TANÚSÍTVÁNY (E-MS05T-TAN.SW_1)
MELLÉKLETE

Dokumentumazonosító:	**TAN.SW_1.ME-01**	
Projektazonosító:	**E-MS05T**	**Microsec Kft. 2005**
MATRIX tanúsítási igazgató:	**Dr. Szőke Sándor**	
Kelt:	**Budapest, 2005. október 12.**	

……

MATRIX tanúsítási igazgató

TARTALOMJEGYZÉK

1. A tanúsítás körülményei 2
2. A vizsgálat tárgya 3
2.1. A tanúsításhoz a fejlesztő által átadott eszközök és dokumentációk 3
2.2. Fejlesztő 4
3. Az e-Szignó bemutatása 4
3.1. Működés leírása 4
3.2. A VT ismertetése 5
3.3. Felhasznált külső szoftver komponensek 6
3.4. Hardver környezet 7
3.5. Támogatott Aláírói dokumentum formátumok 7
4. Megfelelőség 9
4.1. Megfelelőség a normatív dokumentumok alapján 9
4.2. Működési környezet 10
4.2.1. Hardver és szoftver környezet 10
4.2.1.1. Operációs rendszer 11
4.2.1.2. Microsoft Visual Studio futtató környezet könyvtárai 11
4.2.1.3. Netscape könyvtárak 11
4.2.1.4. A bevizsgált program komponensek azonosítása 12
4.2.1.5. BALE eszköz 12
4.2.1.1. Hálózati működés 13
4.2.2. Személyi védelem 13
4.2.3. A fizikai védelem 13
4.2.4. Szállítás és telepítés 14
4.2.5. Felhasználói felület 14
4.3. Algoritmusok és kapcsolódó paraméterek 14
4.4. Biztonsági szint 14
5. Rövidítések 15

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: 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,
-
- 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.

  illetve 2005. április 1. után

- 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 (továbbiakban: BE) alapján kifejlesztette az e-Szignó 3.0 minősített aláírás létrehozó és kezelő alkalmazást, és annak részeként a vizsgálat tárgyát képező XadesSigner.dll 1.0.23.0 aláírást létrehozó modult. A BE követelményrendszere alapján részletes tesztelést hajtott végre a BE-ben azonosított követelmények szerinti csoportosításban. A tesztekről részletes Tesztjegyzőkönyvet készített, amelynek célja annak bizonyítása, hogy az e-Szignó megfelel a BE-ben meghatározott követelményeknek.

A Tesztjegyzőkönyvben a BE-ben azonosított – az e-Szignó alkalmazás egészére vonatkozó – összes követelmény megtalálható. Minden követelménynél fel van tüntetve, hogy az adott követelmény teljesítéséért melyik komponens a felelős. Tesztek elvégzése csak azoknál a követelményeknél történt, ahol a megfelelés a XadesSigner modul a feladata. A felhasználói felület megfelelőségét igazoló teszteket külön dokumentum fogja tartalmazni egy újabb tanúsítás keretében.

A tanúsítási folyamat során ellenőrzésképpen elvégeztük a Tesztjegyzőkönyvben leírt valamennyi tesztet, s megvizsgáltuk, 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.

A tanúsítási eljárás eredményeképp 2005. július 29-én kiállításra került az E-MS05T-TAN.SW azonosítójú tanúsítvány és a mellékletét képező E-MS05T-TAN.SW.ME-01 melléklet.

A Nemzeti Hírközlési Hatóság által 2005. szeptember 23-án végzett szokásos éves ellenőrzés során megállapításra került, hogy a tanúsítványban megadott állapothoz képest változott a jogi szabályozás, ezért a MÁTRIX kezdeményezte a tanúsítási eljárás felülvizsgálatát és a szükséges módosítások elvégzését.

