

TANÚSÍTVÁNY

(I-MS20T1_TAN-SW) MELLÉKLETE

Dokumentumazonosító	TAN-SW.ME-01	
Projektazonosító	I-MS20T1	Microsec Zrt. e-Szignó minősített aláírás létrehozó és kezelő megbízható modul 3.3 szoftver Tanúsítás 2020.
MATRIX tanúsítási igazgató	Molnár Ádám	
Kelt	Budaörs, 2020. augusztus 28	

1. A TANÚSÍTÁS KÖRÜLMÉNYEI

A MATRIX Kft. a NAH-6-0054/2019/K számon a Nemzeti Akkreditáló Hatóság (NAH) által akkreditált terméktanúsító szervezet.

A Microsec Zrt. elektronikus aláírási termékek fejlesztésével és forgalmazásával, valamint bizalmi szolgáltatások nyújtásával foglalkozó vállalat.

A MATRIX Kft. a szoftver értékelése során az önként vállalt normatívák pontról pontra történő vizsgálatát végezte el.

2. NORMATÍV DOKUMENTUMOK

Védelmi profil:

US Government Family of Protection Profiles Public Key-Enabled Applications For Basic Robustness Environments (v2.8, May 2007) archivált profil családból származtatott.

U.S. Government Basic Robustness PKE PP with

- Certification Path Validation – Basic
- PKI Signature Generation
- PKI Signature Verification
- PKI Encryption using Key Transfer

Algorithms:

- PKI Decryption using Key Transfer Algorithms
- Online Certificate Status Protocol Client
- Certificate Revocation List (CRL) Validation at EAL 3 with augmentation

Önként vállalt Normatívák:

- ISO/IEC 15408-1:2009 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

- ISO/IEC 15408-2:2008 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components

- ISO/IEC 15408-3:2008 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components

A vizsgálat módszertana a következő normatíváknak megfelelő:

- ISO/IEC 18045:2008 Informatika Biztonságtechnika Az informatikai biztonság értékelés módszertana

3. AZ ÉRTÉKELÉS TÁRGYA

A Microsec Zrt. által fejlesztett e-Szignó minősített aláírás létrehozó és kezelő megbízható modul 3.3.

3.1. ÉT azonosítása

Jellemző	Érték
ÉT megnevezése	e-Szignó minősített aláírás létrehozó és kezelő megbízható modul 3.3.
ÉT verzió	v3.3
Dátum	2013.05.15
Fejlesztő	Microsec Zrt.
Termék típus	minősített elektronikus aláírás létrehozó és kezelő megbízható modul
Platform	Windows, Linux, Solaris, AIX, Mac OS X
CC verzió	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017
PP megfelelés	<p>US Government Family of Protection Profiles Public Key-Enabled Applications For Basic Robustness Environments (v2.8, May 2007)</p> <p>archivált profil családból származtatott.</p> <p>U.S. Government Basic Robustness PKE PP with</p> <ul style="list-style-type: none"> - Certification Path Validation – Basic - PKI Signature Generation - PKI Signature Verification - PKI Encryption using Key Transfer Algorithms - PKI Decryption using Key Transfer Algorithms - Online Certificate Status Protocol Client - Certificate Revocation List (CRL) Validation <p>at EAL 3 with augmentation</p>

ST megfelelés	BIZTONSÁGI ELŐIRÁNYZAT az e-Szignó minősített aláírás létrehozó és kezelő megbízható modulhoz v1.4 (OID: 1.3.6.1.4.1.21528.2.1.3.57)
---------------	--

