ANNEX OF THE CERTIFICATE

(I-MS20T1_TAN-SW_EN)

Document ID:	**TAN-SW_EN.ME-01**	
Project ID:	**I-MS20T1**	**Microsec Ltd.** **e-Szignó qualified signature creation and management module 3.3 software certification 2020.**
MATRIX director of certification	**Ádám Molnár**	
Date	**Budaörs, august 28. 2020.**	

1. CERTIFICATION CONDITIONS

The certification body of MATRIX Ltd. (henceforth: MATRIX) is accredited by National Accreditation Authority based on NAH-6-0054/2019/K accreditation document.

Microsec Ltd. is a company engaged in the development and distribution of electronic signature products and the provision of trust services.

During the evaluation of the software, MATRIX performed a point-by-point examination of the norms undertaken voluntarily.

2. NORMATIVE DOCUMENTS

Protection Profile:

US Government Family of Protection Profiles Public Key-Enabled Applications For Basic Robustness Environments (v2.8, May 2007) archived profile derived from family.

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

Voluntairly undertaken normatives:

- 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

The evalaution methodology complies with the following:

- ISO/lEC 18045:2008 Information technology - Security Techniques – Methodology for IT security evaluation

3. TARGET OF EVALUATION

E-Szignó qualified signature creation and management trusted module 3.3 developed by Microsec Ltd.

3.1. TOE Description

	Description
TOE Name	E-Szignó qualified signature creation and management trusted module 3.3.
TOE Version	v3.3
Date	2013.05.15
Developer	Microsec Ltd.
Product Type	qualified signature creation and management trusted module
Platform	Windows, Linux, Solaris, AIX, Mac OS X
CC version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017
PP conformity	US Government Family of Protection Profiles Public Key-Enabled Applications For Basic Robustness Environments (v2.8, May 2007) archived profile derived from family. 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

ST conformity	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. TOE documentation

Type	Subject	Version	Form
Software	Microsec e-Szignó minősített aláírás létrehozó és kezelő megbízható modul fájlcsomag (Win32, Linux, Solaris, AIX, Mac OS X)	3.3	Electronic
Software	Tesztesetek	1.0	Electronic
Document	Kiszállítási folyamatok (ALC_DEL.1) v1.0.docx	1.0	docx
Document	Biztonsági intézkedések azonosítása (ALC_DVS.1) v1.0.docx	1.0	docx
Document	Az azonosítás szabályozása (ALC_CMC.3) v0.9.docx	0.9	docx
Document	A telepített verzió CM lefedettsége (ALC_CMS.3) v0.9.docx	0.9	docx
Document	A fejlesztï által definiált életciklus modell (ALC_LCD.1) v1.0.docx	1.0	docx
Document	Funkcionális elïírás teljes összefoglalással (FSP.3) v1.0.docx	1.0	docx
Document	Biztonsági architektúra leírás (ADV_ARC.1) v1.0.docx	1.0	docx
Document	Architektúrális terv (ADV_TDS.2) v0.9.docx	0.9	docx
Document	Felhasználói üzemeltetési útmutató (AGD_OPE.1).docx	1.0	docx
Document	Elïkészítï folyamatok (AGD_PRE.1) v1.0.docx	1.0	docx
Document	A felsïszintv terv vizsgálata (ATE_DPT.1) v0.9.docx	0.9	docx
Document	A lefedettség vizsgálata (ATE_COV.2) v0.9.docx	0.9	docx
Document	Funkcionális vizsgálat (ATE_FUN.1) v0.9.docx	0.9	docx
Document	Hibajelentés folyamatai (ALC_FLR.2) v1.0.docx	1.0	docx
Document	Sebezhetïség vizsgálata (AVA_VAN.2).docx	0.9	docx

3.3. Costumer of the certification

Company name:	Microsec Ltd.
Headquarter:	13 Ángel Sanz Briz Road, Budapest H-1033, Hungary
Company registration number:	01-10-047218
Tax number:	23584497-2-41

