TANÚSÍTVÁNY (E-MS06T_TAN-02.SW) MELLÉKLETE

Dokumentumazonosító:	TAN-02.SW.ME-01	
Projektazonosító:	E-MS06T	Microsec Kft. 2006
MATRIX tanúsítási igazgató:	Dr. Szőke Sándor	
Kelt:	Budapest, 2007. március 14.	
	…… MATRIX tanúsítási igazgató	

TARTALOMJEGYZÉK

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 parancssori alkalmazáshoz” dokumentumot. A MATRIX a dokumentumok bevizsgálása után Tanúsítványokat állított ki (azonosító: E-MS03T-TAN.PP illetve E-MS06T-TAN-01.ST).

A MICROSEC a Biztonsági Előirányzat (továbbiakban: BE) alapján kifejlesztette az e-Szignó 3.1 minősített aláírás létrehozó és kezelő parancssori alkalmazást, és annak részeként a vizsgálat tárgyát képező "Megbízható aláírás-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 "Megbízható aláírás-létrehozó modul" feladata. A felhasználói felület megfelelőségét igazoló teszteket külön dokumentum fogja tartalmazni egy újabb tanúsítás keretében.

A tanúsítási folyamat során ellenőrzésképpen ismételten elvégeztük a Tesztjegyzőkönyvben leírt valamennyi tesztet, s megvizsgáltuk, hogy az átadott eszközök és dokumentumok alapján az e-Szignó program magját képező megbízható 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

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

2.1 A tanúsításhoz a fejlesztő által átadott eszközök és dokumentációk

Típus	Tárgy	Verzió	Dátum	Adat-hordozó
Szoftver	MICROSEC e-Szignó 3.1 minősített aláírás létrehozó és kezelő parancssori alkalmazás	3.1	2007.01.31.	elektronikus

Szoftver	Teszt esetek és teszt eredmények		2007.01.31.	elektronikus
Szoftver	Kiegészítő teszt esetek és teszt eredmények		2007.03.10.	elektronikus
Dokumentáció	Parancssori e-Szignó alkalmazás felhasználói dokumentációja	3.1	2007.01.31.	elektronikus
Dokumentáció	Tesztjegyzőkönyv az e-Szignó minősített aláírás létrehozó és kezelő parancssori alkalmazás Megbízható aláírás-létrehozó moduljához	ver. 1.6.	2007.01.21.	elektronikus
Dokumentáció	Kiegészítés az e-Szignó minősített aláírás létrehozó és kezelő parancssori alkalmazás Megbízható aláírás-létrehozó moduljához készült tesztjegyzőkönyvhöz		2007.03.10.	elektronikus
Dokumentáció	Nyilatkozat a biztonsági körülményekről		2007.03.14.	Papír
Dokumentáció	Nyilatkozat a műszaki normatíváknak való megfelelőségről		2007.03.14.	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. minősített elektronikus aláírás–létrehozó és kezelő parancssori alkalmazás megbízható aláírás-létrehozó modulját (mint elektronikus aláíráshoz kapcsolódó terméket) elsősorban az e-akták szerveroldali kényelmes és hatékony kezelésére fejlesztették ki. Biztosítja az elektronikus ügyvitelben az

- elektronikus iratok (e-iratok) előállítását,
- elektronikus dokumentumok beillesztését,
- elektronikus dokumentumok és e-akták aláírását,
- az e-akták, a dokumentumok és az aláírások leíró adatokkal való ellátását,
- sértetlenségük és hitelességük ellenőrzését,

- átvételi elismervény készítését.

A MICROSEC parancssori e-Szignó Megbízható aláírás-létrehozó modulja parancssorból hívható, shell script-ekben könnyen használható, előre paraméterezhető program. Több platformon (Unix, Linux, Solaris, WinXP, Windows Server 2003, Windows 2000) futtatható, standard C/C++ nyelven készült program. Tipikus felhasználása az e-akták automatikus fogadása és feldolgozása, átvételi elismervény készítése.

A minősített aláírás létrehozásához szükséges, felhasználóval folytatott többlépéses „párbeszédek" vezérlése a Felhasználói felület feladata, így a két modul együttesen alkalmas minősített aláírások létrehozására.

