MINŐSÍTETT TERMÉK

Tanúsítvány

Felülvizsgálati jegyzőkönyv

Felülvizsgálati jegyzőkönyv sz.: E-MS13T2_TAN.SW
Felülvizsgált tanúsítvány sz.: E-MS12T2_TAN.SW
Kelt: Budaörs, 2013. augusztus 12.

Szolgáltató/Megbízó: Microsec Zrt.
1031 Budapest, Záhony utca 7.
Graphisoft Park D épület

A termék megnevezése:

e-Szigno 3.2. Minősített aláírás létrehozó és kezelő megbízható modul Windows, Linux, Solaris, AIX és Mac OS X operációs rendszerre

A MATRIX Kft. tanúsítja, hogy*
a benyújtott dokumentációk és az elvégzett független tesztek alapján a
Microsec Zrt. által fejlesztett elektronikus aláírási termék továbbra is

megfelel

az alábbi normatív dokumentumokban foglalt 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;
- Nemzeti Média- és Hírközlési Hatóság E-Szolgáltatás-felügyeleti Osztály EF/26838-10/2011 határozata a felhasználható biztonságos kriptográfiai algoritmusokról, valamint a hozzájuk tartozó paraméterekről a mellékletekben foglaltaknak megfelelően;
- az Európai Parlament és a Tanács 1999/93/EK Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről;
- 114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól;
- Biztonsági Előirányzat az e-Szigno minősített aláírás létrehozó és kezelő megbízható modulhoz v1.1 (OID 1.3.6.1.4.1.21528.2.1.3.57);
- RFC 3275: XML-Signature Syntax and Processing;
- RFC 5652: Cryptographic Message Syntax;
- ETSI TS 101 903 V1.2.2, V1.3.2, V1.4.2: XML Advanced Electronic Signatures (XAdES); XAdES Baseline Profile v2.1.1 (2012-03)
- ETSI TR 102 038 XML format for signature policies. v1.1.1.;
- ETSI TS 101 733 CMS Advanced Electronic Signatures (CAdES). v1.8.1.; CAdES Baseline Profile, v2.1.1 (2012-03)
- ETSI TS 102 778-1,-2,-3, -4 PDF Advanced Electronic Signature Profiles; Part 1,2,3,4: PAdES Overview - a framework document for PAdES. V1.1.1; PAdES Basic - Profile based on ISO 32000-1, V1.2.1; PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles. V1.1.2.. PAdES Long Term - PAdES LTV Profile. V1.1.2 (2009-12)

Hodován Attila
Tanúsítási igazgató

Einetter Lajos
Ügyvezető igazgató

Érvényes: 2016. augusztus 11.
Melléklet: 12 oldal

*A MATRIX Kft. a 003/2012 számú Kijelölési Okiratban a nemzeti fejlesztési miniszter által kijelölt tanúsító szervezet.

TANÚSÍTVÁNY FELÜLVIZSGÁLATI JEGYZŐKÖNYV (E-MS13T2_TAN-SW) MELLÉKLETE

Dokumentumazonosító	**E-MS13T2_TAN-SW.ME-01**	
Projektazonosító	**E-MS13T2**	**Microsec Zrt. SW tanúsítás 2013**
MATRIX tanúsítási igazgató	**Hodován Attila**	
Kelt	**Budapest, 2013.08.12.**	
MATRIX tanúsítási igazgató		

1. BEVEZETÉS

A MATRIX Kft. a 9/2005. (VII. 21.) IHM rendeletnek megfelelően az elektronikus aláírási termékek tanúsítására a Miniszterelnöki Hivatalt Vezető Miniszter által 001/2009 számú okiratban kijelölt független tanúsító szervezet.

A Microsec Kft. elektronikus aláírási termékét, az e-Szignó modult 2004-től tanúsítja a MATRIX. A tanúsításra a Microsec és a MATRIX közös projektet indított.