4. FUNTIONAL SPECIFICATION

The e-Szignó qualified signature creation and management module is a set of functionalities developed for creating and managing electronic signatures. In addition to the operations related to electronic signatures (creating a signature, verifying, obtaining validation data, verifying it and attaching it to a signature), it is suitable for handling e-files that best support working with electronic documents. With its help, we can provide the individual elements (e-files, documents, signatures, countersignatures) with additional information appropriate to the area of use, facilitating case management. It is also possible to request and prepare an acknowledgment of receipt, as well as to encrypt and decrypt documents and e-files. It is also capable of creating verified signatures in a specific role (handling attribute certificates).

Using the reliable module for creating and managing e-Szignó qualified signatures, systems and applications using electronic signatures can be easily created. E-Signo MM can be used in Windows, Unix, Linux, AIX environments, also in 32 and 64 bits. Its functionalities are available through a standard C interface, JAVA programming interface, COM and .NET interface, but there is also a command line version. The e-Szignó application for the Windows platform, supplemented with a graphical user interface, enjoys a wide range of users in Hungary.

The e-Szignó MM defaults to RFC 3275 (XMLSignature) [RFC 3275] and the ETSI TS 101 903 V1.4.2 based on it. (XAdES - XML Advanced Electronic Signatures) Creates an electronic signature file, e-file [e-file v1.5] in accordance with [XAdES 1.4.2] recommendations, which is a framed type of XAdES signature with additional features. It can also create and manage other XAdES-compliant electronic signatures, allowing, for example, the signing of any node in any XML document (embedded signature) or the signing of large documents in such a way that the signature file itself does not contain the document (separate signature). It also supports XAdES versions 1.2.2 and 1.4.2 [XAdES 1.2.2, XAdES 1.4.2] and complies with [XAdES-BP] and ETSI EN 319 132-1 [XAdES- sig 1] and 319 132-2 [XAdES-sig 2]. Supports RFC 5652 (CMS signature) [RFC 5652] and the ETSI TS 101 733 V2.2.1 based on it. (CAdES - CMS Advanced Electronic Signatures) [CAdES 1.8.3], [CAdES 2.2.1] recommendations, [CAdES-BP 2.1.1] and [CAdES-BP 2.2.1] as well as ETSI EN 319 122-1 [CAdES-sig 1] and 319 122-2 [CAdES-sig 2]. In addition, it is able to create and manage PDF signatures defined by ETSI TS 102 778-1,2,3,4 (PAdES - PDF Advanced Electronic Signature) [PAdES-1, PAdES-2, PAdES-3, PAdES-4] recommendations. , and also complies with [PAdES-BP] and ETSI EN 319 142-1 [PAdES-sig 1] and 319 142-2 [PAdES-sig 2]. Supports ETSI TS 102 918 v 1.3.1. (ASiC - Associated Signature Containers) [ASiC], complies with [ASiC-BP] and ETSI EN 319 162-1 [ASiC-sig 1] and 319 162-2 [ASiC-sig 2] specifications as well. Capable of signing ODF documents [ODF]. It is also suitable for creating MELASZ-ready 1.0 [MELASZ 1.0] and 2.0 [MELASZ 2.0] signatures, and can properly handle signatures created by other signature-creation applications in accordance with the above standards. It also complies with the signature format required for the administration [IHM sig 22.11.2005].

Signatures created by using the RSA-SHA256 algorithm [PKCS # 1 v2.2] or the ECC-based SHA256 algorithm [RFC 5480]. A qualified electronic signature is always created using a secure signature-creation device (MALE) assigned to a person; create a high-security signature with PKCS # 12 [PKCS # 12 v1.0], [PKCS # 12 v1.1], [RFC 7292] format files in the file system, or PKCS # 11 [PKCS # 11 v2.20] or OpenSSL [It is possible with hardware signing devices (chip card, HSM) with OpenSSL] engine interface.

