HUNGUARD Ltd. • 1123 Budapest, Kékgolyó u. 6.
TEL: +36 1 792 0880 • FAX: +36 1 445 0414 WWW.HUNGUARD.HU

HUNGUARD

# Appendix M9:

# Certification procedure for remote qualified electronic signature/seal creation devices in accordance with Article 30(3)(b) of eIDAS

Digitálisan aláírta:
HUNGUARD

| | |
|---|---|
| Date: | 17.07.2023. |
| Made by: | Endrődi Zsolt Attila |
| Filename: | M9_QSCD_certification procedure_v11.docx |
| Version: | 1.1 |
| Classification: | Public |
| Pages: | 11 |

## Document history

| Version | Date | Specification |
|---|---|---|
| v0.1 | 2022. 10. 12. | **Initial version** |
| v0.2 | 2022. 10. 13. | Version for internal agreement 1 |
| v0.3 | 2022. 10. 17. | Version for internal agreement 2 |
| v1.0 | 2022. 10. 26. | Final version |
| **v1.1** | **2023. 07. 17.** | **Adoption of legislative changes** |

## Contents

# I. Introduction

As a designated certification body, HUNGUARD Ltd. evaluates and certifies qualified electronic signatures and/or qualified electronic seal creation devices according to eIDAS [1] with regard to compliance with the security requirements set out in Annex II [1].

This document describes the certification procedure followed by HUNGUARD Ltd. in accordance with Article [1] 30(3)(b) of eIDAS, which uses security levels corresponding to those required by Article [1] 30(3)(a) and is not applicable to the evaluation of QSCDs based on the requirements of Article [1]. 30(3)(a).

Note that Article 30(3)(a) of [1] refers to the security evaluation according to the common criteria of the "ISO/IEC 15408 Evaluation criteria for IT-Security" [6] in accordance with the security profiles defined in the related Commission Implementing Decision [2] whose security assurance level corresponds to the EAL4 security package enhanced by AVA_VAN.5.

## II. Subject of the certification

The Implementing Decision [2] defines in its Article 1 two main types of QSCDs:

- Type 1: devices used entirely but not necessarily exclusively in a user-managed environment;
- Type 2: devices managed on behalf of the user (signer or seal creator) by a qualified trust service provider (e.g. HSMs or signature servers where electronic signature or electronic seal creation data are securely stored and can only be accessed remotely by the user after authentication).

The Implementing Decision [2] explicitly states that the requirements for the security evaluation of Type 1 QSCDs according to Article 30(3)(a) of [1] are limited to:

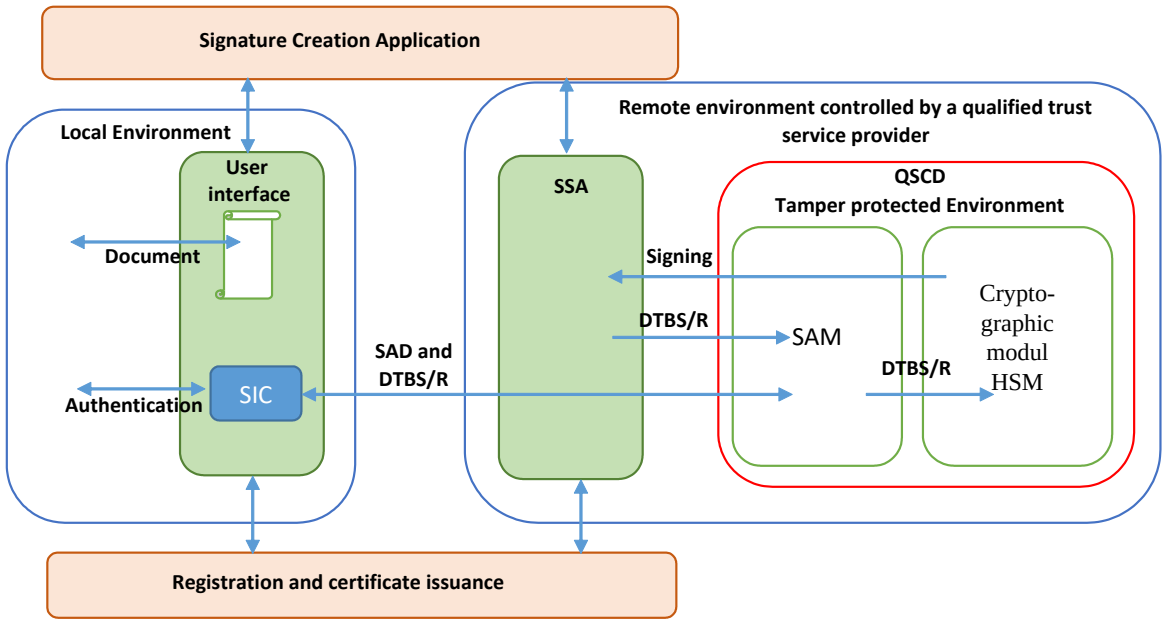
- ISO/IEC 15408 - Information technology — Security techniques — Evaluation criteria for IT security, Parts 1-3. [6] and CEM
- EN 419 211 - Protection profiles for secure signature creation device, Parts 1-6.