Jelen tanúsítvány felülvizsgálat az NMHH által E-MS12T2_TAN-SW azonosítóval 2012-ben nyilvántartásba vett tanúsítvány megújítása.

Az elvégzett vizsgálatokról részletes szakterületi audit jelentések készültek, amelyekből a vizsgálat és a felhasználás körülményeire vonatkozó legfontosabb információkat jelen melléklet tartalmazza.

2. AZ ÉRTÉKELÉS TÁRGYA

Megnevezés: „e-Szignó 3.2 minősített aláírás létrehozó és kezelő megbízható modul Windows, Linux, Solaris, AIX és Mac OS X operációs rendszerekre"

2.1. Az ÉT azonosítása

Az ÉT egyértelmű azonosítása az alábbi adatok alapján lehetséges:

Jellemző	Érték
ÉT márkaneve	Microsec e-Szignó minősített aláírás létrehozó és kezelő megbízható modul
ÉT verzió	a tanúsításkor vizsgált termék verziója: 3.2.6.21.
Dátum	2013. 08. 12.
Fejlesztő	Microsec Kft.
Termék típus	Elektronikus aláírás létrehozó és ellenőrző modul

Platform	Windows, Linux, Solaris, AIX, Mac OS X
CC verzió	3.1
PP megfelelés	US Government Family of Protection Profiles Public Key-Enabled Applications For Basic Robustness Environments (v2.8, May 2007) profil családból származtatott PP
ST megfelelés	Biztonsági Előirányzat az e-Szignó minősített aláírás létrehozó és kezelő megbízható modulhoz v1.1 OID 1.3.6.1.4.1.21528.2.1.3.57

2.2. Az értékelés tárgyát képező komponensek és dokumentációk

Típus	Tárgy	Verzió	Megjelenés
Szoftver	Microsec e-Szignó minősített aláírás létrehozó és kezelő megbízható modul fájlcsomag (Win32, Linux, Solaris, AIX, Mac OS X)	3.2	Elektronikus állományok
Szoftver	Tesztesetek	1.0	Elektronikus állományok
Dokumentum	Tesztjegyzőkönyv az e-Szignó minősített aláírás létrehozó és kezelő megbízható modulhoz (v3.2.6.21)	1.0	DOC állomány
Dokumentum	Kiegészítés az e-Szignó minősített aláírás létrehozó és kezelő megbízható modulhoz (v3.2.6.21) készült tesztjegyzőkönyvhöz	1.0	DOC állomány
Dokumentum	Biztonsági előirányzat az e-Szignó minősített aláírás létrehozó és kezelő megbízható modulhoz	1.1	DOC állomány
Dokumentum	Fejlesztés - működési szabályzat	1.2	DOC állomány
Dokumentum	Fejlesztő nyilatkozata a biztonsági körülményekről	-	papír

A tanúsítás csak az alábbi konkrét szoftverkomponensekre vonatkozik:

eszigno-3.2.6.21-WinNT-i686-vc90-32bit:

Fájl	SHA-256 HASH	Méret(byte)
eszigno3.exe	FE7CA4978BB1324EE41298988846AF2EE0 8594FA07C19D761FDC077B056CC4B5	1 073 152
XadesSigner.dll	8B85DDD4F98AD514EB2EB58E17888E3C E68C8F1B74E11708AFF5C17E0A9E20E3	7 329 792
XadesSignerLoc ale_ENG.dll	3A48DADAE359C57E5788500A424901094 C70D6ACA4412930510B2D2D5222BFED	46 592
XadesSignerLoc ale_HUN.dll	A377152B890ACC73A02915B118FB84FE22 8108C36295B7034ECD38383DBD495C	52 736
XadesSignerLoc ale_GER.dll	2CC125899B6E7370B41293F5305C41A770 95F377504AAD2335C449228EAABAAC	52 224
mscpdf.jar	95E17F13AF3ECAB8778E4861CCAFCEF5 E2E477BDEF824DEEB7E9D65D7427E77F	109 386

eszigno-3.2.6.21-SunOS5.8-sparc-sw-32bit:

