Certificate number:
IT-MS25T_TAN-SW.EN/2026/025

Certificate Valid from:
12.06.2026.

Certificate Valid until:
11.06.2029.

Certificate

Description of trust service:

E-Szignó Qualified Signature Creation and Management Module

v3.5.x

MATRIX Auditing, Evaluating and Certification Ltd. (290 Szabadság út, Budaörs, Hungary, 2040) hereby that the submitted documentation, test results furthermore in accordance with the MATRIX_TS-2 certification scheme (MSZ EN ISO / IEC 17067: 2013 Standard Table 1 Building product certification scheme Type 1a), that provided by

Microsec Zrt.

13 Ángel Sanz Briz Road, Budapest H-1033, Hungary

complies

to the requirements of

the following normative documents:

− ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model
− ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components
− ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components
− ISO/IEC 15408-4:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities
− ISO/IEC 15408-5:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements

in accordnance with:
ISO/IEC 18045 Information security, cybersecurity and privacy protection Evaluation criteria for IT security Methodology for IT security evaluation

On behalf of the certification body:

Ádám Molnár
managing director
12.06.2026.

NAH-6-0054/2024/K
PRODUCT CERTIFICATION BODY

The Certificate is valid only with its Annex.

Annex of the Certficate (IT-MS25T_TAN-SW.EN/2026/025)

Document ID	**IT-MS25T_TAN-SW.EN**	
Project ID	**IT-MS25T**	**Microsec Ltd.** **e-Szignó qualified signature creation and management module v3.5.x software certification 2026.**
MATRIX Director of certification	**Gábor Nagy**	
Date	**Budaörs, at time by the timestamp**	

1. CERTIFICATION CONDITIONS

The certification body of MATRIX Ltd. (henceforth: MATRIX) is accredited by the National Accreditation Authority by the accreditation document No. NAH-6-0054/2024/K.

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.

Detailed Evaluation Reports have been made about the conformity assessment. The most important information on the conditions of the conformity assessment and use is contained in this annex.

2. Conformity Assessment Requirements

The conformity assessment requirements for the Evaluation Target:

Protection Profile:

EN 419111 Part 2: Protection profiles for signature creation and verification application - Signature creation application - Part 2: Core PP (draft)

EN 419111 Part 4: Protection profiles for signature creation and verification application - Signature verification application - Part 4: Core PP (draft)

Security Target for Qualified Signature creation and manager trustworthy module (OID: 1.3.6.1.4.1.21528.2.1.3.57.2.1)

Undertaken normatives:

ISO/IEC 15408-1, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security —Part 1: Introduction and general model

ISO/IEC 15408-2, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components

ISO/IEC 15408-3, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components

ISO/IEC 15408-4, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification evaluation methods and activites

MATRIX Auditing, Evaluating and Certification Ltd. Tax Identification Number: 11969608-2-13
2040 Budaörs, Szabadság út 290. Tel.: (23) 444 600 Internet: www.matrix-tanusito.hu E-mail: info@matrix-tanusito.hu

ISO/IEC 15408-5, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements

ETSI TS 119 101 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI) Policy and security requirements for applications for signature creation and signature validation

ETSI TS 319 102-1 V1.4.1 (2024-06) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

ETSI TS 119 102-1 V1.2.1 (2018-08) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

The evaluation methodology complies with the following:

ISO/IEC 18045 Information security, cybersecurity and privacy protection – Evaluation criteria for IT securtiy – Methodology for IT securtiy evaluation

Voluntary Normatives:

ETSI TS 119 101 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI) Policy and security requirements for applications for signature creation and signature validációnk

ETSI TS 119 102-1 V1.2.1 (2018-08) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

3. TARGET OF EVALUATION

E-Szignó qualified signature creation and management trusted module v3.5.x developed by Microsec Ltd.