In contrast, for type 2 QSCDs, the Commission has not yet formally issued a list of standards, and the Implementing Decision [2] states that until then the certification of such products is based on an alternative procedure under Article 30(3)(b) of [1].

As a designated certification body, HUNGUARD Ltd. only certifies Type 2 QSCDs used for remote server signing and/or remote server sealing by a qualified trust service provider.

Type 2 QSCD is implemented by a combination of a cryptographic module and a signature activation module (SAM). The cryptographic module (HSM) provides the underlying cryptographic functions for secure key generation, signature generation, seal generation and key storage. The Signature Activation Module guarantees the signatory's sole control over the use of electronic signature and/or electronic seal creation data.

A trusted system supporting server signing can consist of local and remote environments. The signer is in the local environment and interacts with the server signing application in the remote environment through a local application. The figure below illustrates the location of a QSCD type 2 in this environment.




Type 2 QSCD is a combination of a cryptographic module and a SAM. The relevant security requirements are set out in the following Protection Profiles (PP) issued as European Standards:

- EN 419221-5 PP Cryptographic Module for Trust Services, [4] or the HSM, and
- EN 419241-2, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing, [5] for the signature activation module (SAM).

In addition to the compliance of the Type 2 QSCD with ISO/IEC 15408 protection profiles [4] and [5] HUNGUARD Ltd. also evaluates the compliance with Annex II [1]. The compliance of the use of protection profiles [4] and [5] with the requirements for QSCD Type 2 in relation to [1] is described in detail in a relevant ENISA study [8]. HUNGUARD Ltd. considers security profiles [4] and [5] to be appropriate for the assessment of QSCD Type 2, which correspond to security levels comparable to those referred to in Article 30(3)(a) of [1] and explicitly listed in the Implementing Decision [2].

HUNGUARD Ltd. will only carry out the certification if:

- the cryptographic module has been assessed and certified according to ISO/IEC 15408 (or Common Criteria) based on a security target that fully complies with the security profile in EN 419 211-5.

# III. The certification procedure

The certification procedure follows the certification scheme HUNG_TMK-2-QSCD according to the information provided by the certification body [9], but is carried out in the following phases, taking into account the additions set out in this document:

- Preparatory phase
- Evaluation phase of compliance with the requirements
- Evaluation result overview phase
- Decision and Certificate Issuance phase
- Assurance tracking phase

Note: The review in Chapter III.5 below is a continuous (not separable) activity after the certificate has been issued.

## III.1. Preparatory phase

Any manufacturer/developer, distributor or user, legally identifiable organisation (hereinafter referred to as the Applicant) may apply for the certification of QSCD Type 2 at the Certification Body, with the exception of manufacturers, service providers and distributors of products where the independence requirements under Article 4 of Act CXXXIII of 2009 on the activities of conformity assessment bodies are not met (see Article 3 (2) d) of Government Decree No. 227/2023 (08 June 2009) [3]). (Further measures taken to ensure impartiality are described in the Information Notice [9].

When submitting the application, the applicant must provide the following documents to the certification body:

a) A completed and signed Application Form (available on the website of HUNGUARD Ltd.);

b) Security Target (ST), claiming full compliance with the security profile of the European Standard EN 419241-2 [5];

c) Conformance mapping matrix showing that the TOE complies with the requirements specified in Annex II [1] in its operational environment (device with guidance);

d) A valid certificate of compliance with EN 419221-5 [4] for the cryptographic module used.