Fájl	SHA-256 HASH	Méret(byte)
eszigno3	2349206AFF4AC62815949B070A159C880E B713CE75A3A26F6F54CEED283CE1BB	1 464 776
libxadessigner.so	7F7F390767B49218C8F3785DA87CAAB12 C16DB7A7FCCDF35DCA25B883F44FE08	19 099 972
libxadessignerlocale_eng.s o	6A0AFB92EBF58534490F5FFF814A11CE45 AD73EF9918AD2F7BCAE4BEEAD2F6E9	51 060
libxadessignerlocale_ger.so	0C5392BAAD4774BC1CB7BE79ACC399D8 2BDB3657FE0ED987877EE872F1FDFE89	56 376
libxadessignerlocale_hun.s o	94160882228B2A969870CBB29C2BC548A3 BAB4DC0C0E694C91093F3B2645B412	57 372
mscpdf.jar	52DEAF00D28808AD4A9C421E676FC5BBD 86401543D6F80C146E68732ECE50FE6	109 386

eszigno-3.2.6.21-Linux2.6-x86_64-gcc33-64bit:

Fájl	SHA-256 HASH	Méret(byte)
eszigno3	B88C76569BA281CBDB0CF5FD08366C2F BCF2872E64A122B9759E851FE6D96F86	1 145 260
libxadessigner.so	4C33D7164EB4CBE02CA44627CAA962E53 0E12E6BA2548384800C24D2C8DC9295	13 375 299

libxadessignerlocale_eng.	3D7AF3AEE078415B5207203BD1B4C65E71544CA8DE816131993DBE12308163EF	69 899
libxadessignerlocale_ger.	F5F04C9E762AAF909628707421538F6292419C9250AF5DBDAC1D43787B60042F	73 995
libxadessignerlocale_hun.	E372E34F61F987B6B1DEAEF335E72B76AC267D03FFC0D6DD630496E906CB81AF	74 538
mscpdf.jar	52DEAF00D28808AD4A9C421E676FC5BBD86401543D6F80C146E68732ECE50FE6	109 386

eszigno-3.2.6.21-Linux2.6-i686-gcc41-32bit:

Fájl	SHA-256 HASH	Méret(byte)
eszigno3	2B52B753D8C2CC144DA67B9754F1B8E8EA7DFA6915DFD7BCBA829F0385F1FC1C	1 138 731
libxadessigner.so	2B52B753D8C2CC144DA67B9754F1B8E8EA7DFA6915DFD7BCBA829F0385F1FC1C	14 849 103
libxadessignerlocale_eng.so	23B19C29FF7D6B2B53D990B892DB089C81DD6AECE8CDB11C944AB1040AE4FE9D	48 781
libxadessignerlocale_ger.so	494D6470CA54C856A377DDA342A4D2B1FA98AD7D2996B4B3C1A43CE0FEFA1C02	56 717
libxadessignerlocale_hun.so	BD2971B5509D24499E5B803457281D88E862ED4DD6BD08F68B9820B4632BE6FE	56 716
mscpdf.jar	52DEAF00D28808AD4A9C421E676FC5BBD86401543D6F80C146E68732ECE50FE6	109 386

eszigno-3.2.6.21-Linux2.4-i686-gcc32-32bit:

