Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Conformity Assessment Procedure for qualified electronic signature and seal creation devices according to the security requirements laid down in Annex II of Regulation (EU) No. 910/2014

OCSI/ACC/01/2016/PROC-EN

Version 1.0

21 December 2016

This page is intentionally left blank

1 Document revisions

Version	Author(s)	Amendments	Date
1.0	OCSI	First issue	21/12/2016

2 Contents

3 List of acronyms

EAL Evaluation Assurance Level

HSM Hardware Security Module

OCSI Organismo di Certificazione della Sicurezza Informatica

PP Protection Profile

SCD Signature Creation Data

ST Security Target

TOE Target of Evaluation

USB Universal Serial Bus

4 References

[R01] “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”, Official Journal of the European Union L 257, 28 August 2014.

[R02] Legislative decree of 7 March 2005, No. 82, “Codice dell'amministrazione digitale”, amended and supplemented by legislative decree of 26 August 2016, No. 179, G.U. No. 214 of 13 September 2016.

[R03] CCRA, “Common Criteria Recognition Arrangement”, 2 July 2014.

[R04] “The Common Criteria for Information Technology Security Evaluation”, <www.commoncriteriaportal.org>.

[R05] CCMB-2009-07-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 3, July 2009.

[R06] CCMB-2009-07-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 3, July 2009.

[R07] CCMB-2009-07-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 3, July 2009

[R08] Joint ministerial decree of 15 February 2006, “Individuazioni delle prestazioni, eseguite dal Ministero delle Comunicazioni per conto terzi, ai sensi dell’articolo 6 del Decreto Legislativo 30 dicembre 2003, n. 366”, G.U. No. 82, 7 April 2006.

[R09] Law of 7 August 1990, No. 241, “Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi”, G.U. No. 19, 18 August 1990, as amended and supplemented.

[R10] “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”, Official Journal of the European Union L 109/40, 26 April 2016.

[R11] SOGIS-MRA “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates", version 3.0, January 2010.

[R12] “SOGIS Portal”, <www.sogisportal.eu>.

[R13] “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”, ETSI TS 119 312 V1.1.1 (2014-11).

[R14] “OCSI – Organismo di certificazione della Sicurezza Informatica”, <www.ocsi.isticom.it>

5 Foreword

A. OCSI (*Organismo di Certificazione della Sicurezza Informatica*) is the body designated according to paragraph 1 of article 30 of Regulation (EU) No. 910/2014 on digital identity - eIDAS (Electronic IDentification, Authentication and Signature) [R01] (hereinafter referred to as “eIDAS Regulation”), and notified according to paragraph 2 of the same article, as the authority responsible in Italy for the assessment of the conformity of a qualified electronic signature and/or qualified electronic seal creation device to the security requirements laid down in Annex II of the aforementioned eIDAS Regulation.

B. OCSI’s designation for the above conformity assessment is established in paragraph 5 of article 35 of legislative decree of 7 March 2005, No. 82, “Codice dell'amministrazione digitale”, amended and supplemented by legislative decree of 26 August 2016, No. 179 [R02].

C. This Assessment Procedure applies to qualified electronic signature and/or qualified electronic seal creation devices (hereinafter, for the sake of brevity, referred to as “signature devices” or “devices”), as defined in article 3 of eIDAS Regulation, covering all cases provided for in paragraph 3 of article 30 of the same Regulation.

D. For devices that successfully pass the Conformity Assessment Procedure, an Attestation of Conformity is issued whose validity is subject to the conditions and assumptions made explicit in the accompanying Assessment Report.

E. The issuance of the Attestation of Conformity requires, for the device submitted for assessment, a security certification deemed adequate by OCSI for the purpose of fulfilling the security requirements laid down in Annex II of eIDAS Regulation.

F. A security certification obtained according to the evaluation standard known as *Common Criteria* [R04] (ISO/IEC 15408) is a necessary but not sufficient condition for the adequacy referred to in sec. E.

G. The Assessment Procedure may be subject to revision due to changes in the regulatory, scientific and technological context of reference. In such a case, OCSI publishes the new version of the procedure on its official website [R14], in the section dedicated to signature devices, while keeping an archive of the previous issues.

H. Fees due to OCSI for the application of the Assessment Procedure are calculated according to the joint ministerial decree of 15 February 2006 [R08].

I. The application of the Assessment Procedure is governed by current Italian legislation on administrative procedures [R09].

6 Introduction to the Conformity Assessment

A. Based on the indications contained in the Implementing Decision (EU) 2016/650 [R10], two main types of signature devices are considered:

   i. **Type 1 devices**: devices to be used in an environment entirely but not necessarily exclusively managed by the signature keys owner (for ex., smartcards, USB tokens and similar devices);

   ii. **Type 2 devices**: devices managed on behalf of the user (signatory or creator of a seal) by a qualified trust service provider (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).