3.1. TOE Description

	Description
TOE Name	e-Szignó minősített aláírás létrehozó és kezelő megbízható modul v3.5.x
TOE Version	v3.5.x
Date	2026.06.12
Developer	Microsec Ltd.
Product Type	Qualified Signature creation and Management trustworthy module
Platform	Windows, Linux, Solaris, AIX, Mac OS X
CC version	ISO_IEC 15408-1:2022 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1 ISO_IEC 15408-2:2022 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2 ISO_IEC 15408-3:2022 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3 ISO_IEC 15408-4:2022 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4 ISO_IEC 15408-5:2022 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5

MATRIX Auditing, Evaluating and Certification Ltd. Tax Identification Number: 11969608-2-13
2040 Budaörs, Szabadság út 290. Tel.: (23) 444 600 Internet: www.matrix-tanusito.hu E-mail: info@matrix-tanusito.hu

PP conformity	EN 419111 Part 2: Protection profiles for signature creation and verification application - Signature creation application - Part 2: Core PP EN 419111 Part 4: Protection profiles for signature creation and verification application - Signature verification application - Part 4: Core PP
ST conformity	BIZTONSÁGI ELŐIRÁNYZAT az e-Szignó minősített aláírás létrehozó és kezelő megbízható modulhoz (OID: 1.3.6.1.4.1.21528.2.1.3.57.2.1) v2.1

3.2. TOE documentation

Type	Subject	Version	Format
Software	Microsec e-Szignó minősített aláírás létrehozó és kezelő megbízható modul fájlcsomag (Windows, Linux, Solaris, AIX, Mac OS X)	v3.5.x	electronic
Software	Tesztesetek		electronic
Document	Kiszállítási folyamatok (ALC_DEL.1) v1.2_final	1.2	docx
Document	Biztonsági intézkedések azonosítása (ALC_DVS.1) v1.2_final	1.2	docx
Document	Az azonosítás szabályozása (ALC_CMC.4) v1.2_final	1.2	docx
Document	A telepített verzió CM lefedettsége (ALC_CMS.4) v1.2_final	1.2	docx
Document	A fejlesztő által definiált életciklus modell (ALC_LCD.1) v1.2_final	1.2	docx
Document	Definiált fejlesztői környezet (ALC_TAT.1) v1.2_final	1.2	docx
Document	Funkcionális előírás teljes összefoglalással (ADV_FSP.4) v1.2_final	1.2	docx
Document	Biztonsági architektúra leírás (ADV_ARC.1) v1.2_final	1.2	docx
Document	Mapping	-	xlsx
Document	TSF Module mapping	-	xlsx
Document	Architektúrális terv (ADV_TDS.3) v1.2_final	1.2	docx
Document	Felhasználói üzemeltetési útmutató (AGD_OPE.1) v1.2_final	1.2	docx
Document	Előkészítő folyamatok (AGD_PRE.1) v1.2_final	1.2	docx
Document	A felsőszintű terv vizsgálata (ATE_DPT.1) v1.2_final	1.2	docx
Document	A lefedettség vizsgálata (ATE_COV.2) v1.2_final	1.2	docx
Document	Független vizsgálat mintán (ATE_IND.2) v1.2_final	1.2	docx
Document	Funkcionális vizsgálat (ATE_FUN.1) v1.2_final	1.2	docx

MATRIX Auditing, Evaluating and Certification Ltd. Tax Identification Number: 11969608-2-13
2040 Budaörs, Szabadság út 290. Tel.: (23) 444 600 Internet: www.matrix-tanusito.hu E-mail: info@matrix-tanusito.hu

Document	Hibajelentés folyamatai (ALC_FLR.2) v1.2_final	1.2	docx
Document	Sebezhetőség vizsgálata (AVA_VAN.3) v1.2_final	1.2	docx
Document	IT-MS25T_SV-01.HELYSZINI_v2.doc	-	docx
Document	S2_MICROSEC_ESZIGNO_VEZETOI_OSSZEFOGLALO_251030	-	pdf
Document	S2_MICROSEC_ESZIGNO_JELENTES_251030	-	pdf

3.3. Customer 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

3.4. Audit time interval

MATRIX Ltd. performed the audit methodology described in chapter v3.5.x in the following time interval:

Audit interval: 15.11.2025. – 12.06.2026.

3.5. Description of the changes to the audit plan

During the audit, the audit team members conducted their activities in accordance with the audit plan, thereby ensuring that the audit proceedings remained consistent with the predetermined schedule and did not deviate therefrom.

