MATRIX

MINŐSÍTETT TERMÉK

# Tanúsítvány

Tanúsítvány száma: E-MS12T2_TAN.SW
Kelt: Budaörs, 2012. július 13.

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 alapján a***
**Microsec Zrt. által kifejlesztett elektronikus aláírási termék**

## 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-x/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-Szignó minősített aláírás létrehozó és kezelő megbizható modulhoz v1.0 (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: XML Advanced Electronic Signatures (XAdES);
- 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 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)

Hornyák Gábor
Tanúsítási igazgató

Einetter Lajos
Ügyvezető igazgató

Érvényes: 2015. július 12.
Melléklet: 12 oldal

*A MATRIX Kft. a 001/2009 számú Kijelölési Okiratban a Miniszterelnöki hivatalt vezető miniszter által kijelölt tanúsító szervezet.

# TANÚSÍTVÁNY (E-MS12T2_TAN-SW)

# MELLÉKLETE

| | | |
|---|---|---|
| Dokumentumazonosító | **E-MS12T2_TAN-SW.ME-01** | |
| Projektazonosító | **E-MS12T2** | **Microsec Zrt. SW tanúsítás 2012** |
| MATRIX tanúsítási igazgató | **Hornyák Gábor** | |
| Kelt | **Budapest, 2012.07.13.** | |
| …….<br>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.

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: 3.2.6.0. |
| **Dátum** | 2012. 06. 21. |
| **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 v1.0<br>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 (v3.2.6.0) | 1.1 | DOC állomány |
| Dokumentum | Kiegészítés az e-Szignó minősített aláírás létrehozó és kezelő megbízható modulhoz (v3.2.6.0) készült tesztjegyzőkönyvhöz | 1.0 | DOC állomány |
| Dokumentum | Biztonsági előirányzat az e-Szignó minősített aláírás létrehozó és kezelő megbízható modulhoz | 1.0 | DOC állomány |
| Dokumentum | Fejlesztés működési szabályzat | 1 | DOC állomány |
| Dokumentum | Fejlesztő nyilatkozata a biztonsági körülményekről | - | papír |

A tanúsítás csak az alábbi konkrét szoftverkomponensekre vonatkozik:

**eszigno-3.2.6.0-WinNT-i686-vc90-32bit:**

| Fájl | SHA-256 HASH | Méret(byte) |
|---|---|---|
| eszigno3.exe | 1FAE699A4C2191F3DB2EF7E9D572AB31A04DCE4E86C7FA1319611455AC4BAE48 | 1 030 144 |
| XadesSigner.dll | 8AD0F4267B91FA1119D2F1AD6AEEE02A18F649C07087BD65AF0D23763E58EDEF | 7 163 392 |
| XadesSignerLocale_ENG.dll | 861C8D085396545007136A8BFD1D062476E08C2A4F456A8169ED40BDE92306CB | 46 592 |
| XadesSignerLocale_HUN.dll | 40923921F64335AD32F8ACC368B3188A5D8EA63D43E8E98D8EE1A294A2C4D99D | 52 736 |
| XadesSignerLocale_GER.dll | 1052AD88BC80695143607F7D056410C1843F093A94E88C4CD62EC4818A6E58EF | 51 712 |
| mscpdf.jar | 5D682463E2C218DECF5175F315AC3AFA8C99C95151C894E6B8ECD8306E768B26 | 108 893 |

**eszigno-3.2.6.0-SunOS5.8-sparc-sw-32bit:**

| Fájl | SHA-256 HASH | Méret(byte) |
|---|---|---|
| eszigno3 | 5D5A215DE647DF1A346664EA9D87EDDF823111E7DD9955D015480D27C3564A66 | 1 403 316 |
| libxadessigner.so | 8D8E01494CB1918F9F4ACFDCF68C46EE059AAD17F4499544336449A7375A385A | 18 677 596 |
| libxadessignerlocale_eng.so | 80FC41A13ACCB4F9E45BD4BE8FB676E5E69F112B1B9EE656E3C0D24CE3FB0E57 | 50 772 |
| libxadessignerlocale_ger.so | AC0DB5D70525F65D6DD06B611ADB61807BD642CC9FDDFC9118B02B327BC15515 | 56 064 |
| libxadessignerlocale_hun.so | A125D3B893FF23A33196C3CCFDC0CEBCDBE1A166641BE0C33234A106EEE318EB | 56 952 |
| mscpdf.jar | 20F815D24880BAEC14DC0D8B7BBCD57B068B0A0AF81ADCEACAF4F3594745B27B | 108 893 |

**eszigno-3.2.6.0-Linux2.6-x86_64-gcc33-64bit:**

| Fájl | SHA-256 HASH | Méret(byte) |
|---|---|---|
| eszigno3 | 9D68F3371F0DB71B25889385DFEA4CFC1E95DC68151C262046C1D14DD9C7EBFE | 1 092 371 |
| libxadessigner.so | 2EDF95D86E64BDAFE534E2729BA026EF915052802B65434CFA4B9991024B7697 | 13 225 663 |

| | | |
|---|---|---|
| libxadessignerlocale_eng. | 20E369BBF35D00F0765233A7E70BAE2C87BEA715416B130D6E2386239FF3D9D4 | 69 851 |
| libxadessignerlocale_ger.s | 4B3E9CCC5C8EA40CEAE339A7CDA8A8710539B4482C6576B50F3BA1286709003A | 73 947 |
| libxadessignerlocale_hun. | 4E8AA56D7441F96075F91A06DD6656EF4679D09E635E6384259BA3DAAE37E770 | 73 978 |
| mscpdf.jar | 20F815D24880BAEC14DC0D8B7BBCD57B068B0A0AF81ADCEACAF4F3594745B27B | 108 893 |