Az eljárás eredményeképpen visszavonásra került az E-MS05T-TAN.SW azonosítójú tanúsítvány és annak E-MS05T-TAN.SW.ME-01 azonosítójú melléklete. Ezzel egyidőben kiadásra került az eredeti szöveget és a módosításokat egységes rendszerbe foglaló E-MS05T-TAN.SW_1 azonosítójú tanúsítvány és annak E-MS05T-TAN.SW_1.ME-01 azonosítójú melléklete.

2. A VIZSGÁLAT TÁRGYA

Megnevezés: „XadesSigner.dll megbízható aláírás létrehozó modul"

2.1. A tanúsításhoz a fejlesztő által átadott eszközök és dokumentációk

Típus	Tárgy	Verzió	Dátum	Adat-hordozó
Szoftver	XadesSigner.dll	1.0.23.0.	2005.07.02.	CD
Hardver	GemPC 410 kártyaolvasó		2005.07.02.	-
Hardver	„STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v.2.2” BALE chipkártya		2005.07.02.	-
Dokumentáció	Tesztjegyzőkönyv az XadesSigner.dll megbízható aláírás létrehozó modulhoz		2005.07.02.	CD + papír
Dokumentáció	Nyilatkozat		2005.07.02.	Papír

2.2. Fejlesztő

Microsec Számítástechnikai Fejlesztő Kft.
1031 Budapest, Záhony u. 7.

3. AZ E-SZIGNÓ BEMUTATÁSA

3.1. Működés leírása

A Microsec e-Szignó 3.0 egy Microsoft Windows 2000 és Microsoft Windows XP operációs rendszeren futó minősített aláírás létrehozó és kezelő alkalmazás, amely biztosítja az elektronikus ügyvitelben az elektronikus dokumentumok kezeléséhez szükséges alábbi funkciókat:

- *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 leíró adataikat az e-Szignó *elektronikus aktákban* (e-aktákban) fogja össze.

Az e-Szignó tipikus felhasználása, hogy az egyes, e-Szignóval rendelkező munkaállomások a helyi 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 elismervényekkel nyugtázhatnak.

Az elektronikus levelek a továbbítandó iratokat e-irat formájában tartalmazzák.

Az e-Szignó által létrehozott e-irat 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 a tartalmazott 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 láttamozott 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 a VT segítségével történik.

3.2. A VT ismertetése

Az e-Szignó 3.0 minősített aláírás létrehozó és kezelő alkalmazás két fő komponensből áll:

- az Aláírás létrehozásához szükséges műveleteket végrehajtó *Megbízható aláírás-létrehozó modulból* (XadesSigner.dll) és

- az aláírással kapcsolatos műveleteket a felhasználó számára elérhetővé tevő *Felhasználói felületből* (EsignoNav.exe).

A jelen vizsgálat tárgyát képező *XadesSigner.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 XadesSigner garantálja, hogy kívülről elérhető műveleteire – tetszőleges szekvenciában történő használat esetén is – teljesülnek a következők:

1. Egy e-akta megnyitása és lezárása között kizárólag az 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) az XadesSigner által.

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

Az XadesSigner 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 az 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 lenyomatkészítés a *Microsoft Crypto API* segítségével 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 listák (CRL-ek) beszerzését, azonkívül a Tanúsítvány OCSP protokollal történő ellenőriztetését a XadesSigner az Interneten HTTP, HTTPS és LDAP kapcsolatok segítségével bonyolítja le a *ws2_32.dll* segítségével.

A Dokumentumok – Aláírás létrehozás során szükséges – formátumoktól függő megjelenítése néhány kiválasztott megjelenítő program segítségével történik, ezek: Notepad, AcrobatReader, XPZip, Word, MS Internet Explorer, XP ImageViewer.

Az e-akta Profiljának megjelenítését az MS Internet Explorer végzi.

3.3. Felhasznált külső szoftver komponensek

Az e-Szignó program működése során közvetlenül meghívja és felhasználja a Windows operációs rendszer egyes moduljait, a Microsoft C/C++ fejlesztő környezet szabad felhasználású könyvtárait valamint a Mozilla projektben szabad felhasználásúvá tett egyes Netscape modulokat.