Fájl	SHA-256 HASH	Méret(byte)
eszigno3	1174D7D77EF562F5227146D87353145B1BDB5347E1B7E9AD3497AAAA7FE82611	1 630 682
libxadessigner.so	3D3F8EDD863D813AB7F790C97B078E1A2A7432448147D350904CBD3C2475832D	16 630 931
libxadessignerlocale_eng.	D3CB8B6975847211C7B27B2B019559D55C90A83DE040FDAA09CE903FE8DC16AF	55 961
libxadessignerlocale_ger.	B8A9AA1C6E647CBFAC7214CF71863E941FAD1710FC1034C315727CA03BF62571	64 153
libxadessignerlocale_hun.	8F0AA18748DA9E1E6E57E032E1431F40C13D0BC85A7A43ABC541723B77A479D1	64 152

mscpdf.jar	52DEAF00D28808AD4A9C421E676FC5BB D86401543D6F80C146E68732ECE50FE6	109 386

eszigno-3.2.6.0-Darwin10.8.0-i386--64bit:

Fájl	SHA-256 HASH	Méret(byte)
eszigno3	DCBCE0F41DC4216CA278911669AEBBDE 4D0F916D87BCDBDAAAAACF700DB2E089	974 704
libxadessigner.so	28B71EF4102F64CEB64DD635E9153B64E 24E0665F5AA728B795E6268CF2E51FB	12 116 168
libxadessignerlocale_eng.so	BAF5816B8DBBAA4ABB8F79B8A3D8DAEC 0A275CA0436268C591AA8F2387FDED8E	45 376
libxadessignerlocale_ger.so	E2E0EE79F26A9E413C57D5CE283A5A165 1789D27EA0A49D7DDCBC4D0ACD8330B	53 568
libxadessignerlocale_hun.so	6F9B53470F291A55B8EC9AFF19BC6027C FF721AC6A7DB8267C7B4B1B356490C1	53 568
mscpdf.jar	20F815D24880BAEC14DC0D8B7BBCD57B 068B0A0AF81ADCEACAF4F3594745B27B	108 893

eszigno-3.2.6.21-AIX5.3-powerpc-xlc-64bit:

Fájl	SHA-256 HASH	Méret(byte)
eszigno3	DCFE50946ABD2BC5BC3EB06EF4A81D6A 7337675238414070C13FB3D6A417D1E0	3 163 031
libxadessigner.so	BE77A884EBEA1DF2B152C29613EF262A3 EEDB36CBF880431727E000FF296CAD5	53 592 675
libxadessignerlocale_eng.so	63689AC09471E5A7DF11CFBA3F0B9EC34 BA1C64CD56AB752397048D85F746ACA	65 227
libxadessignerlocale_ger.so	CE9299FE7024947696ED1577B31C2EA18A B5BC2368DD99961C03F5D765E307DA	70 539
libxadessignerlocale_hun.so	D6F2DFAA026157E1206FF06BF196F3E423 909A739C4D5927F42C67A527FBD8BF	71 154
mscpdf.jar	52DEAF00D28808AD4A9C421E676FC5BBD 86401543D6F80C146E68732ECE50FE6	109 386

2.3. A tanúsítás megrendelője

Az Értékelés Tárgyát képező elektronikus aláírási termék fejlesztője és a tanúsítás megrendelője: Microsec Zrt.

1031 Budapest, Záhony u. 7. Graphisoft park D épület, info@e-szigno.hu

3. FUNKCIONÁLIS LEÍRÁS

Az e-Szignó minősített aláírás létrehozó és kezelő megbízható modul (e-Szignó MM vagy ÉT) az elektronikus aláírások létrehozására és kezelésére kifejlesztett funkcionalitás halmaz. Az elektronikus aláírással kapcsolatos műveleteken kívül (aláírás létrehozás, ellenőrzés, érvényesítési adatok beszerzése, ellenőrzése és azok aláíráshoz csatolása) alkalmas az elektronikus dokumentumokkal való munkavégzést leginkább támogató e-akták kezelésére. Segítségével az egyes elemeket (e-aktákat, dokumentumokat, aláírásokat, ellenjegyzéseket) – a felhasználási területnek megfelelő, az ügykezelést megkönnyítő – kiegészítő információkkal láthatjuk el. Lehetőség nyílik átvételi elismervény kérésére és készítésére, valamint a dokumentumok és e-akták titkosítására és visszafejtésére is. Képes továbbá az igazoltan egy adott szerepkörben tett aláírások készítésére is (attribútum tanúsítványok kezelése).

