Microsec Kft.	5dc234764e067931daecb13ed8085fcb72b349a4	234e819f31cbd7727eca7d30cc6646e49b10e710b64e00e66da13b3ca80752b5
25	language\ Language_ENG.dll	2007.11.01 14:57	1.0.1.92	446 464	Az e-Szignó angol nyelvű GUI erőforrásai	Microsec Kft.	69034ab4fa5361eba21ed1435dc5a49333043ea0	2ec640dbda72bdc2aa7c96b2e466320583b8f3524d171e6437b97ebe46f69191
26	language\ Language_GER.dll	2007.11.01 14:57	1.0.0.60	446 464	Az e-Szignó német nyelvű GUI erőforrásai	Microsec Kft.	f69f2b6edec531e62bba0cd2a29de856b1747bc7	c4b8394f8d273106b38283c60b273f36e0981d61171bc7d2118fbc83fad2f3db
27	language\ Language_HUN.dll	2007.11.01 14:57	1.0.1.99	479 232	Az e-Szignó magyar nyelvű GUI erőforrásai	Microsec Kft.	712e955c85d3961347490480c19d61fbc635e97b	2b406535c7aa4082cbbaa5605edcdb5846c3fa68316a03742de1266e17439a7b
28	language\ ScannerLanguage_ENG.dll	2007.11.01 14:59	1.0.0.8	77˙824	A szkennervezérlő angol nyelvű GUI erőforrásai	Microsec Kft.	7d7b50e4332684b82bb4514f1bf8fc772e339072	c645950fb57456ca49ed2ef859f925f00b017116c6bcf13923015c2f50230f52
29	language\ ScannerLanguage_GER.dll	2007.11.01 14:59	1.0.0.8	81˙920	A szkennervezérlő német nyelvű GUI erőforrásai	Microsec Kft.	29415d70896ed40cd20309890ff17a519fdb2d8b	b9dacf33cc59bb34d519499c4d8d69cce14f0f6a8277982fe6ff2f9b9a9d9e33

30	language\ ScannerLanguage_HUN .dll	2007.11.01 14:59	1.0.0.8	81˙920	A szkennervezérlő magyar nyelvű GUI erőforrásai	Microsec Kft.	39dc27a7a076feb4 25ace52cf04615c6 57c18353	d602c4b32cb45123 18ce95e5edb727fc 1ac387eec63840e4 424199580bd697d6
31	language\ UpdaterLanguage_ENG .dll	2007.11.01 14:59	1.0.0.8	49˙152	A frissítő angol nyelvű GUI erőforrásai	Microsec Kft.	4d539eb34f015dbf fdd30d89cabfcffe 3b010d71	a76506a4c278bc3a 5e631b58e47da26a 50a1840a3dc51ea1 50da9e2672daeea8
32	language\ UpdaterLanguage_GER .dll	2007.11.01 14:59	1.0.0.8	49˙152	A frissítő német nyelvű GUI erőforrásai	Microsec Kft.	f20c35fde5c3b426 7f60ae7db0c36abb 6d6ffed2	b0c9ba4e8bed2a8e 35019ceae789a29d 477dda831829761e a1eb92e7e65b1298
33	language\ UpdaterLanguage_HUN .dll	2007.11.01 14:59	1.0.0.8	49˙152	A frissítő magyar nyelvű GUI erőforrásai	Microsec Kft.	156a05f61d45ee19 9bfa4d68633e0ec8 55470042	9a5437298e11d278 d7432a9571e0f4b0 164e6118b571857e fe8f43c99ef7b38d
34	schema\ AlapertelmezettSema .dll	2007.11.01 14:58	1.0.0.49	32˙768	Alapértelmezett séma modul	Microsec Kft.	7563068356255965 939aee686823b859 8952dd84	1574b6fc4c99e06a 895d90b414def95d b8c5ce681f4a5310 8fb0300c41e07422
35	schema\ CegeljarasSema.dll	2007.06.29. 10:34	1.0.1.57	1˙314˙816	e-Cégeljárás séma modul	Microsec Kft.	ebe497baa67570c5 d0da57353c2eaf81 0e2518e5	1755b10d3df3b10e 6b7318c25a7a4779 76bbe81749c0ef8e 8587c719bdd0d24d
36	schema\ CegeljarasSema2007 .dll	2007.11.01 14:58	1.0.1.57	1˙318˙912	e-Cégeljárás 2007 séma modul	Microsec Kft.	630a86602154bb53 e6bf15d2bd8b9d40 5266aaea	a4aec5e21c4ef683 3c6552f494ea4e0f a430959e3604beab 34c8dfc9fe40fa02
37	schema\ S_Beszamolo.dll	2007.11.01 14:58	1.0.1.109	73˙728	Mérlegbeszámoló séma modul	Microsec Kft.	f364ee38dd33a7f0 e9398e93710b2bfd 95620646	2140aa1028893007 0efc4141c85d1bb5 40f4a0a9d12f2b0e 6d16afa39fcb120c
38	schema\ S_Ceginformacio.dll	2007.11.01 14:58	1.0.1.78	61˙440	Céginformáció séma modul	Microsec Kft.	4d084095f0db347e 834b4f9dc3ecdc32 49b16fa3	d821704a805cf5e4 ecdd2056dc8bde01 24d8781fd318efcf 91b3c015b42aea84

