TTE-71-07_02

Remote Qualified Electronic Signature Creation Device Evaluation Methodology

Edition : 1.

Version : 1.

Valid from : 2022.12.13.

Version	Changed pages	Date	Made by	Checked
1	Document creation	2022.04.04.	Molnár Ádám	dr. Solymár Eszter
1	Evaluation process	2022.12.13.	Molnár Ádám	dr. Solymár Eszter

Index

1. REFERENCES

- 41/2016. (X.13.) decree of Internal Ministry
- 470/2017. (XII. 28.) Government decree
- 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 (eIDAS) and repealing Directive 1999/93/EC
- Commission Implementing Decision (EU) 2016/650 of 25 April 2016
- CEN EN 419 241-2:2019 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing
- EN 419221-5, PP Cryptographic Module for Trust Services (note: TS 419 221-6 – provides conditions for use of EN 419 221-5 as a qualified electronic signature or seal creation Device)
- EN 419 211 — Protection profiles for secure signature creation device, Parts 1 to 6
- ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security
- ISO/IEC 18045 Information technology — Security techniques — Methodology for IT security evaluation
- Common Criteria Recognition Arrangement as published on the website commoncriteriaportal.org
- Enisa, Assessment of Standards related to eIDAS Recommendations to support the technical implementation of the eIDAS Regulation NOVEMBER 2018

2. ACRONYMS

CAP	Composition Assurance Package
ESR	Essential Security Requirements
rSCDev	Remote Electronic Signature Creation Device
rQSCDev	Remote Qualified Electronic Signature Creation Device
SAM	Signature Activation Module
SCDev	Signature Creation Device
SISECS	Spanish Information Security Evaluation and Certification Scheme
SSA	Server Signing Application
TW4S	Trustworthy System Supporting Server Signing

3. INTRODUCTION

The purpose of a Remote Qualified Electronic Signature Creation Device (rQSCDev) is to produce a digital signature, created on behalf of, and under sole control of, a natural person or a legal person, which may be recognised as a qualified electronic signature as defined in the eIDAS 2 Regulation.

4. SCOPE

Trustworthy System Supporting Server Signing (TW4S) may consist of a local and remote environment. The signer is in the local environment and interacts through a local application with the Server Signing Application (SSA) in the remote environment.

To ensure the signer has sole control of his signature keys, the signature operation needs to be authorized. This is carried out by a Signature Activation Module (SAM) which can retrieve and activate the signing key within a Signature Creation Device (SCDev), normally implemented as a Cryptographic Module. The Signature Creation Device and the SAM are to be located within a common tamper resistant environment that may be considered as the Remote Signature Creation Device (rSCDev).

The rSCDev, in combination with the SSA, are the basis for the TW4S, that need to be operated in a secure manner, and meeting some requirements for the system to be qualified as such.

5. EVALUATION METHODOLOGY

Until the establishment by the Commission of a list of standards for the security assessment of information technology products that apply to the certification of qualified electronic signature creation devices, where a qualified trust service provider manages the electronic signature creation data on behalf of a signatory, the certification of such products shall be based on an process that, pursuant to Article 30(3)(b), uses security levels comparable to those required by Article 30(3)(a) and that is notified to the Commission by the public or private body referred to in paragraph 1 of Article 30 of Regulation (EU) No 910/2014.

6. SCOPE OF EVALUATION

6.1. QSCD types

QSCD type A:

QSCD devices to be used in an environment entirely, but not necessarily exclusively managed by the user. (For example: Signing smart cards)

QSCD type B:

rQSCD devices managed on behalf of the user (signatory or creator of a seal) by a Qualified Trust Service Provider (QTSP) (for example: HSMs or signature servers where electronic signature or electronic seal creation data are stored securely, and that can be remotely accessed by the user only upon authentication).

In contrast with QSCD type A, for QSCD type B, no list of standards has yet been formally released by the Commission and document [2] states that, until then, the certification of such products shall be based on an alternative process that, pursuant to Article 30(3)(b) of eIDAS.

The present document defines the following as suitable devices to be assessed as alternative process pursuant to Article 30(3)(b) of eIDAS:

QSCD type B to be used by a QTSP for remote server signing and/or remote server sealing.

Note that a Type 2 QSCD is realized by the combination of a Cryptographic Module and a dedicated Signature Activation Module (SAM). The Cryptographic Module provides the underlying cryptographic functionalities for secure key generation,

signature generation, seal generation and key storage. The Signature Activation Module ensures sole control of the signatory over the use of his electronic signature creation data and/or electronic seal creation data.

6.2. QSCD certification cases

The folllowing cases exist for QSCD certification under eIDAS:

6.2.1. Case 1:

The Security Target of a Type 1 QSCD claims strict conformance to Protection Profile "EN 419221-5 PP Cryptographic Module for Trust Services",. MATRIX Ltd. eIDAS Designated Body considers "EN 419221-5 PP Cryptographic Module for Trust Services" an appropriate Protection Profile for assessment of QSCD type A that meets comparable security levels with respect to those referenced in Article 30(3)(a) of eIDAS and explicitly listed in The Commission Implementing Decision (EU) 2016/650 of 25 April 2016.