4. Summary of the conformity assessment requirements

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, by default, generates an electronic signature file, referred to as an e-file (e-akta) [e-akta v1.5], compliant with RFC 3275 (XML Signature) [RFC 3275] and ETSI TS 101 903 V1.4.2 (XAdES – XML Advanced Electronic Signatures) [XAdES 1.4.2]. The e-file is an encapsulated form of a XAdES signature extended with additional properties. In addition, the product is capable of creating and processing other XAdES-compliant electronic signatures, enabling, for example, the signing of any node within an arbitrary XML document (embedded signature) or the signing of large

MATRIX Auditing, Evaluating and Certification Ltd. Tax Identification Number: 11969608-2-13
2040 Budaörs, Szabadság út 290. Tel.: (23) 444 600 Internet: www.matrix-tanusito.hu E-mail: info@matrix-tanusito.hu

documents in such a way that the signature file itself does not contain the signed document (detached signature). It supports both XAdES versions 1.2.2 and 1.4.2 [XAdES 1.2.2, XAdES 1.4.2] and conforms to the XAdES Baseline Profile (XAdES-BP) as well as the requirements specified in ETSI EN 319 132-1 [XAdES-sig 1] and ETSI EN 319 132-2 [XAdES-sig 2]. It also supports the creation and validation of signatures compliant with RFC 5652 (CMS) [RFC 5652] and ETSI TS 101 733 V2.2.1 (CAdES – CMS Advanced Electronic Signatures) [CAdES 1.8.3], [CAdES 2.2.1], conforms to CAdES Baseline Profile versions 2.1.1 [CAdES-BP 2.1.1] and 2.2.1 [CAdES-BP 2.2.1], and complies with the requirements of ETSI EN 319 122-1 [CAdES-sig 1] and ETSI EN 319 122-2 [CAdES-sig 2]. Furthermore, it is capable of creating and processing PDF Advanced Electronic Signatures (PAdES) as defined by ETSI TS 102 778 Parts 1–4 [PAdES-1, PAdES-2, PAdES-3, PAdES-4], conforms to the PAdES Baseline Profile (PAdES-BP), and complies with the requirements of ETSI EN 319 142-1 [PAdES-sig 1] and ETSI EN 319 142-2 [PAdES-sig 2]. It also supports the creation of signatures compliant with ETSI TS 102 918 v1.3.1 (ASiC – Associated Signature Containers) [ASiC], conforms to the ASiC Baseline Profile (ASiC-BP), and complies with the requirements of ETSI EN 319 162-1 [ASiC-sig 1] and ETSI EN 319 162-2 [ASiC-sig 2]. The product is capable of digitally signing ODF (OpenDocument Format) documents [ODF]. It also supports the creation of MELASZ-ready 1.0 [MELASZ 1.0] and MELASZ-ready 2.0 [MELASZ 2.0] signatures and is capable of correctly processing signatures created by other signature creation applications in accordance with the above standards. Furthermore, it complies with the electronic signature format prescribed for use within the Hungarian public administration [IHM sig 2005.11.22].

Signatures are generated 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 (SSCD) assigned to a specific individual (MALE); an advanced electronic signature may be created using keys stored in the file system in PKCS #12 format [PKCS #12 v1.0], [PKCS #12 v1.1], [RFC 7292], or by using hardware signature creation devices (smart cards or HSMs) supporting the PKCS #11 [PKCS #11 v2.20] or OpenSSL [OpenSSL] engine interface.

The product collects the information required for the validation of X.509 certificates [RFC 5280], including certification authority certificates, time stamps [RFC 3161], certificate revocation lists (CRLs – Certificate Revocation Lists) [RFC 5280], and OCSP (Online Certificate Status Protocol) responses [RFC 2560], and also performs certificate chain construction and validation. By embedding the collected validation data, it is capable of creating -EPES, -T, -C, -X-L, -A, B-B, B-T, B-LT, and B-LTA signature formats or extending an existing signature to one of these formats. The product also supports the use of signature policies compliant with ETSI TR 102 038 v1.1.1 [Sig Pol].

The product provides the capability to encrypt and decrypt embedded documents as well as the entire e-file using the RSA-DES3 algorithm in PKCS #7 format [PKCS #7 v1.5]. In addition, it supports ZIP [ZIP] compression of embedded documents.

The product supports both username/password-based and certificate-based authentication for accessing a Time Stamping Authority (TSA). Error messages and diagnostic messages are available in multiple languages (Hungarian, English, and German).

The e-Szignó MM also utilizes the following third-party components:

• OpenSSL: A library for signature and encryption processing and timestamp processing (implemented in C).