Az e-Szignó minősített aláírás létrehozó és kezelő megbízható modul felhasználásával könnyedén készíthetőek elektronikus aláírást felhasználó rendszerek, alkalmazások. Az e-Szignó MM használható WindowsXP, Windows Server 2003 és 2008, Windows Vista, Windows CE, Windows 7, Windows 8, Unix, Linux, Solaris, AIX és MAC OS X környezetben, 32 és 64 biten is. Funkcionalitásai elérhetőek standard C felületen, JAVA programozói felületen és COM csatoló felületen keresztül, de létezik parancssoros változata is. A Windows platformra készített, grafikus felhasználói felülettel kiegészített e-Szignó alkalmazás Magyarországon széles felhasználói körnek örvend.

Az e-Szignó MM alapértelmezett esetben az RFC 3275 (XMLSignature) és az erre épülő ETSI TS 101 903 V1.3.2. (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 és kezelésére is, így lehetővé téve például tetszőleges XML dokumentum tetszőleges csomópontjának aláírását (beágyazott aláírás) vagy nagy méretű dokumentumok aláírását oly módon, hogy maga az aláírás állomány ne tartalmazza a dokumentumot (különálló aláírás). Támogatja a XAdES 1.2.2-es és 1.4.2-es verzióit is [XAdES 1.2.2, XAdES 1.4.2], és megfelel a XAdES-BP-nek. Támogatja az RFC 5652 (CMS aláírás) és az erre épülő ETSI TS 101 733 V1.8.1. (CAdES – CMS Advanced Electronic Signatures) ajánlásoknak megfelelő aláírás létrehozását és ellenőrzését is, és megfelel a CAdES-BP-nek. Mindezeken kívül képes az ETSI TS 102 778-1,2,3,4 (PAdES – PDF Advanced Electronic Signature) ajánlások által definiált PDF aláírások létrehozására és kezelésére is, és megfelel a PAdES-BP-nek. Támogatja az ETSI TS 102 918 v 1.2.1. (ASiC – Associated Signature Containers) ajánlásnak megfelelő aláírások létrehozását is, megfelel az ASiC-BP-nek. Képes aláírással ellátni az ODF dokumentumokat. Alkalmas továbbá MELASZ-ready 1.0 és 2.0 aláírások létrehozására is, és képes megfelelően kezelni a más aláírás-létrehozó alkalmazás által, a fenti szabványoknak megfelelően készített aláírásokat is. Megfelel továbbá a közigazgatás számára előírt aláírás formátumnak is. Segítségével készíthetünk az RFC 3281 és az erre épülő ETSI TR 102 044 ajánlásnak megfelelő attribútum tanúsítványt is.

Az aláírások RSA-SHA2 (SHA224, SHA256, SHA384 vagy SHA512, alapértelmezetten SHA256) algoritmussal készülnek. A minősített elektronikus aláírás elkészítése minden esetben egy személyhez rendelt biztonságos aláírás-létrehozó eszköz (BALE) segítségével történik; fokozott biztonságú aláírás létrehozása a 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, a tanúsítvány-lánc felépítését és

ellenőrzését is elvégzi. A beszerzett adatok csatolásával képes -EPES, -T, -C, -X-L és -A típusú aláírások létrehozására vagy egy korábban létrehozott aláírás kibővítésére. Kezeli az attribútum tanúsítványokat és támogatja az ETSI TR 102 038 v1.1.1 ajánlásnak megfelelő aláírási szabályzatok használatát is.

