eIDAS: Dutch Conformity Assessment Process

Certification of qualified electronic signature creation devices and/or qualified electronic seal creation devices according to the security requirements laid down in Annex II of Regulation (EU) No. 910/2014 [1]

Version 5.0, July 26th, 2019

Contents

1. Document objective

TUV Rheinland Nederland bv (TRN) is the Dutch eIDAS-Designated Body (certificerende instelling gekwalificeerde middelen aanmaken elektronische handtekeningen cf. [3]), responsible in The Netherlands for the assessment of the conformity of qualified electronic signature and/or qualified electronic seal creation devices (defined in Article 3 of [1] and hereafter referred to as QSCD) to the security requirements laid down in Annex II of [1]. TRN operates the Netherlands Scheme for Certification in the Area of IT Security (NSCIB) [7] based on [12] with qualified ITSEFs [8].

This document describes the Dutch Conformity Assessment Process (DCAP), pursuant to Article 30(3)(b) of [1], that:

- uses security levels comparable to those required by Article 30(3)(a) of [1] and is applicable for assessment of QSCD that do not fulfil the requirements laid down in Article 30(3)(a) of [1]. Note that Article 30(3)(a) of [1] refers to a Common Criteria security evaluation according to the

"ISO/IEC 15408 Evaluation criteria for IT-Security" [12] under Protection Profiles [13], which are conformant to assurance package EAL4 augmented with AVA_VAN.5.

- is notified to the Commission by the public or private body referred to in paragraph 1 of Article 30 of [1]. The process and the formal steps to reach the assessment of conformity of a QSCD against requirements laid down in Annex II of [1] under the authority of the Dutch eIDAS Designated Body is described in this document.

2. Scope of Assessment

Based on indications contained in Article 1 of [2], two main types of QSCD are considered in scope of this conformity assessment:

- **Type 1 QSCD**: devices to be used in an environment entirely but not necessarily exclusively managed by the user;

- **Type 2 QSCD**: devices managed on behalf of the user (signatory or creator of a seal) by a Qualified Trust Service Provider (QTSP) (for ex., 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).

Document [2] explicitly states that, according to Article 30(3)(a) of [1], the standards for the security assessment of **Type 1 QSCD** are limited to:

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

In contrast, for **Type 2 QSCD**, 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 [1].

The present document defines the following as suitable devices to be assessed under DCAP as alternative process pursuant to Article 30(3)(b) of [1]:

- **Type 1 QSCD** that cannot claim conformance to [13] and hence cannot fulfil the requirements of Article 30(3)(a) of [1]. Note that the Protection Profiles in [13] are only applicable to Type 1 signature creation devices based on smartcards, USB tokens and similar. As a consequence, Cryptographic Modules in form of a hardware security module (HSM) cannot claim conformance to such Protection Profiles despite being technically and from security point of view suitable to be used as Type 1 QSCD in the sense of eIDAS. For an HSM to be certified as Type 1 QSCD, an alternative process pursuant to Article 30(3)(b) of [1] must be used as long as no suitable protection profiles are referenced in Article 30(3)(a) of [1] and listed in [2].
- **Type 2 QSCD** 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.

DCAP under the Dutch eIDAS Designated Body, as notified to the Commission with this document, consists of a Common Criteria security evaluation according to the "ISO/IEC 15408 Evaluation criteria for IT-Security" [12] (as already listed in the Commission Implementing Decision (EU) 2016/650 [2]) under either of the following cases.

- **Case A**: The Security Target of a Type 1 QSCD claims strict conformance to Protection Profile "EN 419221-5 PP Cryptographic Module for Trust Services", [10]. The Dutch eIDAS Designated Body considers [10] an appropriate Protection Profile for assessment of Type 1 QSCD that meets comparable security levels with respect to those referenced in Article 30(3)(a) of [1] and explicitly listed in [2].

  Note 1:

  - *In addition to CC conformance of the Type 1 QSCD against the Protection Profile in [10], DCAP assesses compliance with Annex II of [1].*

- **Case B**: 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", [10] for the HSM, and
  - "EN 419241-2, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing", [11] for the Signature Activation Module (SAM).

  Note 2:

  - *In addition to CC conformance of the Type 2 QSCD against the Protection Profiles in [10] and [11], DCAP assesses compliance with Annex II of [1]. The adequacy of usage of PPs [10] and [11] in coverage of the requirements for Type 2 QSCD in relation with [1] is extensively described in [6]. The Dutch eIDAS Designated Body considers [10] and [11] appropriate Protection Profiles for assessment of Type 2 QSCD that meet comparable security levels with respect to those referenced in Article 30(3)(a) of [1] and explicitly listed in [2].*
  - *Case B trivially satisfies also Case A as the evaluation of the HSM against the requirements in Protection Profile [10] proves it suitable to be used either as a standalone Type 1 QSCD or as part of a Type 2 QSCD.*

- **Case C**: The Type 1 or Type 2 QSCD is evaluated in the context of a Common Criteria security evaluation according to the "ISO/IEC 15408 Evaluation criteria for IT-Security" [12] based on Security Target(s) that claim either no conformance to any PP or conformance to other PPs. In this scenario, 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 [1] 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 [1].

