# Certification of the conformity of QSCDs for server-signing with the requirements laid down in Annex II of Regulation (EU) No. 910/2014

**Version**
1.0

**Date**
14.09.2017

**Designated Body**
SRC Security Research & Consulting GmbH
Emil-Nolde-Straße 7
53113 Bonn

## Document revisions

| Version | Date | Amendments | Author |
|---|---|---|---|
| 0.1 | 11.09.2017 | First internal version | SRC |
| 0.2 | 12.09.2017 | Quality Assurance | SRC |
| 1.0 | 14.09.2017 | First version | SRC |

## Contents

# 1 Introduction

For the certification of the conformity of qualified electronic signature creation devices and qualified electronic seal creation devices (QSCD[1]) with the requirements laid down in Annex II of the eIDAS regulation [eIDAS] the EU commission has adopted the Commission Implementing Decision (EU) 2016/650 [CID (EU) 2016/650]. The corresponding Annex consists of a list of standards to be used for the security evaluation process, where the electronic signature resp. seal creation data is held in an entirely but not necessarily exclusively user-managed environment ([CID (EU) 2016/650], Article 1 (1)). In the case where a qualified trust service provider manages the electronic signature resp. seal creation data on behalf of a signatory resp. of a creator of a seal, the certification of such 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 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 ([CID (EU) 2016/650], Article 1 (2)).

Based on this situation the designated certification body “SRC Security Research & Consulting GmbH” notifies to the Commission a security evaluation process for the certification of QSCDs to be used for the so-called server-signing scenario.

Remark: SRC Security Research & Consulting GmbH is one of the German’s designated certification bodies as stated in the list of certified qualified electronic signature creation devices and qualified electronic seal creation devices (cf. [EU QSCD list], section GERMANY (DE)).

[1] In the following the abbreviation QSCD is used for both, qualified signature creation devices as well as qualified seal creation devices

## 2 Security Evaluation Process

The security evaluation process notified to the Commission consists of a security evaluation according to the “ISO/IEC 15408 Evaluation criteria for IT-Security” (Common Criteria Evaluation, cf. [ISO/IEC 15408-1], [ISO/IEC 15408-2], [ISO/IEC 15408-3]) as already listed in the Commission Implementing Decision (EU) 2016/650 [CID (EU) 2016/650] and the use of the following two protection profiles (PP):

- „EN 419221-5 PP Cryptographic Module for Trust Services“ [prEN 419221-5], and
- „EN 419241-2, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing“ [prEN 419241-2].

So the main difference of this security evaluation process is the use of two protection profiles that are not listed yet in [CID (EU) 2016/650]. Under the standardisation mandate M/460 given by the Commission these PPs were developed by CEN/TC224/WG17 for the security evaluation process of QSCDs for server-signing. For this both PPs have to be used, EN 419221-5 for the security evaluation of the cryptographic module and EN 419241-2 for the security evaluation of the signature activation module (SAM). SAM and the cryptographic module realise the QSCD.

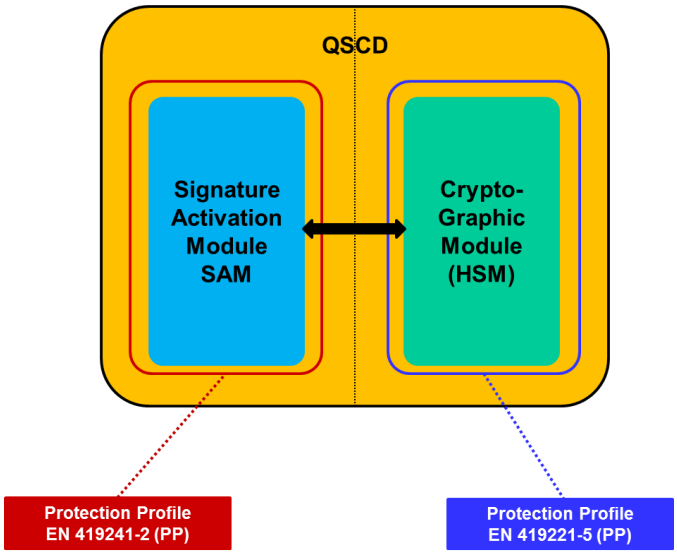


**Figure 1: QSCD and related Protection Profiles**

In the above mentioned PPs the Evaluation Assurance Level EAL4+ (EAL 4 augmented with AVA_VAN.5) is claimed. Hereby the achieved security level of the notified security evaluation process is comparable to the security level defined by the listed security evaluation process.

Both documents are under approval and already stable, essential changes of the contents or the defined requirements should not happen anymore. The version 0.15 of EN 419221-5 is

already certified (cf. certification report [ANSSI CRP]) and available via the official Website of Common Criteria (www.commoncriteriaportal.org). The CEN Enquiry for the protection profile EN 419241-2 was successfully finished on August, 3rd 2017 (closing date) and the evaluation of the PP is also in the final stage. The certification of EN 419241-2 is expected for nearly Q4/2017 or Q1/2018.

Furthermore it can be assumed that these PPs will become part of the list in the Commission Implementing Decision (EU) 2016/650 [CID (EU) 2016/650] after their certification.

Therefore the notified security evaluation process is an obvious solution for the certification of products based on a process pursuant to Article 30(3)(b) of Regulation (EU) No. 910/2014.

# 3 References


[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

[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

[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

[prEN 419221-5] CEN/prEN 419221-5:2016, Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services, v0.15, 2016-11-29

[ANSSI CRP] ANSSI, Rapport de certification ANSSI-CC-PP-2016/05 du profil de protection “Protection profiles for TSP Cryptographic modules - Part 5-Cryptographic Module for Trust Services” (prEN 419 221-5, version 0.15), 16.12.2016

[prEN 419241-2] CEN/prEN 419241-2:2017, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing, v0.12, 2017-06, or newer version

# 4 List of acronyms

| | |
|---|---|
| CC | Common Criteria |
| CEN | European Committee for Standardization |
| CID | Commission Implementing Decision |
| EAL | Evaluation Assurance Level |
| EN | European Norm |
| HSM | Hardware Security Module |
| PP | Protection Profile |
| QSCD | Qualified Signature / Seal Creation Device |
| SAM | Signature Activation Module |
| SCD | Signature Creation Data |
| ST | Security Target |
| TC | Technical Committee |
| WG | Working Group |