• LibXML2: A library providing core Extensible Markup Language (XML) processing functionality (implemented in C).

• xmlsec: A C library implementing core XML Signature and XML Encryption functionality.

• cURL: A module providing network communication functionality (implemented in C/C++).

• ZLIB: An implementation of the PKZIP compression algorithm (implemented in C/C++).

• Boost: A module providing regular expression processing functionality (implemented in C/C++).

• PDFHummus: A C++ library for Portable Document Format (PDF) processing.

MATRIX Auditing, Evaluating and Certification Ltd. Tax Identification Number: 11969608-2-13
2040 Budaörs, Szabadság út 290. Tel.: (23) 444 600 Internet: www.matrix-tanusito.hu E-mail: info@matrix-tanusito.hu

• libtiff: A C++ library for processing Tagged Image File Format (TIFF) images.

• libpng: A C++ library for processing Portable Network Graphics (PNG) images.

• jpeg: A library for processing JPEG image files.

• RapidJSON: A C++ library for processing JavaScript Object Notation (JSON) data.

• QRLib: A C++ library for generating QR codes.

• OpenLDAP: A library used for Lightweight Directory Access Protocol (LDAP) connectivity (implemented in C).

• FreeType: A library providing text rendering functionality (implemented in C).

Windows-specific components:

• MFC140.dll: Microsoft Foundation Classes (MFC) functionality.

• MFC140u.dll: Microsoft Foundation Classes (MFC) functionality with Unicode support.

• msvcp140.dll: Microsoft Visual C++ 14.0 runtime library.

• msvcr140.dll: Microsoft Visual C 14.0 runtime library.

• CryptoAPI: Windows cryptographic services.

Linux, UNIX, and AIX-specific components:

• Standard C++ Library: Component providing the standard C++ library functions.

The third-party components are either freely available for use or are used under appropriate licenses. Licensing terms are detailed in the "e-Szignó End User License Agreement" [eSig lic].

During the build process, some of the components listed above (those shown inside the XadesSigner component in the figure) are statically incorporated into the XadesSigner component, while the remaining components are built as separate compilation units. The following sections describe the components produced for the different supported platforms as a result of the build process. The installation package contains these components, together with other required files (e.g. root certificates, user documentation, etc.).

On the Windows platform:

• XadesSigner.dll

• XadesSignerLocale_ENG.dll

• XadesSignerLocale_GER.dll

• XadesSignerLocale_HUN.dll

Related components, which are not part of the Target of Evaluation (TOE):

• MFC140.dll

• MFC140u.dll

• msvcp140.dll

• msvcr140.dll

MATRIX Auditing, Evaluating and Certification Ltd. Tax Identification Number: 11969608-2-13
2040 Budaörs, Szabadság út 290. Tel.: (23) 444 600 Internet: www.matrix-tanusito.hu E-mail: info@matrix-tanusito.hu

• xsign.dll

• XSign4COM.dll

• XSign4NET.dll

• Xsign4java.dll

• Xsign4java.jar

• eszigno3.exe

On Linux, UNIX, and AIX platforms:

• libxadessigner.so

• libxadessignerlocale_hun.so

• libxadessignerlocale_eng.so

• libxadessignerlocale_ger.so

Related components that are not part of the scope of the Evaluation.:

• libstdc++.so (GCC)

• libxsign.so

• libxsign4java.so

• xsign4java.jar

• eszigno3

4.1. Evaluation Assurance Level

The assurance level of conformity is EAL 4+ ALC_FLR.1, as specified below:

The Security Target developed by Microsec Ltd. achieves Evaluation Assurance Level 4 (EAL 4) in accordance with ISO/IEC 15408, augmented by the ALC_FLR.1 assurance component.

The signature product complies with the above requirements within the secure operational and usage environment described in Section 4.2, provided that the following conditions are met:

The certification applies exclusively to the evaluated version of the system. Any modification to the evaluated system invalidates this certificate with respect to the modified version.

The following are outside the scope of the certification:

• the operating system,

• external software modules and programs used by the product,

• the hardware components used for its operation.