The program requires data required to verify X.509 format certificates [RFC 5280], certificate authority certificates, timestamps [RFC 3161], Certificate Revocation List (CRL) [RFC 5280], OCSP (Online Certificate Status Protocol, Online Certificate). status Protocol) responses [RFC 2560]), builds and verifies the certificate chain. By attaching the acquired data, it is able to create -EPES, -T, -C, -X-L -A and B-B, B-T, B-LT, B-LTA signatures or expand a previously created signature. It also supports the use of signing rules in accordance with ETSI Recommendation TR 102 038 v1.1.1 [Sig Pol].

It allows you to encrypt and decrypt inserted documents or the entire e-file using the RSA-DES3 algorithm in PKCS # 7 format [PKCS # 7 v1.5]. Another functionality is ZIP [ZIP] compression of inserted documents.

It also allows the timestamp provider to use username / password-based and certificate-based authentication. Error and analytical messages are available in several languages (Hungarian, English, German).

E-Szignó MM also uses the following third-party components:

- OpenSSL: A library for signature and encryption management, timestamp processing, also used for HTTP communication (in C).
- LibXML2: Basic XML processing functionality (in C language).
- xmlsec: A module that implements basic XML signature and encryption functions in C.
- curl: Network communication module (in C / C ++).
- ZLIB: Implementation of PKZIP algorithm compression (in C / C ++ language).
- Boost: Module for processing regular expressions (in C / C ++).
- pdfhummus: The c ++ module that processes pdf format.
- libtiff: A c ++ module that processes the tiff image format.
- libpng: The c ++ module responsible for processing the png image format.
- jpeg: Module responsible for processing the jpeg image format.
- rapidjson: a c ++ module that handles the JSON format.
- QRLib: c ++ module for QR code generation.

Windows only:

- MFC140.dll: MS Foundation Classes features
- MFC140u.dll: MS Foundation Classes functions, unicode implementation
- msvcp140.dll: MS Visual C ++ 14.0 runtime features
- msvcr140.dll: MS Visual C 14.0 runtime features
- Crypto API: The cryptographic functionality of Windows

778/5000

Linux, Unix and AIX only:

- standard C ++ library: A component containing standard C ++ functions

Third-party components are either free to use or licensed to use. Licensing issues are detailed in the “eSigno End User License Agreement” [eSig lic] documentation.

During the translation, some of the listed units (located inside the XadesSigner in the figure) turn into the XadesSigner component, while the others form a separate translation unit. The following describes the components that occur after compilation on different platforms. The installation package includes these (as well as other necessary files such as root certificates, user help, etc.).

On Windows platform:

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

Related components that are not part of TOE:

- MFC140.dll
- MFC140u.dll
- msvcp140.dll
- msvcr140.dll
- xsign.dll
- XSign4COM.dll
- XSign4NET.dll
- Xsign4java.dll
- Xsign4java.jar
- eszigno3.exe

On Linux/UNIX/AIX platform:

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

Related components that are not part of TOE:

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

- eszigno3

5. COMPLIANCE ON THE BASIS OF REGULATORY DOCUMENTS

5.1. Compliance with normative documents

The TOE comforms with the following normatives:

5.1.1. Mandatory standards

- 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

5.1.2. The evalaution methodology complies with the following:

- ISO/IEC 18045:2008 Information technology - Security Techniques – Methodology for IT security evaluation

5.2. Evaluation Assurance Level

The level of security guarantee of compliance is EAL 3+ as follows:

- The software developed by Microsec Zrt. Implements the EAL 3 guarantee level according to ISO / IEC 15408, supplemented with the ALC_FLR.2 safety guarantee component.

The signature product shall meet the above requirements in the secure environment of use and operation described in Sections 5.3 and 5.4, provided that the following conditions are met:

The certification only applies to the current version of the system under test, and in the event of any changes, this certificate is invalid for the modified version.