Az e-Szignó alapértelmezett esetben az RFC 3275 (XMLSignature) és az erre épülő ETSI TS 101 903 v1.2.2. (XAdES – XML Advanced Electronic Signatures) ajánlásoknak megfelelő elektronikus aláírás állományt, e-aktát hoz létre, amely a XAdES aláírásnak egy további tulajdonságokkal bővített, keretbe foglalt fajtája. Ezen kívül képes más, a XAdES-nek megfelelő elektronikus aláírások létrehozására is, így lehetővé téve például tetszőleges XML dokumentum tetszőleges csomópontjának aláírását vagy nagy méretű dokumentumok aláírását oly módon, hogy maga az aláírás állomány ne tartalmazza a dokumentumot. Mindezeken kívül az RFC 3852 (CMS aláírás) és az erre épülő ETSI TS 101 733 V1.6.3. (CAdES – CMS Advanced Electronic Signatures) ajánlásoknak megfelelő aláírás létrehozását is támogatja.

Az aláírások RSA-SHA1 algoritmussal készülnek. A minősített elektronikus aláírás elkészítése egy személyhez rendelt biztonságos aláírás-létrehozó eszköz (BALE) és a VT segítségével történik; fokozott biztonságú aláírás létrehozása fájlrendszerben lévő PKCS#12 formátumú kulcsokkal, illetve PKCS#11 vagy OpenSSL engine interfésszel rendelkező hardver aláíró eszközökkel (chipkártya, HSM) lehetséges.

A program az X.509 formátumú tanúsítványok ellenőrzéséhez szükséges adatok – hitelesítés-szolgáltatói tanúsítványok, időbélyegek, visszavonási listák (CRL: Certificate Revocation List), OCSP (Online Certificate Status Protocol, Online Tanúsítvány-állapot Protokoll) válaszok – begyűjtését is elvégzi.

Támogatja az ETSI TS 102 038 v1.1.1 ajánlásnak megfelelő aláírási szabályzatok használatát.

Lehetőséget nyújt a beillesztett dokumentumok, illetve az egész e-akta RSA-DES3 algoritmussal, PKCS#7 formátumban történő titkosítására is.

3.2 A VT felépítése

A VT a vonatkozó CWA ajánlásoknak megfelelően a következő modulokat tartalmazza:

Aláírás-létrehozó komponensek:

- Aláírói Interfész (ALI)
- Aláírói Dokumentum Megjelenítő (ADM)
- Aláírás Jellemzők Megtekintő (AJM)
- Aláírandó Adathalmaz Formázó (AAF)
- Digitális Lenyomatoló (DL)

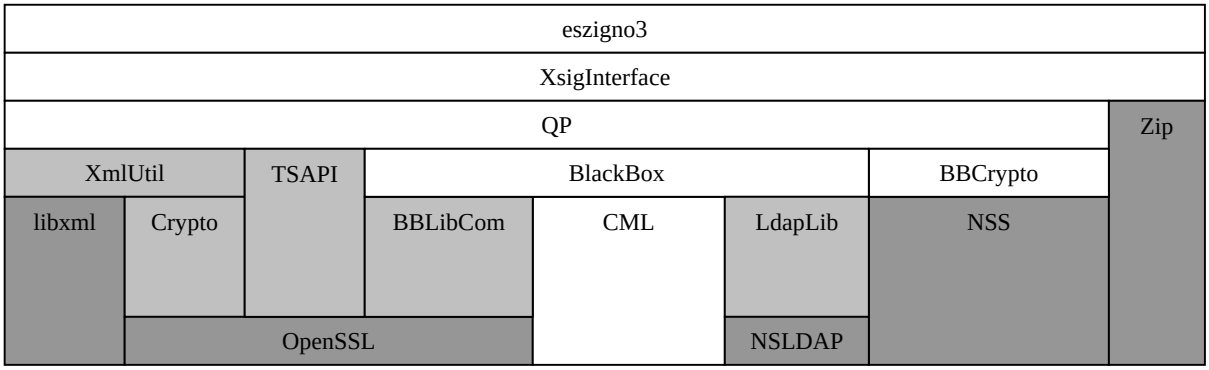
- BALE kommunikátor (BK)
- Aláíró Azonosító (AA)
- BALE Tulajdonos Kijelző (BTK)
- Aláírt Adathalmaz Összeállító (AAÖ)
- Aláírás Naplózó (AN)
- Tanúsítvány Beszerző és Ellenőrző (TBE)
- Aláírói Dokumentum Összeállító (ADÖ)
- Adatforgalmi Interfészek (AI)