3.2. Az értékelés tárgyát képező dokumentációk

Típus	Tárgy	Verzió	Megjelenés
Szoftver	Microsec e-Szignó minősített aláírás létrehozó és kezelő megbízható modul fájlcsomag (Win32, Linux, Solaris, AIX, Mac OS X)	3.3	Elektronikus
Szoftver	Tesztesetek	1.0	Elektronikus
Dokumentum	Kiszállítási folyamatok (ALC_DEL.1) v1.0.docx	1.0	docx
Dokumentum	Biztonsági intézkedések azonosítása (ALC_DVS.1) v1.0.docx	1.0	docx
Dokumentum	Az azonosítás szabályozása (ALC_CMC.3) v0.9.docx	0.9	docx
Dokumentum	A telepített verzió CM lefedettsége (ALC_CMS.3) v0.9.docx	0.9	docx
Dokumentum	A fejlesztői által definiált életciklus modell (ALC_LCD.1) v1.0.docx	1.0	docx
Dokumentum	Funkcionális elírást teljes összefoglalással (FSP.3) v1.0.docx	1.0	docx
Dokumentum	Biztonsági architektúra leírás (ADV_ARC.1) v1.0.docx	1.0	docx
Dokumentum	Architektúrális terv (ADV_TDS.2) v0.9.docx	0.9	docx
Dokumentum	Felhasználói üzemeltetési útmutató (AGD_OPE.1).docx	1.0	docx
Dokumentum	Előkészítési folyamatok (AGD_PRE.1) v1.0.docx	1.0	docx
Dokumentum	A felszínv terv vizsgálata (ATE_DPT.1) v0.9.docx	0.9	docx
Dokumentum	A lefedettség vizsgálata (ATE_COV.2) v0.9.docx	0.9	docx
Dokumentum	Funkcionális vizsgálat (ATE_FUN.1) v0.9.docx	0.9	docx
Dokumentum	Hibajelentés folyamatai (ALC_FLR.2) v1.0.docx	1.0	docx
Dokumentum	Sebezhetőség vizsgálata (AVA_VAN.2).docx	0.9	docx

3.3. A tanúsítás megrendelője

Cég megnevezése:	Microsec Számítástechnikai Fejlesztő Zártkörűen működő Részvénytársaság
Székhely:	1033 Budapest, Ángel Sanz Briz út 13.
Céggjegyzékszám:	01-10-047218
Adószám:	23584497-2-41

4. FUNKCIONÁLIS LEÍRÁS

Az e-Szignó minősített aláírás létrehozó és kezelő megbízható modul az elektronikus aláírások létrehozására és kezelésére kifejlesztett funkcionalitás halmaza. 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 Windows, Unix, Linux, AIX környezetben, 32 és 64 biten is. Funkcionalitásai elérhetőek standard C felületen, JAVA programozói felületen, COM és .NET 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) [RFC 3275] és az erre épülő ETSI TS 101 903 V1.4.2. (XAdES – XML Advanced Electronic Signatures) [XAdES 1.4.2] ajánlásoknak megfelelő elektronikus aláírás állományt, e-aktát [e-akta v1.5] 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 1.2.2-es és 1.4.2-es verzióit is [XAdES 1.2.2, XAdES 1.4.2], és megfelel a [XAdES-BP]-nek, valamint az ETSI EN 319 132-1 [XAdES-sig 1] és a 319 132-2 [XAdES-sig 2] előírásoknak is. Támogatja az RFC 5652 (CMS aláírás) [RFC 5652] és az erre épülő ETSI TS 101 733 V2.2.1. (CAAdES – CMS Advanced Electronic Signatures) [CAAdES 1.8.3], [CAAdES 2.2.1] ajánlásoknak megfelelő aláírás létrehozását és ellenőrzését is, megfelel a [CAAdES-BP 2.1.1]-nek és [CAAdES-BP 2.2.1]-nek, valamint az ETSI EN 319 122-1 [CAAdES-sig 1] és a 319 122-2 [CAAdES-sig 2] előírásoknak is. Mindezekon kívül képes az ETSI TS 102 778-1,2,3,4 (PAdES – PDF Advanced Electronic Signature) [PAdES-1, PAdES-2, PAdES-3, PAdES-4] ajánlások által definiált PDF aláírások létrehozására és kezelésére is, és megfelel a [PAdES-BP]-nek, valamint az ETSI EN 319 142-1 [PAdES-sig 1] és az 319 142-2 [PAdES-sig 2] előírásoknak is. Támogatja az ETSI TS 102 918 v 1.3.1. (ASiC – Associated Signature Containers) ajánlásnak megfelelő aláírások létrehozását is [ASiC], megfelel az [ASiC-BP]-nek, valamint az ETSI EN 319 162-1 [ASiC-sig 1] és a 319 162-2 [ASiC-sig 2] előírásoknak is. Képes aláírással ellátni az ODF dokumentumokat [ODF]. Alkalmas továbbá MELASZ-ready 1.0 [MELASZ 1.0] és 2.0 [MELASZ 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 [IHM sig 2005.11.22].