The operating environment of the program is not subject to certification, so it is:

- Operating system,
- the external software modules or programs used,
- ardware components used for operation.

5.3. Conditions of secure use

The above compliance is conditional on the fulfillment of the following set of requirements for the operating environment, compliance with which is the responsibility of the user. Because the TOE is not designed to operate on its own, it is typically integrated by a program developer into its own electronic signature or application with such functionality. When developing the application, the following conditions must be taken into account, which must be observed for the correct and safe operation of the module.

The evaluated signature product can only be used to create electronic signatures in an environment where all elements meet the generally expected security requirements and together they create a sufficiently secure IT system. The evaluation does not cover the examination of individual elements of the environment, the requirements set out here are guidelines for the proper use of the application.

5.3.1. Operational environment

The TOE can only be used for the development of the trusted module 3.3 for creating and managing e-Szignó qualified signatures.

The safety objective identifiers for the environment of the subject of the Assessment shall begin with the prefix "OE".

1. OE.AUDIT_GENERATION The IT environment is able to detect and log security-related events related to users.

2. OE.AUDIT_PROTECTION The IT environment can protect audit information.

3. OE.AUDIT_REVIEW The IT environment provides the opportunity to view audit information filtered under specific conditions.

4. OE.Configuration The IT environment is properly installed and configured so that the TOE can start operating from a secure state.

5. OE.CORRECT_TSF_OPERATION The IT environment allows the security features of the TOE to be tested, thus ensuring that the security features will work properly on users' computers as well.

6. OE.CRYPTOGRAPHY_ENG The TOE must use the cryptographic services provided by the IT environment, which can be used for the given purpose at the time of use in accordance with European and Hungarian laws, regulations and other relevant requirements. If it is necessary to create a qualified electronic signature, the TOE environment must contain a MALE registered with the NMHH, together with other components (card reader, driver) required for its use.

7. OE.DISPLAY_BANNER The IT environment shall display an advisory warning about the use of the TOE.

8. OE.Basic The TOE should be designed and implemented according to the attack potential categorized as “basic” by the vulnerability analysis.

9. OE.MANAGE The IT environment provides administrators with all the functionality and other tools necessary to manage the security of the TOE, while preventing unauthorized use of these functions and tools.

10. OE.MEDIATE The IT environment protects user data in accordance with the applicable security policies.

11. OE.NO_EVIL The community / organization using the TOE must ensure that administrators are not malicious, properly trained, and follow all administrative instructions.

12. OE.PHYSICAL The non-IT environment must provide a level of physical protection that prevents the TOE from being affected in any way or subjected to a side channel attack, such as some form of analysis of current consumption or timing.

13. OE.RESIDUAL_INFORMATION The IT environment must ensure that if the resources it protects are reassigned, the information stored in them will not be made public.

14. OE.SELF_PROTECTION The IT environment must maintain a runtime environment for its own executable code that protects itself and its resources from outside interference, influence, or unauthorized disclosure.

15. OE.TIME_STAMPS The IT environment must allow reliable timestamps to be accessed and the administrator to set the system time according to the timestamps.

16. OE.TIME_TOE The IT environment shall provide reliable time for the TOE.

17. OE.TOE_ACCESS The IT environment shall provide the mechanisms to control the logical access of users to the TOE.

18. OE.TOE_PROTECTION The IT environment shall protect the TOE and the TOE resources from external influences, influences or unauthorized disclosure and modification.

6. ABBREVATIONS

Abbrevation	Content
ISO/IEC 15408	Information technology - Security techniques - Evaluation criteria for IT security
ISO/IEC 18045	Information technology - Security Techniques – Methodology for IT security evaluation
PP	Protection Profile
ST	Security target
TOE	Target of Evaluation
CC	Common Criteria
MM	Trusted Module

End of the document.