A tanúsítás érvényessége szempontjából kritikus az első 4 program modul, a többi a felhasználói felület részét képezi, és csak a vizsgált konfiguráció dokumentálása érdekében lett megadva.

Az első alkalmazás maga az aláíró funkciókat végző modul, a másik három a három támogatott nyelnek (magyar, angol, német) megfelelő beállításokat, üzeneteket tartalmazza.

A tanúsítás érvényessége csak a vizsgált programverziókra vonatkozik.

4.3 Működési környezet

A fenti megfelelőség feltétele az alábbi működési környezetre vonatkozó követelményrendszer teljesülése, amelynek betartása a felhasználó felelőssége.

4.3.1 Hardver és szoftver környezet

A VT csak olyan környezetben használható minősített aláírások létrehozására, amelynek minden eleme kielégíti az elvárható 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.

4.3.1.1 Operációs rendszer

A Microsoft 'Windows XP Professional SP2 operációs rendszer EAL-4+ Common Criteria tanúsítvánnyal rendelkezik. A tanúsítványt az USA Nemzeti Biztonsági Hivatala (NSI: National Security Agency) állította ki 2005. november 6-án, majd egy újabb, kibővített tanúsítványt 2007. április 1-én A szoftver tanúsítások a 'CONTROLLED ACCESS PROTECTION PROFILE Version 1.d' védelmi profilon alapulnak, amely 1999. október 8-án kapott EAL-3 szintű Common Criteria alapú tanúsítványt. A vizsgálatok tárgyáról, körülményeiről és eredményeiről részletes információk találhatók az alábbi oldalakról letölthető dokumentumokban:

- http://niap.bahialab.com/cc-scheme/pp/pp.cfm?id=PP_OS_CA_V1.d
- http://niap.bahialab.com/cc%2Dscheme/st/?vid=4025
- http://niap.bahialab.com/cc%2Dscheme/st/?vid=9506

A program biztonságos használatának alapfeltétele a megfelelően biztonságos operációs rendszer használata. Ügyelni kell arra, hogy az operációs rendszert a tanúsítási eljárásban megfogalmazott követelményeknek megfelelő beállításokkal és környezetben kell használni.

A Microsoft VISTA operációs rendszer a Microsoft szoftvercég legújabb fejlesztésű operációs rendszere, amely jelenleg még nem rendelkezik Common Criteria alapú biztonsági tanúsítvánnyal. Az operációs rendszer használata a Microsoft által adott felhasználói és adminisztrációs specifikációk alapján lehetséges a javasolt biztonsági beállítások betartásával.

4.3.1.2 Microsoft Visual Studio futtató környezet könyvtárai

A Microsoft C++ fejlesztő környezet könyvtárai nem rendelkeznek tanúsítással, nem rendelkezünk a fejlesztés körülményeire vonatkozó információkkal, a VT fejlesztőjének nincs ráhatása a modulok kialakítására, így a tanúsítás nem terjed ki ezen modulok működésére.

A Microsoft könyvtárak használatánál figyelembe kell venni, hogy egy neves – magát a Windows operációs rendszert is előállító – szoftvercég széleskörűen felhasznált termékének részei, amelyeknek esetleg jelentkező hibáit folyamatosan javítják és a javítócsomagokat publikálják. A megjelenő javításokat folyamatosan figyelni kell, és

változás esetén a javított könyvtárak felhasználásával új javító illetve telepítő csomagot kell kiadni.