Az aláírások RSA-SHA256 algoritmussal [PKCS #1 v2.2] vagy ECC alapú SHA256 algoritmussal [RFC 5480] készülnek. A minősített elektronikus aláírás elkészítése minden esetben egy személyhez rendelt biztonságos aláírás-létrehozó eszköz (MALE) segítségével történik; fokozott biztonságú aláírás létrehozása a fájlrendszerben lévő PKCS #12 [PKCS #12 v1.0], [PKCS #12 v1.1], [RFC 7292] formátumú kulcsokkal, illetve PKCS #11 [PKCS #11 v2.20] vagy OpenSSL [OpenSSL] engine interfésszel rendelkező hardver aláíró eszközökkel (chipkártya, HSM) lehetséges.

A program az X.509 formátumú tanúsítványok [RFC 5280] ellenőrzéséhez szükséges adatok (hitelesítés-szolgáltatói tanúsítványok, időbélyegek [RFC 3161], visszavonási listák (CRL:

Certificate Revocation List) [RFC 5280], OCSP (Online Certificate Status Protocol, Online Tanúsítvány-állapot Protokoll) válaszok [RFC 2560]) begyűjtését, a tanúsítvány-lánc felépítését és ellenőrzését is elvégzi. A beszerzett adatok csatolásával képes -EPES, -T, -C, -X-L -A és B-B, B-T, B-LT, B-LTA típusú aláírások létrehozására vagy egy korábban létrehozott aláírás kibővítésére. Támogatja az ETSI TR 102 038 v1.1.1 ajánlásnak [Sig Pol] megfelelő aláírási szabályzatok használatát is.

Lehetőséget nyújt a beillesztett dokumentumok, illetve az egész e-akta RSA-DES3 algoritmussal, PKCS #7 formátumban [PKCS #7 v1.5] történő titkosítására és azok visszafejtésére. További funkcionálitása a beillesztett dokumentumok ZIP [ZIP] tömörítése.

Lehetőséget nyújt az időbélyeg szolgáltatóhoz a felhasználónév/jelszó alapú és a tanúsítvány alapú azonosításra is. A hiba- illetve analitikus üzenetek több nyelven (magyar, angol, német) is elérhetőek.

Az e-Szignó MM továbbá a következő, harmadik fél által készített komponenseket használja fel:

- OpenSSL: Az aláírások és a titkosítás kezelését, az időbélyegek feldolgozását végző függvénykönyvtár, a HTTP kommunikációra is használatos (C nyelven).
- LibXML2: Alapvető XML feldolgozási funkcionálitás (C nyelven).
- xmlsec: Alapvető XML aláírás, titkosítás funkciókat implementáló modul C nyelven.
- curl: Hálózati kommunikációt végző modul (C/C++ nyelven).
- ZLIB: A PKZIP algoritmusú tömörítés implementációja (C/C++ nyelven).
- Boost: Reguláris kifejezéseket feldolgozó modul (C/C++ nyelven).
- pdfhummus: A pdf formátum feldolgozást végző c++ modul.
- libtiff: A tiff képformátum feldolgozását végző c++ modul.
- libpng: A png képformátum feldolgozásáért felelős c++ modul.
- jpeg: A jpeg képformátum feldolgozásáért felelős modul.
- rapidjson: JSON formátum kezelését végző c++ modul.
- QRLib: QR-kód generálást végző c++ modul.

Kizárólag Windows-os környezetben:

- MFC140.dll: MS Foundation Classes funkciók
- MFC140u.dll: MS Foundation Classes funkciók, unicode-os megvalósítás
- msvcp140.dll: MS Visual C++ 14.0 futtatókörnyezet funkciók
- msucr140.dll: MS Visual C 14.0 futtatókörnyezet funkciók
- Crypto API: A Windows kriptográfiai funkcionálitása

Kizárólag Linux, Unix és AIX környezetben:

- standard C++ könyvtár: A standard C++ függvényeket tartalmazó komponens

A harmadik fél által készített komponensek vagy szabadon felhasználhatóak, vagy rendelkezünk a felhasználásukra feljogosító licenccel. A licencelés kérdéseit az „e-Szignó végfelhasználói licencszerződés” [eSig lic] című dokumentáció részletezi.