Aláírás-ellenőrző komponensek

- Ellenőrzői Interfész (ELI)
- Aláírói Dokumentum Megjelenítő (ADM)
- Aláírási Szabályzat Beszerző (ASB)
- Aláírási Szabályzat Megjelenítő (ASM)
- Aláírói Információ és Kimeneti Állapot Megjelenítő (AKM)
- Érvényesítési Adat Beszerző (EAB)
- Aláírást Érvényesítési Adatokkal Bővítő (AEB)
- Biztonságos Aláírás Ellenőrző (BAE)
- Időjel Író (IJI)
- Ellenőrzés Naplózó (EN)

3.3 A Megbízható aláírás-létrehozó modul felépítése

A Megbízható aláírás-létrehozó modul számos alrendszerből – függvénykönyvtárból – áll, amelyek egy része a különböző platformok mindegyikén szerepel, más részük pedig csak egyes operációs rendszereken szükséges (1. ábra). A függvénykönyvtárak legegyszerűbben funkcionalitásuk szerint osztályozhatók.



1. ábra A megbízható aláírás-létrehozó modul szerkezete

XML feldolgozás

libxml Alapvető XML feldolgozási funkcionalitás, C nyelven megvalósítva.

XAdES (MELASZ) formátum

XmlUtil A XAdES alapját képező XMLDSIG feldolgozását végző függvénykönyvtár, C++ nyelven megvalósítva, kivételkezelés nélkül.

QP A XAdES által definiált kiegészítő aláírási tulajdonságok kezelését végző függvénykönyvtár, C++ nyelven megvalósítva, kivételkezeléssel. (Neve a XAdES formátumban fő szerepet játszó QualifyingProperties XML elem nevéből származik.)

E-akta formátum kezelése

XsigInterface Az e-aktán végezhető műveleteket tartalmazó függvénykönyvtár, C++ nyelven megvalósítva, részleges kivételkezeléssel.

Parancssori interfész

eszigno3 A parancssori paraméterek értelmezését, a ki- és bemenet kezelését végző függvénykönyvtár, C++ nyelven megvalósítva, kivételkezeléssel.

Kriptográfiai szolgáltatások

NSS A tanúsítványok és OCSP válaszok kezelését végző függvénykönyvtár, C nyelven megvalósítva.

OpenSSL Az aláírások és a titkosítás kezelését, az időbélyegek feldolgozását végző függvénykönyvtár, C nyelven megvalósítva. A HTTP kommunikációra is használatos.

CML A tanúsítványlánc ellenőrzését végző függvénykönyvtár, C++ nyelven megvalósítva, kivételkezeléssel.

RSA-SHA1 aláírások kezelése:

Crypto Az aláírások kezelését végző, OpenSSL-re épülő függvénykönyvtár, C++ nyelven megvalósítva, kivételkezelés nélkül. A PKCS #11 modulok és az OpenSSL engine kezelését is ez végzi.

Az X.509 infrastruktúra formátumainak kezelése

BBCrypto A tanúsítványok, CRL-ek és OCSP válaszok kezelését végző függvénykönyvtár, C++ nyelven megvalósítva, kivételkezeléssel. Az NSS-t használja.

TSAPI Az időbélyegek kezelését végző függvénykönyvtár, C++ nyelven megvalósítva, kivételkezelés nélkül. Az OpenSSL-t használja.

BlackBox A tanúsítványok ellenőrzését (tanúsítványlánc és visszavonás-ellenőrzés) végző függvénykönyvtár, C++ nyelven megvalósítva, kivételkezeléssel. A CML-t használja.

BBUtil Segédfüggvények, C++ nyelven megvalósítva, kivételkezeléssel.

Hálózati kommunikáció

NSLDAP Az LDAP kapcsolódáskor használatos függvénykönyvtár, C nyelven megvalósítva.

LdapLib Az NSLDAP-ra épülő C++ burkoló („wrapper") könyvtár. Kivételkezelést nem alkalmaz.

BBLibCom A HTTP kommunikációra használt C++ wrapper az OpenSSL alapjain. Kivételkezelést részlegesen alkalmaz.

Tömörítés

Zip A PKZIP algoritmusú tömörítés implementációja Windows operációs rendszeren, C és C++ nyelven megvalósítva, kivételkezelés nélkül.