Lehetőséget nyújt a beillesztett dokumentumok, illetve az egész e-akta RSA-DES3 algoritmussal, PKCS #7 formátumban történő titkosítására és azok visszafejtésére. További funkcionalitása a beillesztett dokumentumok ZIP tömörítése. Lehetőséget nyújt az időbélyeg szolgáltatóhoz a felhasználónév/jelszó alapú és a tanúsítvány alapú azonosításra is, valamint a közigazgatásban alkalmazott viszontazonosítási protokollnak megfelelő adategyeztetésre. A hiba- illetve analitikus üzenetek több nyelven (magyar, angol, német) is elérhetőek.

Az ÉT a következő külső (a tanúsítás tárgyát nem képező) modulok funkcionalitását használja fel Windows platformon:

- MimeChecker.dll
- MimeCheckerLocale_HUN.dll
- MimeCheckerLocale_ENG.dll
- MimeCheckerLocale_GER.dll
- MFC90.dll
- MFC90u.dll
- msvcp90.dll
- msvcr90.dll
- bcprov.jar
- iText.jar
- xsign.dll
- XSign4COM.dll
- Xsign4java.dll
- Xsign4java.jar
- eszigno3.exe

Az ÉT a következő külső (a tanúsítás tárgyát nem képező) modulok funkcionalitását használja fel Linux, Solaris, AIX platformokon:

- bcprov.jar
- iText.jar
- libstdc++.so (GCC)
- libxsign.so
- libxsign4java.so
- xsign4java.jar
- eszigno3

4. MEGFELELŐSÉG

4.1. Megfelelőség a normatív dokumentumoknak

Az ÉT megfelel az alábbi követelményeknek:

4.1.1. Kötelezően betartandó 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;
- Nemzeti Média és Hírközlési Hatóság E-Szolgáltatás-felügyeleti osztály EF/26838-x/2011 határozata a felhasználható biztonságos kriptográfiai algoritmusokról, valamint a hozzájuk tartozó paraméterekről a mellékletekben foglaltaknak megfelelően;

4.1.2. Önként vállalt normatívák

A vizsgálat során azt kell megállapítani, hogy a vizsgálat tárgya mennyiben felel meg a fejlesztő által önként vállalt alábbi normatíváknak:

MATRIX által bevizsgálandó normatívák:

- Az Európai Parlament és a Tanács 1999/93/EK számú Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről,
- 114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól;
- Biztonsági Előirányzat az e-Szignó minősített aláírás létrehozó és kezelő megbízható modulhoz v1.1 (OID 1.3.6.1.4.1.21528.2.1.3.57)

A fejlesztő, vagy más szervezetek által igazolandó megfelelések:

- RFC 3275: XML-Signature Syntax and Processing,
- ETSI TS 101 903 V1.2.2 és V1.3.2 és 1.4.2: XML Advanced Electronic Signatures (XAdES),
- ETSI TS 103 171 Electronic Signatures and Infrastructures (ESI);XAdES Baseline Profile v2.1.1 (2012-03)
- ETSI TR 102 038 XML format for signature policies, v1.1.1.,
- ETSI TS 101 733 CMS Advanced Electronic Signatures (CAdES), v1.8.1.,
- ETSI TS 103 173 Electronic Signatures and Infrastructures (ESI);CAdES Baseline Profile, v2.1.1 (2012-03)
- ETSI TS 102 778-1-2-3-4 PDF Advanced Electronic Signature Profiles; Part 1,2,3,4: PAdES Overview - a framework document for PAdES, V1.1.1; PAdES Basic - Profile based on ISO 32000-1, V1.2.1; PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles, V1.1.2., PAdES Long Term - PAdES LTV Profile, V1.1.2 (2009-12)

- ETSI TS 103 172 Electronic Signatures and Infrastructures (ESI);PAdES Baseline Profile, v2.2.1 (2012-10)
- ETSI TS 102 918 v 1.2.1. Associated Signature Containers (ASiC), v1.2.1 (2012-02)
- ETSI TS 103 174 Electronic Signatures and Infrastructures (ESI);ASiC Baseline Profile, v2.1.1 (2012-03)

A MATRIX által validált tesztekkel alátámasztott megfelelés normatívája a MATRIX által kiadott tanúsítványon feltüntetésre kerül.