4.2. Conditions of secure using

Compliance with the above requirements is conditional upon satisfying the following requirements applicable to the operational environment, the fulfilment of which is the responsibility of the user. Since the TOE is not designed to operate as a standalone product, it is typically integrated by an

MATRIX Auditing, Evaluating and Certification Ltd. Tax Identification Number: 11969608-2-13
2040 Budaörs, Szabadság út 290. Tel.: (23) 444 600 Internet: www.matrix-tanusito.hu E-mail: info@matrix-tanusito.hu

application developer into an electronic signature application or another application providing electronic signature functionality. During the development of such an application, the following conditions shall be taken into account, as compliance with these conditions is necessary to ensure the correct and secure operation of the module.

The evaluated signature product may only be used to create electronic signatures in an operational environment in which all constituent elements satisfy generally accepted security requirements and collectively provide an adequately secure information system. The evaluation does not cover the assessment of the individual components of the operational environment; therefore, the requirements specified below are intended to provide guidance for the proper and secure use of the product.

4.2.1. Operational Enviroment

The results of the evaluation may only be used for the development of version 3.5.x of the e-Szignó Qualified Signature Creation and Management Trusted Module.

The security objectives for the operational environment of the Target of Evaluation (TOE) are identified by the prefix “OE”.

#Objective Identifier Description

1. OE.AUDIT_GENERATION The IT environment is capable of detecting and recording security-relevant events attributable to users.

2. OE.AUDIT_PROTECTION The IT environment is capable of protecting audit information.

3. OE.AUDIT_REVIEW The IT environment provides the capability to review audit information by applying specified filtering criteria.

4. OE. Configuration The IT environment has been properly installed and configured, enabling the TOE to operate securely from a known baseline..

5. OE.CORRECT_TSF_OPERATION The IT environment enables the testing of the TOE Security Functions (TSF), thereby ensuring that the security functions operate correctly on the user's computer.

6. OE.CRYPTOGRAPHY_HUN The TOE shall use the cryptographic services provided by the IT environment that are suitable for the intended purpose at the time of use and comply with applicable European and Hungarian laws, regulations, and other relevant requirements. Where the creation of a qualified electronic signature is required, the TOE operational environment shall include a Secure Signature Creation Device (SSCD/MALE) listed in the register maintained by the NMHH, together with all components required for its operation (e.g. a smart card reader and the corresponding device driver).

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

8. OE.Basic The TOE shall be designed and implemented to resist an attack potential classified as Basic by the vulnerability analysis.

9. OE.MANAGE The IT environment shall provide administrators with all functions and other necessary means required for the secure administration of the TOE, while preventing the unauthorized use of such functions and means.

10. OE.MEDIATE The IT environment shall protect user data in accordance with the applicable security policies governing such data.

11. OE.NO_EVIL The organization or user community operating the TOE shall ensure that administrators are non-malicious, appropriately trained, and follow all applicable administrative guidance.

MATRIX Auditing, Evaluating and Certification Ltd. Tax Identification Number: 11969608-2-13
2040 Budaörs, Szabadság út 290. Tel.: (23) 444 600 Internet: www.matrix-tanusito.hu E-mail: info@matrix-tanusito.hu

12. OE.PHYSICAL The non-IT environment shall provide a level of physical protection sufficient to prevent any unauthorized physical influence on the TOE or its exposure to side-channel attacks, such as power analysis or timing analysis.

13. OE.RESIDUAL_INFORMATION The IT environment must ensure that, in the event of reallocation of protected resources, the information stored within those resources is not disclosed publicly.

14. OE.SELF_PROTECTION The IT environment shall provide an execution environment for its own executable code that protects itself and its resources against unauthorized interference, modification, or disclosure.

15. OE.TIME_STAMPS The IT environment shall provide access to trusted time-stamping services and shall enable the administrator to set the system time in accordance with the trusted time stamps.

16. OE.TIME_TOE The IT environment shall provide the TOE with a trusted time source.

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

18. OE.TOE_PROTECTION The IT environment shall protect the TOE and its resources against unauthorized interference, unauthorized modification, and unauthorized disclosure.

5. Abbreviations

Acronym	Content
CC	Common Criteria
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
MM	Trusted Module

End of the document.

MATRIX Auditing, Evaluating and Certification Ltd. Tax Identification Number: 11969608-2-13
2040 Budaörs, Szabadság út 290. Tel.: (23) 444 600 Internet: www.matrix-tanusito.hu E-mail: info@matrix-tanusito.hu