ZipArchive A PKZIP algoritmusú tömörítés implementációja Linux és Solaris operációs rendszeren, C++ nyelven megvalósítva, kivételkezeléssel.

Egyéb

Trio A többnyelvűséghez elengedhetetlen változó sorrendű paraméterekkel használható szövegformázó függvénykönyvtár, C nyelven megvalósítva.

UUID UUID-k létrehozására szolgáló függvénykönyvtár, C nyelven megvalósítva. Csak Linuxon és Solarison használatos.

XadesSignerLocale Az eszigno3 nyelvenkénti üzenettábláját tartalmazza, valamint ez végzi az UTF-8 és a lokális karakterkészlet (pl. ISO-8859-2) közötti konverziót.

A fent felsorolt függvénykönyvtárakból a fordítást követően több különböző modul jön létre, amelyeket a telepítő csomag is tartalmaz.

3.4 Felhasznált külső szoftver komponensek

Az e-Szignó 3.1 alkalmazás Felhasználói felülete Microsoft Windows XP platformon futtatható, a következő Windows rendszerkomponensekkel van határfelülete:

- advapi32.dll (kriptográfiai csatoló (BALE); Registry kezelés)
- crypt32.dll (kriptográfiai rutinok)

- cryptui.dll (tanúsítvány megjelenítő)
- kernel32.dll (Windows filesystem funkciók)
- shell32.dll (Windows shell funkciók)
- user32.dll (menükezelés)
- ws2_32.dll (Windows socket átviteli és namespace funkciók)

A Felhasználói Felület által ezen kívül igényelt szoftver komponenseket a telepítő csomag tartalmazza.

3.5 Hardver környezet

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

- Minősített aláírás létrehozásához:
  - 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.

3.6 Támogatott Aláírói dokumentum formátumok

Az e-Szignó három kategóriába sorolja az Aláírói dokumentumokat azok formátuma, s az ettől függő megbízhatóságának mértéke 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 (tartalmat) mutatja.

Az e-Szignó 3.1 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
image/bmp	Windows Bitmap Format
application/zip	PKWARE 98
application/x-zip-compressed	PKWARE 98
application/eszigno	MICROSEC e-Szignó 2.0
application/eszigno3	MICROSEC e-Szignó 3.0

Az e-aktába beillesztett Aláírói dokumentum eltárolásra kerülhet tömörített vagy tömörítetlen formában is. Amennyiben tömörítésre kerül a sor, az eredeti – tömörítés előtti – formátumra vonatkozó információ akkor is eltárolásra kerül.

A támogatott formátumok közül azokat, amelyek biztosan nem tartalmazhatnak aktív elemet, valamint amelyekhez a VT tartalmaz biztonságos (beépített) megjelenítő programot, támogatott biztonságos formátumnak nevezzük. 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 ismeretlen formátumú állomány kategóriája mindig Elektronikus adat.

4 MEGFELELŐSÉG

4.1 Megfelelőség a normatív dokumentumok alapján

Az elvégzett vizsgálatok és a beszerzett nyilatkozatok alapján a "Megbízható aláírás létrehozó modul" megfelel az alábbi normatív 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: Az informatikai biztonság értékelésének közös szempontjai
      1. 15408-1:2002 1. rész: Bevezetés és általános modell,
      2. 15408-2:2003 2. rész: A biztonság funkcionális követelményei,
      3. 15408-3:2003 3. rész: A biztonság garanciális követelményei,
    - Az Európai Parlament és a Tanács 1999/93/EK számú Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről,
    - A Miniszterelnöki Hivatalt vezető miniszter 2/2002. (IV. 26.) MeHVM irányelve 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 Megbízó által készített Biztonsági Előirányzat (ST-MS-06/002 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,
    - RFC 3369: Cryptographic Message Syntax (CMS),
    - ETSI TS 101 733 V1.6.3.: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES),
    - ETSI TS 101 903 V1.2.2 (2004-04): XML Advanced Electronic Signatures (XAdES),
    - ETSI TR 102 038 V1.1.1 (2002-04): TC Security - Electronic Signatures and Infrastructures (ESI); 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.

A biztonságos aláírás létrehozó modul megfelel a fenti követelményeknek a 4.3 pontban leírt működési környezetben az alábbi feltételek teljesülése mellett:

- A tanúsítás kizárólag a 4.2 pontban részletezett, bevizsgált verziószámú program modulokra vonatkozik,

- Nem képezi a tanúsítás részét a program működési környezete, mint például az

  - operációs rendszer,

  - a felhasznált külső szoftver modulok illetve programok,

  - a működéshez szükséges hardver elemek.