3. Assessment Process

3.1 Assessment phases and steps

DCAP can be divided into the following three phases:

1. Applying for conformity assessment:

   The Sponsor sends to NSCIB the following documents:

   a. Filled **application form** with indication for eIDAS compliance (can be downloaded from www.tuv-nederland.nl/nl/36/certification.html).
   b. **Security Target (ST)** as detailed in section 'Scope of Assessment' of this document.
   c. **Compliance Mapping Matrix** indicating coverage by the TOE in its operational environment (device with guidance) of the requirements laid down in Annex II of [1].
   d. (if available) **Security certificate** of the TOE against the ST and obtained according to the Common Criteria (ISO/IEC 15408).

2. Conformity Assessment:

   If all input **a**, **b**, **c**, **d** is available:

   - The ITSEF performs an examination of the claims in the ST (input b) and verifies that **all input documents** are complete, accurate and valid according to the process defined in this document.
   - The examination of all input relies on the provided security certificate (input d).
   - An assessment of the Compliance Mapping Matrix (input c) must justify the coverage of requirements in Annex II of [1].

     Note 3:
     Such examination:

     - *Relies on the provided input to verify that the characterizations of the QSCD in scope and of the operational environment are in line with the designated scope defined in section 'Scope of Assessment';*
     - *In the scenario described in Case C (section 'Scope of Assessment'), the ITSEF ensures that the security objectives of the Target of Evaluation (TOE) together with the security objectives of the TOE operating environment are in line with the requirements from Annex II of [1] and that the statement of security problem definition is equivalent or more restrictive than the statement of security problem definition in the PP(s) of Article 30(3)(a) of [1]. In addition, it must be ensured that the evaluation conducted in Case C reaches a security level (i.e. assurance level) comparable to those described in Article 30(3)(a) of [1].*
     - *The examination performed by the ITSEF does not include, either directly or indirectly, the conformity of a real environment to the security objectives for the operational environment defined in section 'Scope of Assessment'.*

   - In case of positive outcome, the conformity assessment report is issued (see next phase for further details);

- In case of negative outcome, the sponsor is notified with the reasons for refusal to issue the conformity assessment.

If document d (security certificate) is not available:

- In this scenario, NSCIB and the ITSEF (in line with NSCIB standard procedures described in [4] and [5]) first conduct the TOE Common Criteria evaluation in order to produce the security certificate and afterwards proceed with DCAP process as described in this document.

3. Release of conformity assessment certificate:

   Once all Sponsor input and ITSEF deliverables have been approved by the certifier, the certifier creates a Certification Report with a summary of the evaluation and any important operational items relevant for the end-user. The Certification Report is in line with the requirements of [12], [14] and [15]. The certificate to be released by TRN (and published together with the ST on [9]) indicates the type of device related to [1] and any notes that are deemed to be relevant to be published on the compilation list of the EU.

   TRN notifies this process to the European Commission via the Ministry of Economic Affairs.

3.2 Maintenance of eIDAS: Dutch Conformity Assessment Process

DCAP may be subject to revision due to changes in the regulatory, scientific and technological context of reference. In such a case, an updated version of this document will be released and submitted to the European Commission.

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, or a valid successor.

[3] Ministerie van Economische Zaken, Besluit van 22 februari 2017, houdende vaststelling van eisen inzake verlening van vertrouwensdiensten, tot intrekking van het Besluit elektronische handtekeningen en tot aanpassing van enige andere besluiten (Besluit vertrouwensdiensten)

[4] NSCIB Scheme Documentation, version as published on the NSCIB website

[5] NSCIB Scheme Procedure #6 Alternative Evaluator Reporting, version valid according to NSCIB List of reference documents

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

[7] www.tuv-nederland.nl/nl/17/common_criteria.html

[8] www.tuv-nederland.nl/nl/19/itsefs.html

[9] www.tuv-nederland.nl/nl/37/certificates.html

[10] 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)

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

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

[13] EN 419 211 — Protection profiles for secure signature creation device, Parts 1 to 6

[14] Common Criteria Recognition Arrangement as published on the website commoncriteriaportal.org

[15] SOGIS Recognition Agreement as published on the website sogis.eu

Terms and abbreviations

CCRA	Common Criteria Recognition Arrangement
DCAP	Dutch Conformity Assessment Process
eIDAS	electronic Identification, Authentication and Signatures *Note*: This is the informal name for Regulation 910/2014 [1]
HSM	Hardware Security Module
ITSEF	IT Security Evaluation Facility
NSCIB	Netherlands Scheme for Certification in the Area of IT Security
PP	Protection Profile
QSCD	Qualified Seal Creation Device or Qualified Seal Creation Device
(Q)TSP	(Qualified) Trust Service Provider
SAM	Signature Activation Module
SOGIS	Senior Officials Group Information Systems Security
ST	Security Target
TOE	Target Of Evaluation
TRN	TUV Rheinland Nederland bv

Document history

Version	*Date*	*Description*
3.0	28 February 2019	First public release
4.0	8 April 2019	Alignment
5.0	26 July 2019	Explicitly include Type 1 QSCD, and assessment experience