Note:

In addition to CC conformance of the Type 1 QSCD against the Protection Profile in EN 419221-5, MATRIX Ltd. assesses compliance with Annex II of eIDAS.

6.2.2. Case 2:

The Type 2 QSCD is a combination of HSM and SAM and their respective Security Targets claim strict conformance to the following Protection Profiles (PP):

- "EN 419221-5 PP Cryptographic Module for Trust Services", for the HSM, and
- "EN 419241-2, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing", for the Signature Activation Module (SAM).

Note:

In addition to CC conformance of the Type B QSCD against the Protection Profiles in EN 419221-5 and EN 419241-2, MATRIX Ltd. assesses compliance with Annex II of eIDAS. The adequacy of usage of PPs EN 419221-5 and EN 419241-2 in coverage of the requirements for Type B QSCD in relation with eIDAS is extensively described in „Enisa, Assessment of Standards related to eIDAS Recommendations to support the technical implementation of the eIDAS Regulation NOVEMBER 2018". MATRIX Ltd. considers EN 419221-5 and EN 419241-2 appropriate Protection Profiles for

assessment of Type B QSCD that meet comparable security levels with respect to those referenced in Article 30(3)(a) of eIDAS and explicitly listed in 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, or a valid successor.

6.2.3. Case 3:

The following scenario is possible for QSCD type A or QSCD type B evaluated in the context of a Common Criteria security accordingly to the “ISO/IEC 15408 Evaluation criteria for IT-Security” based on Security Target(s) that claim either no conformance to any PP or conformance to other PPs. The security objectives together with the security objectives for the operational environment must ensure that the security claim is in line with the requirements from Annex II of eIDAS and that the statement of security problem definition is equivalent or more restrictive than the statement of security problem definition in the PP(s) referenced in Article 30(3)(a) of eIDAS.

7. CERTIFICATION PROCESS

7.1. Application for certification

In order to apply for a QSCD certification the applicant should send an application form or e-mail containing the relevant information about the product to be certified.

The application form for QSCD certification can be downloaded from the follwing pages:

[HU] https://matrix-tanusito.hu/letoltheto-anyagok/ or [ENG] https://eng.matrix-tanusito.hu/letoltheto-anyagok/.

7.2. Non-Disclosure-Agreement (NDA)

If the application is valid, MATRIX Ltd. will contact the applicant for further information and sends a NDA to be signed by both parties.

7.3. Documentation submission

After the NDA the following documents are necessary to be submitted for the certification:

- Security Target (ST) as detailed in section 'Scope of Assessment' of this document;
- Compliance Mapping Matrix indicating coverage by the TOE in its operational environment (device with guidance) of the requirements laid down in Annex II of Eidas;
- (if available) Security certificate of the TOE against the ST and obtained according to the Common Criteria (ISO/IEC 15408);
- Product documentation according to Common Criteria (ISO/IEC 15408).

7.4. Evaluation

7.4.1. Evaluation A:

MATRIX Ltd. prepares the evaluation project for the product certification if the documentation submission is complete and all input is available for evaluation.

MATRIX Ltd. either performs a product evaluation of the claims in the ST and verifies that all submitted documentation are complete, accurate and valid accordingt to the process defined in this document.

The examination of all input relies on the provided security certificates.

An evaluation of the compliance mapping matrix must justify that all requirements laid down in Annex II of eIDAS has been fulfilled.

Such evaluation relies on the input provided to verify that the the characterizations of the QSCD in scope and of the operational environment are in line with the designated scope defined in the evaluation scope.

In case of evaluation of a QSCD in the evaluation context of a Common Criteria security accordingly to the "ISO/IEC 15408 Evaluation criteria for IT-Security" based on Security Target(s) that claim either no conformance to any PP or conformance to other PPs MATRIX ltd. subcontracts the security evaluation to a trusted security testing laboratory that ensures that the security objectives of the Trget of Evaulation togheter with the security objectives of the TOE operating environment are in compliance with the requirements from Annex II of eIDAS and the statement of security problem definition is equivalen or more restrictive than the statement of security problem definition in the PP(s) of Article 30(3)(a) of eIDAS. In addition, it must be ensured that the evaluation conducted in this evaluation process reaches a security level (i.e. assurance level) comparable to those described in Article 30(3)(a) of eIDAS.

If all the requirements are fulfilled, the product certification is issued.

In case of negative outcome, the applicant is notified with an errata with the details of the refusal of product certification.

7.4.2. Evaluation B:

MATRIX Ltd. subcontracts the TOE Common Criteria evaluation to a trusted testing laboratory in order to produce security certificate and proceeds with process Evaluation A described in this document.

7.5. Release of the certificate

Once all applicant input and subcontractor deliverables have been approved by the MATRIX Ltd's certification body, the certification body creates an Evaluation Report. The certificate issued contains an annex with the summary of the evaluation and any important operational items relevant for the end-user. The certificate to be released by MATRIX Ltd. (and published together with the ST on [HU] https://matrix-tanusito.hu/tanusitvanyok-2/ and [ENG] https://eng.matrix-tanusito.hu/tanusitvanyok-2/) indicates the type of device related to eIDAS and any notes that are deemed to be relevant to be published on the compilation list of the EU.

MATRIX Ltd. notifies this process to the European Commission via National Media and Infocommunications Authority.