4.2 A bevizsgált program komponensek azonosítása

4.2.1 A Windows 32 bites környezet program komponensei

Program modul	Verzió	Méret	Leírás	Szerzői jog	SHA-1 lenyomat	SHA-256 lenyomat
eszigno3.exe	3.1.20.6	4 956 160	Az elektronikus aláírással kapcsolatos műveleteket végző alapkönyvtár, ez végzi a parancssori paraméterek értelmezését és a ki- és bemenet kezelést is.	Microsec Kft.	495615fa70dd423de5657a3d862f1c6bb4fe1733	e0a17ff5bd66a643299714de671ba99eefa5ddae079368e3a705bf7fac93669a
XadesSignerLocale_ENG.dll		86 016	Üzenetek, helyi kódolás angolul.	Microsec Kft.	4d6a2ebf64ee9a17509c30d8f68ebe2d7b6a9759	1ab650877041c072e2c49f2ab75ee476df3a007071868d36de64a9423566ba56
XadesSignerLocale_GER.dll		90 112	Üzenetek, helyi kódolás németül.	Microsec Kft.	eee25fef065eaee4a750570e0cac75a4bc0ef371	084197a113db0dcf6bc140f6d213acebdc0531dfe0888525b5db70a5de172502
XadesSignerLocale_HUN.dll		86 016	Üzenetek, helyi kódolás magyarul.	Microsec Kft.	6c38e9fe9c3288172a3803854857c2a69954f04e	b288dc6bdc720836f11ac0f6dbeb5678c8bf659b4497f532d1598c25ee706b72
MFC71.dll	7.10.3077.0	1 060 864	MS Foundation Classes funkciók	Microsoft Corporation	664dc99e78261a43d876311931694b6ef87cc8b9	4da5efdc46d126b45daeee8bc69c0ba2aa243589046b7dfd12a7e21b9bee6a32
libnspr4.dll	4.4.1.0	204 800	NSPR környezet	Netscape Communications Corporation	ca06c10ce209e61ab71122dc22088855659137dc	2a38c4858f7c504bc7a9428136ea3f266eb4c0571a142eb183affbd18b7d93ee

libplc4.dll	4.4.1.0	13 312	NSPR string funkciók	Netscape Communications Corporation	5a33229aa0a8dbcb2804920a3917dd33863033a3	19486278dda77bcaa1a340a7280a21f9a1cadf3005310b557f5b0fcc7371b8b4
libplds4.dll	4.4.1.0	9 216	NSPR memória funkciók	Netscape Communications Corporation	2ac17e059552b83fd75af41bac061dc0df29da0b	81c2539b195a3fa8dd4912b20562b21ce5762b1b9974dcc432230b469ad0a9b7
msvcp71.dll	7.10.3077.0	499 712	MS Visual C++ 7.1 futtatókörnyezet funkciók	Microsoft Corporation	c8ccb04eedac821a13fae314a2435192860c72b8	df96156f6a548fd6fe5672918de5ae4509d3c810a57bffd2a91de45a3ed5b23b
msvcr71.dll	7.10.3052.4	348 160	MS Visual C 7.1 futtatókörnyezet funkciók	Microsoft Corporation	d5502a1d00787d68f548ddeebbde1eca5e2b38ca	8094af5ee310714caebccaeee7769ffb08048503ba478b879edfef5f1a24fefe
nsldap32v50.dll		143 360	Mozilla LDAP környezet	Netscape Communications Corporation	9f409e9b8c90aba0bac4e433f372539778e34ccd	48a092caa48388918ff82a79ce0a74d80b0175e5eab2786f0262a412c2da398c