Az aláírási termék megfelel a fenti követelményeknek a 4.2 pontban leírt működési környezetben az alábbi feltételek teljesülése mellett:

A tanúsítás kizárólag a bevizsgált rendszerre vonatkozik, bárminemű változtatás esetén a módosított verzióra jelen tanúsítás érvénytelen.

Nem képezi a tanúsítás tárgyát a program működési környezete, így az

- operációs rendszer,
- a felhasznált külső szoftver modulok illetve programok,
- a működéshez szükséges hardver elemek.

4.2. Működési környezet

A fenti megfelelőség feltétele az alábbi működési környezetre vonatkozó követelményrendszer teljesülése, amelynek betartása a felhasználó felelőssége. Mivel az ÉT-t nem önálló működésre tervezték, tipikus felhasználása esetén egy programfejlesztő integrálja saját elektronikus aláíró vagy ilyen funkcionalitással is rendelkező alkalmazásába. Az alkalmazás fejlesztésénél figyelembe kell venni az alábbi feltételeket, amelyek betartása szükséges a modul helyes és biztonságos működéséhez.

4.2.1. Hardver és szoftver környezet

A vizsgált aláírási termék csak olyan környezetben használható elektronikus aláírások létrehozására, amelynek minden eleme kielégíti az általánosan 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 alkalmazás megfelelő használatához.

4.2.1.1. Operációs rendszer

Az ÉT az alábbi 32 és 64 bites operációs rendszereken használható:

Microsoft Windows XP, Windows CE

Microsoft Windows Server 2003 és 2008,

Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows 8,

Linux,

Sun Solaris,

IBM AIX,

Mac Os X.

4.2.1.2. Egyéb program komponensek

Az ÉT működéséhez szükséges egyéb komponensek:

- Java Runtime Environment és Software Development Kit (PDF aláírás esetén)
- Visual C++ 2008 futásidejű komponensek (csak Windows környezetben)
- Víruskereső szoftver, amely képes megvédeni a modul és az egyéb felhasznált komponensek integritását, de legalább képes jelezni az integritás sérülését

Az egyes programokat, program komponenseket megfelelően biztonságos forrásból kell beszerezni, a telepítés és üzemeltetés során pontosan be kell tartani a telepítési és felhasználói útmutatóban megfogalmazott utasításokat, követelményeket.

4.2.1.3. Hálózati működés

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

4.2.2. A fizikai védelem

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

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

4.2.3. Szállítás és telepítés

Az alkalmazás telepítésével kapcsolatos biztonsági előírások:

- A program telepítőkészletét nem módosítható, biztonságos adathordozón kell a felhasználónak átadni. Az átadás-átvételt hitelt érdemlő módon igazolni kell az átadás pontos időpontjának rögzítésével. A felhasználók az internetről is letölthetik a terméket, ebben az esetben biztosítani kell számukra az ellenőrzési lehetőséget, hogy a program megbízható forrásból származik.
- A telepítést csak a megfelelően előkészített, biztonságos környezetben szabad megkezdeni, a telepítési útmutatóban rögzített lépések pontos betartásával.
- A terméket ajánlott rendszeresen frissíteni az új verziókra.

4.2.4. Algoritmusok és kapcsolódó paraméterek

Az alkalmazás csak a mindenkor érvényes szabályzásnak megfelelő algoritmusokkal és paraméterekkel használható. Az elektronikus aláíráshoz használható kriptográfiai algoritmusokat egységesen szabályozzák az Európai Unióban, aktuális információ az alábbi normatívákból nyerhető:

- Nemzeti Média és Hírközlési Hatóság E-Szolgáltatás-felügyeleti osztály EF/26838-x/2011 határozata a felhasználható biztonságos kriptográfiai algoritmusokról, valamint a hozzájuk tartozó paraméterekről a mellékletekben foglaltaknak megfelelően;

- ETSI TS 102 176-1 Algorithms and Parameters for Secure Electronic Signatures

A specifikációk rendszeresen megújításra kerülnek, ezért a felhasználónak folyamatosan figyelemmel kell kísérnie az elektronikus aláírás létrehozatalához használható kriptográfiai algoritmusokra vonatkozó normatívák változását, s az annak megfelelő algoritmusokat és paramétereket kell használnia.