Windows rendszerkomponensek:

- advapi32.dll (kriptográfiai csatoló (BALE); Registry kezelés)
- crypt32.dll (kriptográfiai rutinok)
- cryptui.dll (tanúsítvány megjelenítő)
- kernel32.dll (Windows filesystem funkciók)
- rpcrt4.dll (UUID generátor)
- shell32.dll (Windows shell funkciók)
- user32.dll (menükezelés)
- ws2_32.dll (Windows socket átviteli és namespace funkciók)

MS Visual Studio futtatókörnyezet:

- mfc71.dll (MS Foundation Classes 7.1 funkciók)
- msvcp71.dll (MS Visual C++ 7.1 futtatókörnyezet funkciók)
- msvcr71.dll (MS Visual C 7.1 futtatókörnyezet funkciók)

Netscape Mozilla komponensek:

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

Dokumentum megjelenítő programok

- MS Internet Explorer
- Notepad
- XPZip
- XP ImageViewer
- MS Word
- Adobe Acrobat Reader

Az MS Internet Explorer, a Notepad, az MS Zip és az MS ImageViewer a Microsoft Windows operációs rendszer részei, az MS Word és az Acrobat Reader független szoftveres cégek termékei.

3.4. Hardver környezet

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

- Aláírás-létrehozó adatok használatához:

  - Biztonságos Aláírás-Létrehozó Eszköz

- 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.

3.5. Támogatott Aláírói dokumentum formátumok

Az e-Szignó három kategóriába sorolja az Aláírói dokumentumokat azok formátuma alapján.

Elektronikus állomány:	Bármilyen elektronikus formátumban létező adathalmaz.
Elektronikus dokumentum:	Olyan elektronikus állomány, amelynek ismert a formátuma, azonban nem zárható ki, hogy aktív elemet tartalmaz, és így nem garantálható, hogy mindig mindenhol ugyanúgy lehet megjeleníteni.
Elektronikus irat:	Olyan elektronikus dokumentum, amely nem tartalmaz aktív elemet, valamint egyértelműen ismert a használandó megjelenítő alkalmazás; így garantálható, hogy minden megjelenítéskor ugyanazt a képet mutatja.

Az e-Szignó a következő formátumú állományokat kezeli:

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

Az e-Szignó a támogatott formátumok mindegyikéhez egyértelműen hozzárendeli a megjelenítéshez használandó alkalmazást. Ezek a következőek:

Formátum	Megjelenítőprogram
text/plain	NotePad
text/xml	Internet Explorer
application/pdf	Adobe Acrobat Reader
text/rtf	MS Word
text/html	Internet Explorer
application/msword	MS Word
image/jpeg	Windows kép és faxmegjelenítő
image/tiff	Windows kép és faxmegjelenítő
image/png	Windows kép és faxmegjelenítő
image/gif	Windows kép és faxmegjelenítő
application/zip	Windows kép és faxmegjelenítő
application/eszigno	e-Szignó 2.0
application/eszigno3	e-Szignó 3.0

Amennyiben egy beillesztett állomány formátuma nem ezek közül való (’unknown’), akkor a felhasználó a beillesztés során megadhatja a használni kívánt megjelenítő programot.

Egy beillesztett állomány formátuma mindig ellenőrzésre kerül. Amennyiben ennek révén bizonyságot nyert a formátuma, a következő kategóriákba sorolódik:

Formátum	Veszély	Kategória
text/plain	–	Elektronikus irat
text/xml	–	Elektronikus irat
application/pdf	–	Elektronikus irat
text/rtf	–	Elektronikus irat
text/html	Aktív elemet tartalmazhat	Elektronikus dokumentum
application/msword	Aktív elemet tartalmazhat	Elektronikus dokumentum
image/jpeg	Aktív elemet tartalmazhat	Elektronikus dokumentum
image/tiff	Aktív elemet tartalmazhat	Elektronikus dokumentum
image/png	Aktív elemet tartalmazhat	Elektronikus dokumentum
image/gif	Aktív elemet tartalmazhat	Elektronikus dokumentum
application/zip	Beágyazott állományról nincs információ	Elektronikus adat
application/eszigno	Beágyazott állományról nincs információ	Elektronikus adat
application/eszigno3	Beágyazott állományról nincs információ	Elektronikus adat

Egy ismeretlen formátumú állomány kategóriája mindig Elektronikus adat.