4.2.2 A LINUX környezet program komponensei

Program modul	Verzió	Méret	Leírás	Szerzői jog	SHA-1 lenyomat	SHA-256 lenyomat
eszigno3	3.1.20.6	981˙231	A parancssori paraméterek értelmezését, a ki- és bemenet kezelését végző függvénykönyvtár.	Microsec Kft.	142cbdc9fc3f90960edc4022083d51b0efaa3cf4	fd9c0a517665a1d3f4515cab4455f4c73646356f46af01cba030880c0f6c878b
libxadessigner.so		6˙655˙257	Az elektronikus aláírással kapcsolatos műveleteket végző alapkönyvtár.	Microsec Kft.	8c175d7049a71f0eb86db149b8e9545993dbed9e	e794be935a8f73152f165d972e728be1cebc588179a5859175953b35c8d23f96

libxadessignerlocale_eng.so		56˙329	Üzenetek, helyi kódolás angolul.	Microsec Kft.	23cbdf1ba38000bdf2685a3548c1909aadb500db	37ba6ec60cbe44b77c8841e8c4791738491dfa19dc7b4e070a350f58ffeddc10
libxadessignerlocale_ger.so		60˙425	Üzenetek, helyi kódolás németül.	Microsec Kft.	0e38bc7503187bf1dc3825ace01adc2c27a4d935	cc29f1bf4c07c54c142a0c46dfbc07b3a8d959250b28ed8ae013cb302a8a281e
libxadessignerlocale_hun.so		60˙510	Üzenetek, helyi kódolás magyarul.	Microsec Kft.	aa0442858b25ff0b31bc6ff49793622e977c2083	11838e7adfd223934b4a55468f1f892dac0ee84848faa7b2636ead7d3a619a15
libc++asn1.so		328˙587	CML	U.S. Government (SMP Public License)	789630c720cd008a23a7f6307f2733d47f944112	b98f0f92e7dae789a0cf8c934dcccbe53c397710c13a26c30eee2c44a3fe706f
libcmapi.so		1˙168˙932	CML	U.S. Government (SMP Public License)	04783216e725eeb11cd5b9fc409977a1625310b2	23c81c083c4684fb209ffddb98a3541f1d981652bc93faffcc2f3e7e0fe4e292
libcmlasn.so		5˙309˙220	CML	U.S. Government (SMP Public License)	484eb41728c91fa55b86f7a30bbab313e1713444	449a86867a4d3b9ea1c223409221807014fb20ab038896d63eea23bddc6d6cca
libctil.so		417˙950	CML	U.S. Government (SMP Public License)	7db8875a09ac9e52d29bc0282844a19a9beedd51	79987a64cada6a506810a2d910332b2ba02d8a72390359884aa06635ba051b93
libldap50.so		194˙173	NS LDAP	Netscape Communications Corporation	ce6e58412f466a39f02c98b1076e9b4b0f7ee084	c402d4a6e44a86e68acca9f1a2dae9fcff15ac56521baf5da66016495ac2e381

libnspr4.so		325˙482	NSS	Mozilla Corporation (Mozilla Public License)	78ab7884ffcb0d09ad578c2316e76b14d0ca11e6	dba5766fb91b2f793714ae41db855f8c67342fabd563c7b70203d1fd3b9d3859
libpkcs11_cryptopp.so		3˙961˙127	CML	U.S. Government (SMP Public License)	1f980651a6d1a200606da4d8900958842fe035c0	c5e204a3d20f482f845036d64f46a21fe4471fa2efbfa90715481266b3fc997d
libplc4.so		19˙825	NSS	Mozilla Corporation (Mozilla Public License)	4d8b170a219e28e4203d4f0e455a4f2cb7796f69	47458bd698f02ed4982c993d942860a4508c76e4e9851924f073128327bd9c33
libplds4.so		13˙092	NSS	Mozilla Corporation (Mozilla Public License)	550093b1fd6e69b34ef959324f01a189d2dcbe81	ab6315e61ea7cb872beedcd2f0edc2bd2b90dcf53b9be19c884db89aff203c48
libsrlapi.so		272˙353	NSS	Mozilla Corporation (Mozilla Public License)	1b28cb59a5c247641292661b3130be6fa66e9bab	85fb6a52e9add00afa6e083766865d14426f461078de494f4c812e64fd8d675d
libstdc++.so.5		921˙659	GCC	GNU Project	197b90f5b17507ca803da6dca43460c216fd9157	71ad64f18b0ce9d5328ec350c0aaeed4d029a2af8437c83545694bbc809bb3b5
libxml2.so.2		3˙276˙364	libxml	Gnome project (MIT License)	a44a92935e506ae3babf5857685ca3a4c8dea0dc	b41e5ec8417b67545b155a9005369946385e92cdd179d3ad8ddd8aae488d3fbb