B. For both of the above device types a *Common Criteria* certification deemed adequate by OCSI is required.

C. This Assessment Procedure is based on the following elements of the *Common Criteria* certification model:

   i. the Security Target (ST), which provides the security characterisation of the Target of Evaluation (TOE) and the TOE environment and, in particular, identifies the security objectives for the TOE and for the TOE environment;

   ii. the Certificate, which provides evidence that a *Common Criteria* certification has been carried out for a given device as the realisation of the TOE described in a given ST, under the assumption that the environment of the device meets the security objectives for the TOE environment.

D. This Assessment Procedure defines the key requirements for the ST (chap. 7, par. A, B, and C) and for Certificate recognition (chap. 7, par. D) for the purpose of fulfilling the security requirements laid down in Annex II of eIDAS Regulation [R01].

E. OCSI is available, upon request, to consider the possibility of adapting the constraints referred to in par. D to specific cases. In case of issuance of the Attestation of Conformity, such adaptations shall be stated in the accompanying Assessment Report, referred to in chap. 11, par. B.

F. The elements jointly contributing to the adequacy of a ST are:

   i. the security characterisation of the TOE;

   ii. the security characterisation of the TOE operating environment.

G. It must be noted that this Assessment Procedure:

   i. directly analyses the security characterisations referred to in par. F;

   ii. does not directly analyse the conformity of an actual device to the security characterisation of the TOE, relying for this aspect on the evidence provided in the Certificate referred to in point C.ii;

iii. does not analyse, either directly or indirectly, the conformity of a real environment to the security characterisation of the TOE environment.

H. The characteristics of the Attestation of Conformity are given in chap. 11.

I. This Assessment Procedure provides two alternative modalities of execution:

i. **Modality 1**: the first modality is recommended for cases where the Certificate is available at the start of the Procedure, and consists of a single phase that ends with the issuance of the Attestation of Conformity or with a communication of the reasons for the refusal to issue.

ii. **Modality 2**: the second modality is recommended for cases where the Certificate is not available at the start of the Procedure, and the certification process has not yet been started or is in an early stage. The second modality consists of a first phase that ends with a preliminary Pronouncement (Positive or Negative) regarding the examined information materials. In case of a Positive Pronouncement, the second modality of the procedure continues into a second phase starting upon delivery of the Certificate, that ends with the issuance of the Attestation of Conformity or with a communication of the reasons for the refusal to issue.

7 Adequacy of the Common Criteria certification

A. For **Type 1 devices**, referred to in chap. 6, point A.i, for the purposes of the Conformity Assessment the ST must claim conformance to one or more, as needed, of the *Protection Profiles* (PPs) indicated in the Annex to the Implementing Decision (EU) 2016/650 [R10].

B. For **Type 2 devices**, referred to in chap. 6, point A.ii, for the purposes of the Conformity Assessment the ST must meet the following adequacy requirements:

   i. the ST must claim conformance to *Common Criteria* version 3.1, Revision 3 ([R05], [R06], [R07]) or later;

   ii. the ST must claim conformance to the EAL4 assurance package augmented with the assurance component AVA_VAN.5;

   iii. the security objectives of the TOE, together with the security objectives of the TOE operating environment, must ensure the fulfillment of the security requirements laid down in Annex II of eIDAS Regulation [R01];

   iv. the division between the security objectives of the TOE and the security objectives of the TOE operating environment must be such that the TOE includes all the security functions involving signature keys (SCDs) for any operation related to their entire life cycle;

   v. with reference to the previous point, the TOE must include the signature key (SCD) generation function;

   vi. to fulfill requirement 1, point (d) of Annex II of eIDAS Regulation, the TOE must contain specific security functions that, together with the assumptions and the security objectives of the TOE operating environment, contribute to ensure the “sole control” of the signatory on the use of his/her own signature keys (SCDs);

   vii. in case of a multi-user, multi-key device (i.e., a device managing multiple SCDs owned by different signatories) the TOE must provide user-based identification, authentication and access control mechanisms, described in the ST in form of TOE objectives and SFRs, allowing it to:

      a. distinguish the signatories from other authorised users (for ex., administrative users);

      b. distinguish the various signatories;

      c. univocally and exclusively associate SCDs to their legitimate owners, and allow access to SCDs for signing operation solely to the legitimate owners.

C. For all device types, for the purposes of the Conformity Assessment all TOE cryptography-based security functions described in the ST must use algorithms, key lengths, hash functions, protocols, and parameters compliant to ETSI TS 119 312 V1.1.1 [R13] and subsequent editions.

D. Requirements for the recognition of the Certificate for the purposes of the Assessment Procedure:

   i. the Certificate is issued by the Italian Scheme (OCSI);

   ii. the Certificate is issued by a Scheme participating in the CCRA framework [R03] with the role of *Certificate Authorizing Scheme* (the current list is available in the "Certificate Authorizing Schemes" section of the *Common Criteria* portal [R04]);

   iii. the Certificate is issued by a Scheme participating in the SOGIS-MRA framework [R03] with the status of *Qualified/Authorising Participant* (the current list of participating Schemes with the relevant status is available in the "Status of Participants" section of the SOGIS portal [R12]).