## III.2. Evaluation phase of compliance with the requirements

If all inputs are available:

- The Certification Body shall verify that all input documents are complete, accurate and valid according to the procedure set out in this document;
- The Evaluation Division of the Certification Body performs the verification of the claims in the ST according to ISO/IEC 18045 [7].

- The Certification Body verifies that the conformance mapping matrix demonstrates coverage of the requirements of Annex II [1].

In case of positive results, a conformity assessment report is issued.

In case of a negative result, the sponsor is informed of the reasons for refusing to issue the conformity assessment report.

### III.3. Evaluation result overview phase

At the end of the evaluation phase, the certifier will overview the findings of the evaluation. Validate whether they demonstrate compliance with the requirements of Annex II [1]. During the overview, the certifier examines the individual decisions in the conformity assessment report. Where necessary, he/she consults the evaluation manager or, in some cases, overviews the evidence of the evaluation.

### III.4. Decision and Certificate Issue phase

After the certification body has approved all the Applicant's inputs and the assessor's deliverables, the certification body will prepare a certification report, which will include a summary of the evaluation and the operational elements relevant to the end-user. The Certification Jury of HUNGUARD will take a decision on issuance of the certificate. The certificate issued by HUNGUARD Ltd (and published on its website together with the ST) will indicate the type of device associated with [1] and any comments deemed relevant for publication on the EU list of qualified electronic signature creation devices[1]. The certification documents will be sent to the national trust authority (NMHH).

The Certificate is valid for a maximum of 5 years, but not longer than the validity of the cryptographic module certificate.

### III.5. Review procedure

The certificate issued is subject to revision due to regulatory or scientific and technological changes. In such a case, a review report will be issued if the certified product still meets the revised requirements on the basis of the documentation previously submitted.

The review procedure is initiated by the certification body while informing the Applicant, but the Applicant may also initiate the review procedure.

If there is not enough information to issue a review report or if the certified product needs to be modified in order to maintain the certification of the certified product, the assurance tracing phase of the certification procedure needs to be initiated, and the Certification Body (if it has initiated the procedure independently) will inform the Applicant.

[1] https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD

### III.6. Assurance tracking phase

QSCD certification is only valid for the SAM and HSM versions tested (which are identical to the software submitted for testing). In the case of any change (whether bug fixes or new features), the validity of the Certificate cannot be automatically transferred to the new version. To deal with such cases, the assurance tracking phase is provided according to chapter II.7 of the Guide [9].

## IV. References

[1] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[2] COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

[3] Government Decree No 227/2023 (8 June) on the designation for conformity assessment activities of qualified electronic signature and qualified electronic seal devices and on specific rules for the activities of the designated organisations

[4] EN 419221-5, Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services

[5] EN 419241-2, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing

[6] ISO/IEC 15408 — Information technology — Security techniques — Evaluation criteria for IT security, Parts 1 to 3 and CEM

[7] ISO/IEC 18045 Information technology — Security techniques — Methodology for IT security evaluation

[8] Enisa, Assessment of Standards related to eIDAS Recommendations to support the technical implementation of the eIDAS Regulation NOVEMBER 2018

[9] Information on the use of the Certification Body certification procedures

[10] Quality Management Manual of the Certification Division

## V. Abbreviations

| | |
|---|---|
| AVA_VAN | Vulnerability analysis |
| CEN | Comité Européen de Normalization (European Committee for Standardization) |
| DTBS/R | Data To Be Signed Representation |
| EAL | Evaluation Assurance Level |
| eIDAS | REGULATION (EU) No 910/2014 |
| EN | European Standard |
| ENISA | European Union Agency for Cybersecurity |
| HSM | Hardware Security Module |
| IEC | International Electrotechnical Commission |
| ISO | International Organization for Standardization |
| PP | Protection Profiles |
| QSCD | qualified electronic signature/seal creation devices |
| SAD | Signature Activation Data |
| SAM | Signature Activation Module |
| SIC | Signer's Interaction Component |
| SSA | Server Signing Application |
| ST | Security Targets |
| TOE | Target of Evaluation |