Certification Process for eIDAS conformant QSCDs of the certification body of TÜV Informationstechnik GmbH

Version 1.2 / 2020-10-27

Table of Contents

1 Introduction

TÜV Informationstechnik GmbH (short TÜViT) is a designated certification body according to articles 30.1 and 39.2 of Regulation (EU) 910/2014 [eIDAS] for the certification of conformity of qualified signature and seal creation devices (QSCDs) with the requirements laid down in Annex II of [eIDAS].

In this context, TÜViT offers companies certification services for QSCDs.

The EU commission has established a list of standards for the certification of the conformity of QSCDs with the requirements laid down in Annex II [eIDAS] by adopting the Commission Implementing Decision (EU) 2016/650 [CID (EU) 2016/650]. Article 1 of [CID (EU) 2016/650] distinguishes 2 types of QSCD:

1. Article 1.1 addresses QSCDs where the electronic signature creation data or electronic seal creation data is held in an entirely but not necessarily exclusively user-managed environment. Corresponding standards for the security assessment of IT products are listed in the Annex of [CID (EU) 2016/650].
2. Article 1.2 addresses QSCDs where the qualified trust service provider manages the electronic signature creation data or seal creation data on behalf of a signatory or of a creator of a seal. No corresponding standards for the security assessment are included in [CID (EU) 2016/650]. Instead, it is required that security assessment of such IT products shall be based on a process that, pursuant to Article 30.3 (b), uses security levels comparable to those required by Article 30.3 (a) and that the corresponding process is notified to the Commission by the public or private body referred to in paragraph 1 of Article 30 of [eIDAS].

In the context of Article 1.2 of [CID (EU) 2016/650], TÜViT established a process which uses security levels comparable to those required by Article 30.3 (a).

The present document describes the process for the certification of QSCDs where the qualified trust service provider manages the electronic signature creation data or seal creation data on behalf of a signatory or of a creator of a seal. The document is intended to be used for notification to the European Commission.

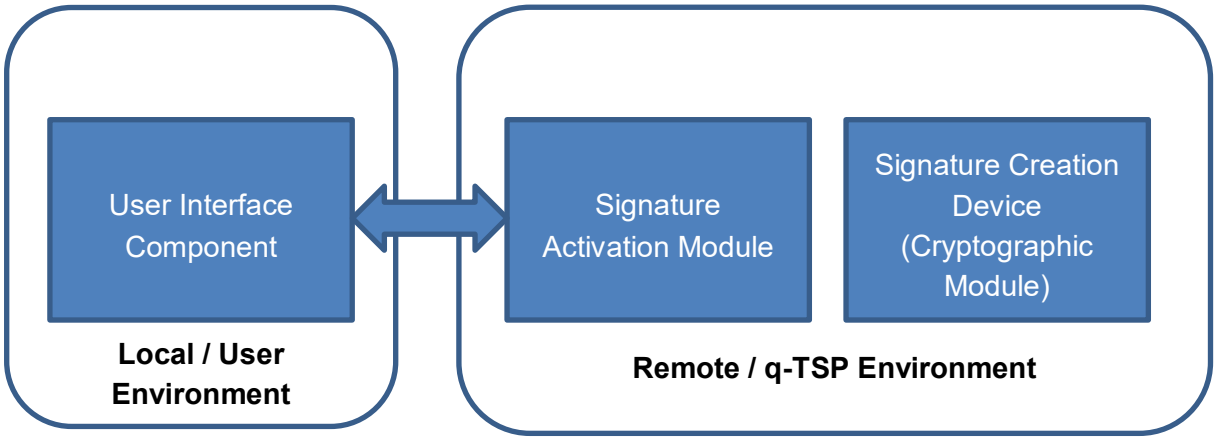
2 Scope

QSCDs where the qualified trust service provider (short: q-TSP) manages the electronic signature creation data or seal creation data on behalf of a signatory or of a creator of a seal (short: remote QSCD or r-QSCD) typically consists of 3 components that are operated in a local (user) and a remote (q-TSP) environment:

1. A User Interface Component that is operated in the local environment, where the signer / seal creator enters authentication data that is transmitted via a secure channel to the Signature Activation Module. A secure channel is also used to transmit data to be signed/sealed from the signature creation application to the r-QSCD.
2. A Signature Activation Module that is operated in the remote environment, used to manage authentication of different signers / seal creators.
3. A Signature Creation Device, typically a cryptographic module, that is operated in the remote environment and which is used to protect and manage signature / seal creation data of different signers / seal creators.