E. With reference to the previous paragraph it should be noted that, given the special technological nature of signature devices and the specific regulatory framework (eIDAS Regulation), OCSI decided to recognise, exclusively for the purposes of the Conformity Assessment of such devices, *Common Criteria* certificates with no limitations on the assurance level, notwithstanding the rules for the mutual recognition imposed by the agreements referred to in points D.ii and D.iii.

8 Activation of the Conformity Assessment Procedure

A. The information materials to present at the time of application for the Conformity Assessment of a signature device are:

   i. Request for Conformity Assessment, prepared using the appropriate form available on OCSI's official website [R14], in the section dedicated to signature-creation devices, which must specify:

      a. the subject requesting the assessment and its role;

      b. the device for which the Conformity Assessment is requested, identified by the identifier used in the ST;

      c. the modality of the Assessment Procedure to be activated (modality 1 or 2), as referred to in chapters 9 and 10;

   ii. the ST of the device for which the Conformity Assessment is requested.

B. Within 30 days of receipt of the Conformity Assessment request, OCSI carries out a preliminary examination of the delivered information materials in order to verify their completeness and suitability for the Procedure. If no issues arise, OCSI sends the applicant a quote that specifies the minimum expected duration of the Procedure, the forecasted commitment of OCSI staff and the total cost, calculated according to the joint ministerial decree of 15 February [R08].

C. In case potential issues in the delivered information materials are detected, OCSI shall notify the applicant, specifying the reasons for the non-admissibility of the Conformity Assessment request, and the needed additions and amendments.

D. The procedure is activated by OCSI upon receipt of a copy of the quote signed for acceptance by the applicant accompanied, where applicable, by proof of payment of the deposit, made according to the instructions provided with the quote.

E. The stipulated maximum time limits for the application of the Procedure are indicated, for the two modalities, respectively in chapters 9 and 10.

9 Modality 1 of the Procedure

A. The following items need to be provided for the activation of the Procedure:

   i. the information materials referred to in chap. 8;

   ii. the Certificate referred to in chap. 6, point C.ii.

B. The Procedure consists of a single phase of the stipulated maximum duration of 180 days from activation, during which OCSI analyses the delivered information materials in order to verify the fulfillment of the security requirements laid down in Annex II of eIDAS Regulation. At the end of this phase the Attestation of Conformity is issued or the reasons for the refusal to issue are given.

C. During the analysis of the items referred to in par. A, OCSI may find them insufficient to express a judgment on the adequacy of the submitted certification, and therefore ask the applicant to integrate them with further evidence. Such a request suspends, up to its outcome, the time limits for the application of the Procedure specified in the quote.

10 Modality 2 of the Procedure

A. The information materials referred to in chap. 8 need to be provided for the activation of the Procedure.

B. The Procedure consists of a first phase of the stipulated maximum duration of 180 days from activation, during which OCSI analyses the delivered information materials in order to verify the fulfillment of the security requirements laid down in Annex II of eIDAS Regulation. At the end of this phase OCSI issues a Positive or Negative Pronouncement regarding the adequacy for the purposes of the Conformity Assessment of the information materials referred to in par. A.

C. During the analysis of the items referred to in par. A, OCSI may find them insufficient to issue the Pronouncement (Positive or Negative), and therefore ask the applicant to integrate them with further evidence. Such a request suspends, up to its outcome, the time limits for the application of the Procedure specified in the quote.

D. In case of a Negative Pronouncement, the Procedure ends. Note that a Negative Pronouncement is accompanied by the reasons for the refusal to issue the Attestation of Conformity.

E. In case of a Positive Pronouncement, the Procedure continues into a second phase starting upon delivery of the Certificate referred to in chap. 6, point C.ii. Note that a Positive Pronouncement is accompanied by its conditions of validity for conducting the second phase. In particular, all elements of the ST deemed relevant for the purposes of the Conformity Assessment are substantially “frozen” by a Positive Pronouncement.

F. The second phase of the Procedure has a stipulated maximum duration of 30 days, during which OCSI verifies the compliance of the certified version of the ST to the validity conditions referred to in par. E. At the end of this phase the Attestation of Conformity is issued or the reasons for the refusal to issue are given.

11 Characteristics of the Attestation of Conformity

A. The Attestation of Conformity specifies the following:

   i. the regulatory context of the Conformity Assessment (eIDAS Regulation [R01]);

   ii. the assessed device, identified by the identifier used in the ST;

   iii. the ST and the corresponding Certificate, identified by their assigned *Common Criteria* certification identifiers;

   iv. the modality of the Procedure applied in the Assessment Process (modality 1 or 2);

   v. the unique reference to the accompanying Assessment Report referred to in par. B;

   vi. the issuance date of the Attestation of Conformity.

B. The Attestation of Conformity is accompanied by an Assessment Report containing the assumptions under which the Attestation of Conformity has been issued and the conditions for its validity, along with additional information necessary to obtain a complete picture of the assessment carried out.

12 Conformity Assessment Registry

A. OCSI maintains a public registry, available on its official website [R14], in the section dedicated to signature devices, containing the list of the signature devices for which the Attestation of Conformity has been issued.