TANÚSÍTVÁNY (E-MS09T_TAN-SW) MELLÉKLETE

Dokumentumazonosító	**E-MS09T_TAN-SW.ME-01**	
Projektazonosító	**E-MS09T**	**Microsec Kft. SW tanúsítás 2009**
MATRIX tanúsítási igazgató	**Szádeczky Tamás**	
Kelt	**Budapest, 2010.08.12.**	
	……. 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. Verzióváltás miatt ismételt tanúsítás vált szükségessé. 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 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	3.2
Dátum	2010. 05. 26.
Fejlesztő	Microsec Kft.
Termék típus	Elektronikus aláírás létrehozó és ellenőrző modul
Platform	Windows, Linux, Solaris, AIX
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 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)	3.2	Elektronikus állományok
Szoftver	Tesztesetek	1.0	Elektronikus állományok
Dokumentum	Tesztjegyzőkönyv az e-Szignó minősített aláírás létrehozó és kezelő megbízható modulhoz (v3.2.1.0)	1.0	DOC állomány
Dokumentum	Kiegészítés az e-Szignó minősített aláírás létrehozó és kezelő megbízható modulhoz (v3.2.1.0) készült tesztjegyzőkönyvhöz	1.0	DOC állomány
Dokumentum	Biztonsági előirányzat az e-Szignó minősített aláírás létrehozó és kezelő megbízható modulhoz	1.0	DOC állomány
Dokumentum	Szoftverfejlesztés, szoftver üzemeltetés, szolgáltatások nyújtása minőségügyi eljárás	5	DOC állomány
Dokumentum	Fejlesztő nyilatkozata a biztonsági körülményekről	-	papír

A tanúsítás csak az alábbi konkrét szoftverkomponensekre vonatkozik:

Windows platform

Név	Verzió	Méret	Sha-256 Lenyomat
XadesSigner.dll	3.2.1.0	5 665 792	565c5589174ceb66059f8b897cf46775c3b93e9765dcb52f607b006759a12f8e
XadesSignerLocale_ENG.dll	3.2.1.0	46 080	11de220c1407ec261ad3cc73f2e4c8cc73f1f0b703b8bd7514ba40b87e219d05
XadesSignerLocale_GER.dll	3.2.1.0	51 712	e18eca42eb2b9c6322c75cb4959dcc0acfbc3f0e8111147cc20352992c8f6895
XadesSignerLocale_HUN.dll	3.2.1.0	52	0ac659b00aa01034da77a4d1d412d84899b30ce5a6e7ecda

		224	d6b110e48cdd6f50
mscpdf.jar	-	267 362	6ed0c3d7ce628f6f254f8b7c22 e408fdc3dbcf700fb4e567dc8fc d3f9ff1694c

Linux platform

Név	Méret	Sha-256 Lenyomat
libxadessigner.so	14 916 542	c5a2703f21fdd097433519e1a56ec 2e9fa5a6e1fbfa4f49e1b3bf4a0b60 ca536
libxadessignerlocale_eng.so	55 905	38ceffdc4a7a3e2635a8defc5c10a 3b68ead6c6e34e47111d6eb732b1 1ba72d4
libxadessignerlocale_ger.so	64 097	2d2bc9f14dc2991987206b5b69d9 b24d156314069017635a47a96992 3e37d80f
libxadessignerlocale_hun.so	64 096	3ed49a74a2fa218206d606b75e82 d484f0e7cf113f5d2090db5db1c69 b93dd41
mscpdf.jar	267 361	0ccf1c38e4f7c2677ae02cc9b0928 b96b505dcab68faeba8c2603bbe2 bafb5a6

Solaris platform

Név	Méret	Sha-256 Lenyomat
libxadessigner.so	17 040 124	883641ec37da9ac3078306a7c4b6 443885773e34918b8f42ad1338da de8402b4
libxadessignerlocale_eng.so	50 456	f9a445f0a863c93707b0eee95401f 5892aafb8963a94acc6a9e865089 089fe60
libxadessignerlocale_ger.so	55 692	503eda10136dad410a37ba2a6155 f4aa5297f654a07016d322793648c 2ba7cf1
libxadessignerlocale_hun.so	56 564	487a20e0c11b916c3fc860ab1194 0ef840562ea3debd91803a8532e6 309f65fe
mscpdf.jar	267 361	0ccf1c38e4f7c2677ae02cc9b0928 b96b505dcab68faeba8c2603bbe2 bafb5a6

AIX platform

Név	Méret	Sha-256 Lenyomat

libxadessigner.so	17 040 124	883641ec37da9ac3078306a7c4b6 443885773e34918b8f42ad1338da de8402b4
libxadessignerlocale_eng.so	50 456	f9a445f0a863c93707b0eee95401f 5892aafb8963a94acc6a9e865089 089fe60
libxadessignerlocale_ger.so	55 692	503eda10136dad410a37ba2a6155 f4aa5297f654a07016d322793648c 2ba7cf1
libxadessignerlocale_hun.so	56 564	487a20e0c11b916c3fc860ab1194 0ef840562ea3debd91803a8532e6 309f65fe
mscpdf.jar	267 361	0ccf1c38e4f7c2677ae02cc9b0928 b96b505dcab68faeba8c2603bbe2 bafb5a6

2.3. A tanúsítás megrendelője

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

Microsec Számítástechnikai Fejlesztő Kft.

1022 Budapest, Marczibányi tér 9.

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 Windows2000, WindowsXP, Windows Server 2003, Windows Vista, Windows CE, Unix, Linux, Solaris és AIX 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 (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-SHA1 vagy RSA-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 Hírközlési Hatóság Hivatala Informatikai Szabályozási Igazgatóság HL-21917/2008 határozata a felhasználható biztonságos kriptográfiai algoritmusokról, valamint a hozzájuk tartozó paraméterekről a mellékletekben foglaltaknak megfelelően;

4.1.2. Önként vállalt normatívák

MATRIX által vizsgált megfelelés:

- Az Európai Parlament és a Tanács 1999/93/EK számú Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről;
- 2/2002. (IV. 26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről;
- 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 igazolt megfelelés:

- RFC 3275: XML-Signature Syntax and Processing,
- RFC 5652: Cryptographic Message Syntax,
- ETSI TS 101 903 V1.2.2, V1.3.2 és V1.4.1: XML Advanced Electronic Signatures (XAdES),
- RFC 5280: Certificate and Certificate Revocation List (CRL) Profile,
- RFC 2560: Online Certificate Status Protocol (OCSP),
- RFC 3161: Time-Stamp Protocol (TSP),
- 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 PDF Advanced Electronic Signature Profiles; Part 1,2,3: 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.
- MELASZ Munkacsoport Megállapodás, v2.0, 2008. december. Egységes MELASZ formátum elektronikus aláírásokra,
- Biztonsági körülmények, környezet.

Ezek közül a MATRIX által validált tesztekkel alátámasztott megfelelés:

- 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 PDF Advanced Electronic Signature Profiles; Part 1,2,3: 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.

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 2000,

Microsoft Windows XP,

Microsoft Windows Server 2003,

Microsoft Windows Vista,

Linux,

Sun Solaris,

IBM AIX.

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 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.

4.2.4. 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 Hírközlési Hatóság Hivatala Informatikai Szabályozási Igazgatóság HL-21917/2008 határozata.
- 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 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)