4.2.3 A SOLARIS környezet program komponensei

Program modul	Verzió	Méret	Leírás	Szerzői jog	SHA-1 lenyomat	SHA-256 lenyomat
eszigno3	3.1.20.6	945 072	A parancssori paraméterek értelmezését, a ki- és bemenet kezelését végző függvénykönyvtár.	Microsec Kft.	a813d4d3eec71fac2b3b01bbd894812267205fa9	9f11eb23d0aafe43c9b5a47cecb8764c53dbc28e6b60e802fc05d9a148bfd45b
libxadessigner.so		6˙617˙087	Az elektronikus aláírással kapcsolatos műveleteket végző alapkönyvtár.	Microsec Kft.	b9b63bc5e5a5e3330ef97a9c8f58141b418575f5	bd6588397ec13506ca271c0b466d76d555d0a660c6a423d14fed838a24b93d48
libxadessignerlocale_eng.so		52˙275	Üzenetek, helyi kódolás angolul.	Microsec Kft.	daf2b2c7157b3108bd010308c88b5c8d800a1f95	f1b069f302eabf1f395d8c2958df3286fa3f552bdae2c32c082fb77b83cedab8
libxadessignerlocale_ger.so		56˙635	Üzenetek, helyi kódolás németül.	Microsec Kft.	07574ea75f2082c603786e52d2aefc854ee1e123	771b9fd979920ed027b5b6393181c6331b8399286ef3d3102de4108ede646052
libxadessignerlocale_hun.so		54˙784	Üzenetek, helyi kódolás magyarul.	Microsec Kft.	75577aec2fadccde1d61d50fd885122b09cf4257	5d9246faa058b9e2dae8a284b1136ff13fc27185ec07922bd55b615160a00c79
libc++asn1.so		307˙796	CML	U.S. Government (SMP Public License)	ec04b196287dde8463043ac08a6d46b3a06fa64c	da3f05c1f45a6d3f3f071ab133f95934a58ac2ec7846597de13cd8b081f05495
libcmapi.so		1˙330˙613	CML	U.S. Government (SMP Public License)	cc6ae28bdf2391873a16f295b4481c1bdb7b6aa5	df871215b98acd8e210b27714a75e7f84697c967385900a25d99ff366002f171
libcmlasn.so		6˙062˙287	CML	U.S. Government (SMP Public License)	849053050b67f3f5772d1a6bcfb0265653f79550	e600f41bff3c15adecdd78c9c0d3ac8d77d847721703c621f9f5785ea99ac4a8

libctil.so		504˙774	CML	U.S. Government (SMP Public License)	2b13bb20fd71425d673761479ac6ce68efd2562e	42b021d8ff5995041b3061787d412b71c8ae77b789083c516ce45721d6e24b33
libfreebl_hybrid_3.so		277˙656	NSS	Mozilla Corporation (Mozilla Public License)	69102f333dd28e858d6404d41c0f2aa49449bd5c	8c47b89b9a7df750ef76a73711f53f15e39a6bf517bf759816a51bc43db31d27
libgcc_s.so.1		170˙735	GCC	GNU Project	2c6036bcf79c3688e998be6ca389d858d2c69c41	adf52993b62abcc04c9e992c87e07c65103821de64ecd6c3aa181c3bd1894683
libldap50.so		195˙128	NS LDAP	Netscape Communications Corporation	5233f08b090579cfcca0258ff2ac58c7734b1dc6	5db24688ab247e8b946a141e2d7b349ad8991516b34b77657b810cc01364ac0e
libnspr4.so		253˙564	NSS	Mozilla Corporation (Mozilla Public License)	7369644884bd01b87f09366d2b0d6d34c5595cd0	a68069e388e8973c52e7419133ec071482cc32936917a26004029c943cf3ed15
libpkcs11_cryptopp.so		4˙824˙887	CML	U.S. Government (SMP Public License)	14f74633917cd4075fce9f6aadd23989a2459c21	0bf70216474c3f8de50eae3b3b2c75556c6151b9519d45a73db3a46d33b82736
libplc4.so		23˙052	NSS	Mozilla Corporation (Mozilla Public License)	71d75a9d5822127f58b9a6763f5e4f6f371e78c7	712532b1937d03101ad5f6252e36d999ee63664987cb57193dc3f08ca3a007ea
libplds4.so		13˙700	NSS	Mozilla Corporation (Mozilla Public License)	12857768937aa70b2b61d9b38f4e1e9bf4f8aef3	126397344bc682b2385c8b4e7d3931d64d7bda450382e08c520b43d856dc27eb