4. MEGFELELŐSÉG

4.1. Megfelelőség a normatív dokumentumok alapján

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

- 2001. évi XXXV. törvény az elektronikus aláírásról,
- 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről,
- 2/2002. (IV. 26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről,

- 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,
- CWA 14170:2001 E – Security Requirements for Signature Creation Applications,
- CWA 14171:2001 E – Procedures for Electronic Signature Verification,
- 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
- a megrendelő által készített Biztonsági Előirányzat (ST-MS-05/001(ver. 1.0)).

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.dll 1.0.23.0. 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. Működési környezet

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

4.2.1. 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.

4.2.1.1. Operációs rendszer

A VT Microsoft Windows 2000 és Microsoft 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 2000 tanúsított, a Windows XP Professional jelenleg biztonsági tanúsítás alatt áll. A tanúsítás elkészülte után a rendszert a tanúsításban megfogalmazott feltételek betartásával kell telepíteni és üzemeltetni.

A fentiektől eltérő Windows operációs rendszer is használható, ilyen esetben azonban fokozottan kell ügyelni a rendszer fizikai biztonságára és az alkalmazott üzemeltetési védelmi intézkedések szigorú betartására.

4.2.1.2. 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.

4.2.1.3. 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.

4.2.1.4. A bevizsgált program komponensek azonosítása

Krit.	Név	Verzió	méret	SHA1 lenyomat
	eszigno3.exe	3.0.10.0	2838528	cabb826cb5d86b40f382 3e69784d55c01ed19b5e
+++	libnspr4.dll	4.4.1.0	204800	ca06c10ce209e61ab711 22dc22088855659137dc
+++	libplc4.dll	4.4.1.0	13312	5a33229aa0a8dbcb2804 920a3917dd33863033a3
+++	libplds4.dll	4.4.1.0	9216	2ac17e059552b83fd75a f41bac061dc0df29da0b
+++	MFC71.dll	7.10.3077.0	1060864	664dc99e78261a43d876 311931694b6ef87cc8b9
+++	msvcp71.dll	7.10.3077.0	499712	c8ccb04eedac821a13fa e314a2435192860c72b8
+++	msvcr71.dll	7.10.3052.4	348160	d5502a1d00787d68f548 ddeebbde1eca5e2b38ca
+++	nsldap32v50.dll		139264	7f517fc7fa721e540ae0 b22f1b8a33c1b6d0fe54
+++	XadesSigner.dll	1.0.23.0	4468736	ab7ec86115721c932c2e c928d5a2c3838df51b4a
	TwnLib4.dll	4.0.12.0	356352	e490cadab7a211774e4f 7f46965f8243982a3467
	TwnPRO4.dll	4.0.12.0	251096	4f87cdd9cacd173fc779 8e0be78cee10d3db7263

A tanúsítás érvényessége szempontjából kritikusak az 1. oszlopban megjelölt könyvtárak, amelyek függvényeit a XadesSigner.dll meghívja működése során. A tanúsítás érvényessége csak a vizsgált programverziókra vonatkozik.

4.2.1.5. 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.

4.2.1.1. 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 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.).

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

4.2.5. Felhasználói felület

Az XadesSigner.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 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.

4.4. Biztonsági szint

A MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. igazolja, hogy a Microsec Kft. által fejlesztett e-Szignó 3.0 nevű aláírás létrehozó és ellenőrző alkalmazás 1.0.23.0 verziószámú XadesSigner.dll 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

TOE Target Of Evaluation, a Vizsgálat Tárgya

VT Vizsgálat Tárgya

Dokumentum vége

[1] Az EAL szint tájékoztató jellegű, CCRA hatókörben nem automatikusan elfogadott.