**eszigno-3.2.6.0-Linux2.6-i686-gcc41-32bit:**

| Fájl | SHA-256 HASH | Méret(byte) |
|---|---|---|
| eszigno3 | 2F8F8EB8839677DE8DF82DA3B10DA6D6BB477F512FAA4B4298C10C1CDA7F9779 | 1 034 097 |
| libxadessigner.so | 232DC58578E2DFB74A95294F138ED79D69E769810484AA7BAC5847DBC5BFA078 | 14 698 523 |
| libxadessignerlocale_eng.so | AB1853F4BE3844A606BF1A71E03F66D19CA1460AB383E32E046DFCC06166104D | 48 501 |
| libxadessignerlocale_ger.so | 80A7013F85F61BCAF9DA1AB7C867320374E3BEBEE67527449FF380B1298E3ED5 | 56 693 |
| libxadessignerlocale_hun.so | D4010DB7B8B4374B9AB8DB403C2D3EC909BE951473D5C63269B23E8F262A4CE8 | 56 692 |
| mscpdf.jar | 20F815D24880BAEC14DC0D8B7BBCD57B068B0A0AF81ADCEACAF4F3594745B27B | 108 893 |

**eszigno-3.2.6.0-Linux2.4-i686-gcc32-32bit:**

| Fájl | SHA-256 HASH | Méret(byte) |
|---|---|---|
| eszigno3 | 308B1C1C999A605AF52C793C1B96E46103D6EABFAE74DC823F64FCCC50F43D2B | 1 539 022 |
| libxadessigner.so | E260C6F59F7C6941F8ACD6CEA5270B0EE0B755EDD4F9841C6FC6E919F72889B2 | 16 432 533 |
| libxadessignerlocale_eng. | 185574A2B759CF9A90103BD6885549B35D009E1859BC1320C610FEA0F968BC06 | 55 937 |
| libxadessignerlocale_ger.s | 2C27DFE196B3B8FDA73EEE3230BDD1AD70F363EE8F8335DB5C3F5C9BD094808A | 64 129 |
| libxadessignerlocale_hun. | 88B24E38F10BA5C5E5EFE97135EC2DB8A354B2D0D6CC35181CA0051C0448CE3A | 64 128 |

| | | |
|---|---|---|
| mscpdf.jar | 20F815D24880BAEC14DC0D8B7BBCD57B<br>068B0A0AF81ADCEACAF4F3594745B27B | 108 893 |

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

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

**eszigno-3.2.6.0-AIX5.3-powerpc-xlc-64bit:**

| Fájl | SHA-256 HASH | Méret(byte) |
|---|---|---|
| eszigno3 | 604ADC37F15C5B6A1494A13CFC8B4390F<br>F97AF185C415B920F9A3195B07B4E0D | 4 753 792 |
| libxadessigner.so | 262224C78105494259D22BC912F75ECA57<br>82FEDB21DBA7C0D0F17C2A2CCA075A | 60 903 653 |
| libxadessignerlocale_eng.so | 19D0099B9226D1F4C3B677A8E0B731D7D<br>68E78D5C40A12847B537E4B4185BB04 | 64 791 |
| libxadessignerlocale_ger.so | EECC32EB3FA43A32EF08D5A67393597C8<br>FE629918B43C42E7D94ABC7C03601AF | 70 071 |
| libxadessignerlocale_hun.so | 0010328E3856BF28FA427FA540316487072<br>28E838FE0738991F77BA3779A87A7 | 70 582 |
| mscpdf.jar | 20F815D24880BAEC14DC0D8B7BBCD57B<br>068B0A0AF81ADCEACAF4F3594745B27B | 108 893 |

### *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, 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 V1.2.2. (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 és kezelésére is, így lehetővé téve például tetszőleges XML dokumentum tetszőleges csomópontjának aláírását (beágyazott aláírás) vagy nagyméretű dokumentumok aláírását oly módon, hogy maga az aláírás állomány ne tartalmazza a dokumentumot (különálló aláírás). Támogatja a XAdES 1.3.2-es verzióját is. 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. 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. 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 v1.0 (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: XML Advanced Electronic Signatures (XAdES),
- 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 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)

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,

Microsoft Windows Server 2003 és 2008,

Microsoft Windows Vista,

Microsoft Windows 7,

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,<br>Egységes MELASZ formátum elektronikus aláírásokra |
| **[2]** | ETSI TS 101 903 V1.4.1 (2009-06),<br>XML Advanced Electronic Signatures (XAdES) |
| **[3]** | Network Working Group, RFC 5280,<br>Internet X.509 Public Key Infrastructure<br>Certificate and Certificate Revocation List (CRL) Profile |
| **[4]** | Network Working Groups, RFC 2560,<br>X.509 Internet Public Key Infrastructure<br>Online Certificate Status Protocol - OCSP |
| **[5]** | ETSI TS 101 861 V1.3.1 (2006-01),<br>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) |