libsrlapi.so		362˙140	CML	U.S. Government (SMP Public License)	a7af0cf529720878f650c1ee78ec0b7f28f8d557	b927e280abd2deada8db8822dc759bda33f372ccfcef8a74ccfa96a71fa0f18e
libstdc++.so.5		3˙778˙840	GCC	GNU Project	c70d0c6e39f56b0694db2c2a2c08c69c22297f19	6fe36e4a857acf5780b65bb6b3c6a56a6528f61cb3c8f53e73ca784c0d5ebb20
libxml2.so.2		2˙710˙704	libxml	Gnome project (MIT License)	ff842391d91c722a0a537c405d066919d77c4e71	323cc5cbe68b9eeb7c05da6198235ddbec34bb3cf37d779c807ad2467164c654
\cpu\sparcv8plus\libnspr_flt4.so		1 968	NSS	Mozilla Corporation (Mozilla Public License)	478b80ef29d1ca995e92b27531de5a7aa999bfe2	046056ef74d4701c38713c1f04e0e4b35954f79569bf465d20fbd8e302bbce2a

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

Az e-Szignó alkalmazás *Megbízható aláírás-létrehozó modulja* Linux, Solaris és Windows platformon is futtatható. A futáshoz szükséges minimális követelmények:

Linux platform esetében:	legalább 2.4-es kernelű Linux operációs rendszer, legalább v. 2.2.5 glibc,
Solaris platform esetében:	legalább 5.8 SunOS,
Windows platform esetében:	Windows 2000, WindowsXP vagy Windows Server 2003 operációs rendszer szükségesek.

A Megbízható aláírás-létrehozó modul által használt modulok vagy a fenti operációs rendszerek részét képezik, vagy a telepítő csomag tartalmazza őket.

A vizsgált aláírási termék biztonságos használatának előfeltétele, hogy az adott operációs rendszert megfelelően biztonságos konfigurációban használjuk. Előnyben kell részesíteni az IT biztonsági tanúsítással rendelkező operációs rendszereket, pld.. a SUN SOLARIS 10, a Windows 2000 és a Windows XP Professional SP2 CC EAL4+ tanúsítással rendelkezik. A tanúsítással rendelkező operációs rendszereket a biztonságos működtetés érdekében a tanúsításban megfogalmazott feltételek betartásával kell telepíteni és üzemeltetni.

CC tanúsítással nem rendelkező operációs rendszer is használható, ilyen esetben azonban fokozottan kell ügyelni a rendszer fizikai biztonságára és az alkalmazott üzemeltetési védelmi intézkedések szigorú betartására.

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

A Biztonságos aláírás-létrehozó 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 meghajtó modul megbízhatóságára. A BALE csak olyan meghajtóval használható, amelyet a BALE gyártója szállít, vagy amelynek fejlesztője hitelt érdemlően garantálja a modul 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 megoldás 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 Megbízható aláírás-létrehozó 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.

A minősített aláírás létrehozása 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 garancia szint

A MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. igazolja, hogy a MICROSEC Kft. által kifejlesztett e-Szignó 3.1 minősített aláírás létrehozó és kezelő parancssori alkalmazás megbízható aláírás-létrehozó modulja megfelel a normatív dokumentumokban foglalt követelményeknek a vizsgált környezetben.

A megfelelés biztonsági garancia szintje megfelel a **Common Criteria** értékelési rendszere szerinti **EAL 3+** szintnek 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

Rövidítés	Tartalom
BE	Biztonsági Előirányzat - egy megvalósítandó termék biztonsági rendszerterve
CC	Common Criteria - MSZ ISO/IEC 15408 Az informatikai biztonság értékelésének közös szempontrendszere

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

Rövidítés	Tartalom
PP	Protection Profile – a Védelmi Profil eredeti, angol elnevezése
ST	Security Target – a Biztonsági Előirányzat eredeti, angol elnevezése
TOE	Target Of Evaluation – a Vizsgálat Tárgya eredeti, angol elnevezése
VP	Védelmi Profil – egy megvalósítandó termék általános, technológia-független leírása, követelményrendszere
VT	Vizsgálat Tárgya – az a termék, amelynek leírását és rendszertervét a BE (ST) tartalmazza

Dokumentum vége