Note: The Signature Creation Application that create signed / sealed documents is not part of the r-QSCD. Details can be found in EN 419241-2.

This is illustrated in the following figure:



3 Certification Process

The basis of the certification of a r-QSCD according to articles 30.3 (b) and 39.2 of [eIDAS] is a security evaluation according to Common Criteria [ISO/IEC 15408-1], [ISO/IEC 15408-2], [ISO/IEC 15408-3]. Common Criteria (CC) is listed in the annex of [CID (EU) 2016/650] as standard for the evaluation of QSCD where the electronic signature creation data or the electronic seal creation data are held in an entirely but not necessarily exclusively user-managed environment. This standard is considered equally suitable for certification of r-QSCDs.

During security evaluation of a r-QSCD according to CC the following evidences must be provided:

- Security relevant parts of the r-QSCD implementing functionality of the Signature Activation Module or the Signature Creation Device (Cryptographic Module) must be evaluated according the minimum CC Evaluation Assurance Level EAL4 augmented with AVA_VAN.5.
- The Security Target for the r-QSCD shall take into account requirements from the certified Protection Profiles [EN 419241-2] and [EN 419221-5].
- The Security Target for the r-QSCD shall demonstrate that the Security Objectives, Security Functional Requirements and Security Functions are sufficient to fulfil requirements of Annex II of [eIDAS].
- A successful CC evaluation shall be proven by a corresponding CC certificate.

Alternatively, in case that the operation of the r-QSCD is restricted to one dedicated QTSP only, the evaluation assurance level EAL4 augmented with AVA_VAN.5 may be replaced by an appropriate assurance package that takes into consideration the dedicated operating environment of the QTSP. The components of the assurance package shall be agreed with the certification body before starting the evaluation and certification process. The environment of the dedicated QTSP together with the evaluation assurance package shall mentioned in the security target.

The successful certification of the r-QSCD will result in a r-QSCD certificate, which states the fulfilment of requirements of Annex II of [eIDAS] on r-QSCDs. The validity period of the r-QSCD certificate depends on the strength of security mechanisms and algorithms that are implemented in the product and shall not exceed a maximum period of 5 years. At a given time, the validity period can be extended or shortened if there are new findings regarding the suitability of security mechanisms or algorithms.

Issuance and withdrawal of r-QSCD certificates will be published in the list of certificates on the website of TÜViT.

According to article 31.1 of [eIDAS] Member States shall notify to the Commission without undue delay and no later than one month after the certification is concluded, information on

qualified electronic signature creation devices that have been certified by the bodies referred to in Article 30.1 and they shall also notify to the Commission, without undue delay and no later than one month after the certification is cancelled, information on electronic signature creation devices that are no longer certified. TÜViT will inform the German supervisory body about the issuance and the withdrawal of r-QSCD certificates.

4 Standards

[CID (EU) 2016/650]	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
[eIDAS]	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
[EU QSCD list]	Compilation of: Member States' notifications on: Designated Bodies under Article 30(2) and 39(2) of Regulation 910/2014 and Certified Qualified Signature Creation Devices under Article 31(1)-(2), and Certified Qualified Seal Creation Devices under Article 39(3) of Regulation 910/2014, and information from Member States on: Secure Signature Creation Devices benefiting from the transitional measure set in article 51(1) of Regulation 910/2014
[ISO/IEC 15408-1]	ISO/IEC 15408-1:2009 – Information technology – Security techniques – Evaluation criteria for IT security – Part 1 ISO, 2009
[ISO/IEC 15408-2]	ISO/IEC 15408-2:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 2 ISO, 2008
[ISO/IEC 15408-3]	ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3 ISO, 2008
[EN 419 221-5]	CEN/EN 419 221-5:2018, Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services
[EN 419 241-2]	CEN/EN 419 241-2:2019, Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing

5 Glossary

term	explanation
CC	Common Criteria
eIDAS	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
evaluation	comprises the activities audit, testing, inspection, design appraisal, assessment of services and processes as well as other activities for determination of characteristics of products by conformity assessment
QSCD	Qualified signature/seal creation device
r-QSCD	Remote QSCD
r-QSCD certificate	Certificate which states the fulfilment of requirements of Annex II of [eIDAS] on r-QSCDs
ST	Security target
TSP	Trust Service Provider
q-TSP	Qualified Trust Service Provider