4.3. Értékelési módszertan

Az értékelés nyelvezete a Közös Szempontrendszerben meghatározott, az értékelés módszertanának alapját a Közös Szempontrendszerhez használt módszertani ajánlás képzi.

A tanúsítási eljárás során elvégzett, fejlesztőktől független értékelő vizsgálat a Common Criteria szerinti EAL3+ szinthez hasonló volt. Az EAL3 jelentős garancianövekedést jelent az EAL2-höz képest azzal, hogy a biztonsági funkciók és mechanizmusok és/vagy eljárások vizsgálatának sokkal teljesebb lefedettségét követeli, ami bizonyos mértékű bizalmat teremt abban, hogy a fejlesztés során a TOE-t nem hamisítják meg.

4.4. Biztonsági garancia szint

A MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. igazolja, hogy a MICROSEC által kifejlesztett „e-Szignó 3.2 minősített aláírás létrehozó és kezelő megbízható modul Windows, Linux, Solaris, AIX és Mac OS X operációs rendszerekre” azonosítójú elektronikus aláírási termék megfelel a normatív dokumentumokban foglalt követelményeknek a vizsgált környezetben és felhasználható minősített és fokozott biztonságú elektronikus aláírások létrehozására, az aláírások érvényességének ellenőrzésére.

A megfelelés biztonsági garancia szintje a Common Criteria értékelési rendszere szerinti EAL 3+ szinthez hasonló, ami a fejlesztőktől függetlenül garantált biztonság mérsékelt szintjét jelenti.

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

5. HIVATKOZÁSOK

Az Értékelési Jelentésben a következő dokumentumokra hivatkoztunk:

Szám	Dokumentum
[1]	MELASZ Munkacsoport Megállapodás, v2.0, 2008 december, Egységes MELASZ formátum elektronikus aláírásokra
[2]	ETSI TS 101 903 V1.4.1 (2009-06), XML Advanced Electronic Signatures (XAdES)
[3]	Network Working Group, RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[4]	Network Working Groups, RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
[5]	ETSI TS 101 861 V1.3.1 (2006-01), Time stamping profile

6. RÖVIDÍTÉSEK

Az Értékelési Jelentésben a következő rövidítéseket használtuk általános jelleggel:

Rövidítés	Magyarázat
ALE	Aláírás Létrehozó Eszköz – olyan hardver, illetve szoftver eszköz, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza (Eat. 2. § 3.)
BE	Biztonsági Előirányzat – egy megvalósítandó termék biztonsági rendszerterve
CC	Common Criteria for Information Technology Security Evaluation – Az informatikai biztonság értékelésének közös szempontrendszere
DSS	DSS Consulting Kft., az elektronikus aláírási termék fejlesztője
Eat.	2001. évi XXXV. törvény az elektronikus aláírásról
ÉT	Értékelés Tárgya – az a termék, amelynek leírását és rendszertervét a BE (ST) tartalmazza
MATRIX	MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft., a tanúsító szervezet
PP	Protection Profile – a Védelmi Profil eredeti, angol elnevezése
ST	Security Target – a Biztonsági Előirányzat eredeti, angol elnevezése
TOE	Target Of Evaluation – az Értékelés Tárgya eredeti, angol elnevezése
VP	Védelmi Profil – egy megvalósítandó termék általános, technológia-független leírása, követelményrendszere
VT	Vizsgálat Tárgya (ld. ÉT)