A fordítás során a felsorolt egységek közül néhány (amelyek az ábrán a XadesSigner belsejében találhatóak) belefordul a XadesSigner komponensbe, míg a többi külön fordítási egységet képez. A következőkben ismertetjük a fordítást követően előálló komponenseket a különböző platformokon. A telepítőcsomag ezeket (valamint egyéb szükséges állományokat, pl. gyökértanúsítványok, felhasználói segédlet stb.) tartalmazza.

Windows platformon:

- XadesSigner.dll
- XadesSignerLocale_ENG.dll
- XadesSignerLocale_GER.dll
- XadesSignerLocale_HUN.dll

Kapcsolódó komponensek, amelyek nem képezik az Értékelés tárgyának részét:

- MFC140.dll
- MFC140u.dll
- msvcp140.dll
- msucr140.dll
- xsign.dll
- XSign4COM.dll
- XSign4NET.dll
- Xsign4java.dll
- Xsign4java.jar
- eszigno3.exe

Linux/UNIX/AIX platformon:

- libxadessigner.so
- libxadessignerlocale_hun.so
- libxadessignerlocale_eng.so
- libxadessignerlocale_ger.so

Kapcsolódó komponensek, amelyek nem képezik az Értékelés tárgyának részét:

- libstdc++.so (GCC)
- libxsign.so

- libxsign4java.so
- xsign4java.jar
- eszigno3

5. MEGFELELŐSÉG A NORMATÍV DOKUMENTUMOK ALAPJÁN

5.1. *Megfelelőség a normatív dokumentumoknak*

Az ÉT megfelel az alábbi normatív dokumentumoknak:

5.1.1. Kötelezően betartandó normatívák

- ISO/IEC 15408-1:2009 Informatika Biztonságtechnika Az informatikai biztonság értékelés szempontjai, 1. rész. ISO, 2009
- ISO/IEC 15408-2:2008 Informatika Biztonságtechnika Az informatikai biztonság értékelés szempontjai, 2. rész. ISO, 2008
- ISO/IEC 15408-3:2008 Informatika Biztonságtechnika Az informatikai biztonság értékelés szempontjai, 3. rész. ISO, 2008

5.1.2. A vizsgálat módszertana a következő normatíváknak megfelelő

- ISO/IEC 18045:2008 Informatika Biztonságtechnika Az informatikai biztonság értékelés módszertana

5.2. *Biztonsági garanciaszint vállalás*

A megfelelés biztonsági garancia szintje EAL 3+ az alábbiak szerint:

A Microsec Zrt. által fejlesztett szoftver az ISO/IEC 15408 szerinti EAL 3 garanciaszintet valósítja meg, kiegészítve az ALC_FLR.2 biztonsági garanciális összetevővel.

Az aláírási termék megfelel a fenti követelményeknek a 5.3 és a 5.4 pontban leírt biztonságos felhasználási és működési környezetben az alábbi feltételek teljesülése mellett:

A tanúsítás kizárólag a vizsgált rendszer aktuális verziójára vonatkozik, bármilyen változás esetén a módosított verzióra jelen tanúsítvány érvénytelen.

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

- Operációs rendszer,
- a felhasznált külső szoftver modulok, illetve programok,
- a működéshez használt hardver elemek.

5.3. *Biztonságos felhasználás feltételei*

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

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.

5.3.1. Működési környezet

A vizsgálat tárgya kizárólag az e-Szignó minősített aláírás létrehozó és kezelő megbízható modul 3.3 fejlesztéséhez vehető igénybe.

Az Értékelés tárgyának környezetére vonatkozó biztonsági célkitűzések azonosítói „OE” előtaggal kezdődnek.