A változások nyomon követése a fejlesztő feladata és felelőssége.

4.3.1.3 Netscape könyvtárak

A Netscape könyvtárak nem rendelkeznek tanúsítással, nem rendelkezünk a fejlesztésük körülményeire vonatkozó információkkal, ezért a tanúsítás nem terjed ki ezen modulok működésére.

A használat során figyelembe kell venni, hogy a Netscape egy neves szoftverfejlesztő cég, aki meghatározó szerephez jutott a PKI technológiák alkalmazása és elterjesztése terén, s a kérdéses könyvtárak forráskódját a Mozilla projekt kapcsán nyilvánosságra hozta. Bárki szabadon letöltheti, megvizsgálhatja és felhasználhatja a publikált kódokat, beépítheti saját programjaiba. A nagy nyilvánosságnak köszönhetően az esetleges programhibák, a kódban lévő rejtett csapdák valószínűleg már felderítésre kerültek. Bár a programot nem a MICROSEC írta, a forráskód rendelkezésére áll, amiből maga állította elő megfelelően biztonságos körülmények között a felhasznált könyvtárakat, s ezt bármikor reprodukálni tudja.

A publikált javításokat, fejlesztéseket folyamatosan figyelni kell, és változás esetén a javított könyvtárak felhasználásával új javító illetve telepítő csomagot kell kiadni. Feltárt hiba esetén a MICROSEC is képes az esetleges javítás elvégzésére.

A változások nyomon követése a fejlesztő feladata és felelőssége.

4.3.1.4 BALE eszköz

Az XadesSigner 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 nyilvántartásban.

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.

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.

4.3.1.5 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.

4.3.2 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 a VT üzemeltetését veszélyeztető tényezők leírásra kerülnek, 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.).

4.3.3 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.

4.3.4 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 eredeti adathordozó felhasználásával rendszeresen ellenőrizni kell a számítógépre telepített program integritását.

4.3.5 Felhasználói felület

A XadesSigner modul biztonságos üzemeltetéséhez a szoftver felhasználói felületének biztosítania kell a Biztonsági Előirányzatban rögzített körülményeket.

4.4 Algoritmusok és kapcsolódó paraméterek

Az aláírandó adathalmaz lenyomatának létrehozására (hash) használt függvény:

- **sha1** FIPS PUB 180-1. (1995) / ISO/IEC 10118-3 (1998).

A kitöltő adatok hozzáadására használt függvény:

- **emsa-pkcs-v1_5** RSA Laboratories, .PKCS #1 v2.0 (1998).

Az alkalmazott algoritmusok megfelelnek a kötelező és önként vállalt normatívák előírásainak.

Az aláírás elvégzése a VT határain kívül, a BALE eszközben történik, így az erre vonatkozó megfelelést nem kell igazolni. A megfelelő tanúsítvánnyal rendelkező BALE eszköz választása garantálja a normatíváknak való megfelelést.

4.5 Biztonsági szint

A MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. igazolja, hogy a Microsec Kft. által fejlesztett e-Szignó 3.1 aláírás létrehozó és kezelő alkalmazás 1.1.10.13. verziószámú XadesSigner modulja megfelel a normatív dokumentumokban foglalt követelményeknek a vizsgált környezetben.

A megfelelés biztonsági garancia szintje a Common Criteria értékelési rendszere szerint EAL 3+ az ALC_FLR (A termék felfedezett hibáinak javítása) garanciacsaládnak való megfelelés vállalásával.[1]

A megfelelőségre vonatkozó megállapítást a témakör biztonságát érintő jelentős tudományos felfedezés, illetve új verzió kiadása esetén felül kell vizsgálni.

5 RÖVIDÍTÉSEK

BE	Biztonsági Előirányzat
CC	MSZ ISO/IEC 15408 Az informatikai biztonság értékelésének közös szempontrendszere
PP	Protection Profile, Biztonsági Specifikáció
ST	Security Target, Biztonsági Előirányzat

[1] A kiadott tanúsítvány nem kerül automatikusan elfogadásra külföldön, mivel a MATRIX nem rendelkezik a CCRA körben érvényes tanúsítvány kibocsátói jogosítvánnyal.

TOE Target Of Evaluation, a Vizsgálat Tárgya

VT Vizsgálat Tárgya

Dokumentum vége