#Célkitűzés azonosítója Leírás

1. OE.AUDIT_GENERATION Az IT környezet képes felismerni és naplózni a felhasználókhöz köthető, biztonsággal kapcsolatos eseményeket.
2. OE.AUDIT_PROTECTION Az IT környezet képes megvédeni az audit információt.
3. OE.AUDIT_REVIEW Az IT környezet szolgáltatja a lehetőséget arra, hogy az audit információt adott feltételek szerint szűrve tekintsük meg.
4. OE.Configuration Az IT környezetet megfelelően telepítették és konfigurálták, ezáltal a TOE biztonságos állapotból tudja megkezdeni a működését.
5. OE.CORRECT_TSF_OPERATION Az IT környezet lehetővé teszi a TOE biztonsági funkciói tesztelését, biztosítva ezáltal, hogy a biztonsági funkciók megfelelően fognak működni a felhasználók számítógépén is.
6. OE.CRYPTOGRAPHY_HUN A TOE-nak az IT környezet által biztosított, az európai, illetve magyar törvények, jogszabályok és egyéb mértékadó követelmények szerint az adott célra, a használat időpontjában felhasználható kriptográfiai szolgáltatásokat kell használnia. Amennyiben minősített elektronikus aláírás létrehozására van szükség, a TOE környezetének tartalmaznia kell egy, az NMHH nyilvántartásában szereplő MALE-t, az ennek használatához szükséges egyéb komponensekkel (kártyaolvasó, illesztőprogram) együtt.
7. OE.DISPLAY_BANNER Az IT környezetnek egy tanácsadó figyelmeztetést kell megjelenítenie a TOE használatára vonatkozóan.
8. OE.Basic A TOE-t a sebezhetőségi analízis által „alap” kategóriába sorolt támadási potenciálnak megfelelően kell megtervezni és implementálni.
9. OE.MANAGE Az IT környezet szolgáltatja az adminisztrátoroknak a TOE biztonságának menedzselésével kapcsolatos összes funkcionális és egyéb szükséges eszközt, míg megakadályozza ezen funkciók és eszközök jogosulatlan felhasználását.
10. OE.MEDIATE Az IT környezet megvédi a felhasználói adatokat az azokra vonatkozó biztonsági irányelveknek megfelelően.
11. OE.NO_EVIL A TOE-t felhasználó közösségnek/szervezetnek kell biztosítania, hogy az adminisztrátorok nem rosszindulatúak, megfelelően képzettek és követnek minden adminisztrátori útmutatót.
12. OE.PHYSICAL A nem-IT környezetnek olyan szintű fizikai védelmet kell biztosítania, amely meggátolja, hogy a TOE-t bármilyen módon befolyásolják vagy valamely side channel

attack – mint például az áramfelvételt vagy időzítéseket vizsgáló analízisek valamely formája – tárgyává válhasson.

13.OE.RESIDUAL_INFORMATION Az IT környezetnek kell biztosítania, hogy amennyiben az általa védett erőforrások újra hozzárendelésre kerülnek, az azokban tárolt információk nem kerülnek nyilvánosságra.

14.OE.SELF_PROTECTION Az IT környezetnek a saját futtatható kódjai számára fent kell tartania egy olyan futtatási környezetet, amely megvédi önmagát és az erőforrásait a külső beavatkozástól, befolyásolástól vagy jogosulatlan közzétételtől.

15.OE.TIME_STAMPS Az IT környezetnek biztosítania kell a megbízható időbélyegek elérésének lehetőségét, valamint, hogy az adminisztrátor az időbélyegeknek megfelelően beállíthassa a rendszeridőt.

16.OE.TIME_TOE Az IT környezetnek kell biztosítania a TOE számára használható megbízható időt.

17.OE.TOE_ACCESS Az IT környezetnek kell biztosítania azokat a mechanizmusokat, amelyekkel kontrollálható a felhasználók logikai hozzáférése a TOE-hez.

18.OE.TOE_PROTECTION Az IT környezetnek kell megvédenie a TOE-t és a TOE erőforrásait a külső behatásoktól, befolyásolástól vagy jogosulatlan közzétételtől és módosítástól.

6. RÖVIDÍTÉSEK

Rövidítés	Tartalom
BE	Biztonsági Előirányzat
ISO/IEC 15408	Az informatikai biztonság értékelésének közös szempontrendszer
ISO/IEC 18045	Az informatikai biztonság értékelés módszertana
PP	Protection Profile – Védelmi profil
ST	Security target – Biztonsági Előirányzat
TOE	Target of Evaluation – az értékelés tárgya
VP	Védelmi profil – Protection Profile

Dokumentum vége