Joint Interpretation Library

Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices

JIL Interpretations for Security Certification according to eIDAS Regulation 910/2014

Version 1.0

July 2022

This page is intentionally left blank.

Table of contents

1 Introduction

1.1 General Information

1 Since 1 July 2016 the Regulation No 910/2014 of the European Parliament and of the Council of the European Union (eIDAS) [eIDAS_Reg] regulates amongst others legal and technical aspects for the creation of qualified electronic signatures and seals. It requires all European Member States to follow its legal and technical requirements.

2 Based on [eIDAS_Reg, Article 30 (1), (3a)], the corresponding Commission Implementing Decision (EU) 2016/650 [eIDAS_Impl] specifies more detailed the technical requirements and stipulates that the devices for the creation of qualified electronic signatures and seals (QSCD) have to be evaluated and certified according to the standardized Protection Profiles for Secure Signature Creation Device [PP_1, PP_2, PP_3, PP_4, PP_5, PP_6], whereby taking into consideration the Common Criteria standards [ISO_15408, ISO_18045]. The required Protection Profiles (standardized by DIN and EN and henceforth also called SSCD PP standards) consist of the following six parts:

- Protection profiles for secure signature creation device – Part 1: Overview, CEN/ISSS – Information Society Standardization System, EN 419211-1:2014, 2016-06-30 [PP_1]
- BSI-CC-PP-0059-2009-MA-02, Protection profiles for secure signature creation device – Part 2: Device with key generation, CEN/ISSS – Information Society Standardization System, EN 419211-2:2013, 2016-06-30 [PP_2]
- BSI-CC-PP-0075-2012-MA-01, Protection profiles for secure signature creation device – Part 3: Device with key import, CEN/ISSS – Information Society Standardization System, EN 419211-3:2013, 2016-06-30 [PP_3]
- BSI-CC-PP-0071-2012-MA-01, Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application, CEN/ISSS – Information Society Standardization System, EN 419211-4:2013, 2016-06-30 [PP_4]
- BSI-CC-PP-0072-2012-MA-01, Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application, CEN/ISSS – Information Society Standardization System, EN 419211-5:2013, 2016-06-30 [PP_5]
- BSI-CC-PP-0076-2013-MA-01, Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted channel to signature creation application, CEN/ISSS – Information Society Standardization System, EN 419211-6:2014, 2016-06-30 [PP_6]

3 Part 1 [PP_1] serves as an overview introducing the terminology and describing the TOE in its various forms, as well as its lifecycle. Parts 2 to 6 [PP_2, PP_3, PP_4, PP_5, PP_6] contain the actual SSCD protection profiles. Hereby, Parts 2 to 6 are grouped into two clusters. The first cluster addresses SSCDs with onboard key generation. The basic security requirements are described in Part 2 [PP_2]. Part 4 [PP_4] and Part 5 [PP_5] represent extensions to Part 2 [PP_2] with regard to secure communication with the certificate generation application and signature creation application. The second cluster

addresses SSCDs with the ability to import keys generated by the certification service provider. The basic security requirements are described in Part 3 [PP_3], and Part 6 [PP_6] provides the extension with respect to the secure communication with the signature creation application.

1.2 Background and Problem Description

4 The eIDAS Regulation [eIDAS_Reg] and the related Commission Implementing Decision [eIDAS_Impl] represent applicable law throughout the EU, and explicitly reference the SSCD PP standards discussed here, making them authoritative. However, those PPs have been written and standardized long before the eIDAS Regulation and Commission Implementing Decision were published. The SSCD PP standards therefore reflect (and in fact considerably reference) the earlier legal context in which they were written – concretely, the Electronic Signatures Directive 'Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures' [ES_Dir] along with the corresponding Commission Implementing Decision 'Commission Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council' [ES_Impl].

5 The SSCD PP standards have been declared by law (namely, the Commission Implementing Decision [eIDAS_Impl]) to be authoritative and sufficient as a specification of the technical and security requirements that qualified electronic signature creation devices (according to [eIDAS_Reg, Article 29]) and qualified electronic seal creation devices (according to [eIDAS_Reg, Article 39]) must comply with in order to ensure fulfilment of the legal requirements laid down in [eIDAS_Reg, Annex II]. Therefore, the SSCD PP standards are used and have to be applied without further restrictions or adaptations on an ongoing basis in product certification processes for signature devices by CC certification schemes throughout the EU.

6 Nevertheless, experience from such certifications since the time [eIDAS_Reg] and [eIDAS_Impl] came into force has shown that the fact that the SSCD PP standards are based on outdated legal documents is often seen as problematic and makes their comprehension and correct application in certifications difficult. Furthermore, beyond and unrelated to the evolution of the legal framework some additional issues have shown up during the application of the SSCD PP standards in the certification practice. More precisely, the following issues arise for which clarification and interpretation is requested:

- While the old legal framework [ES_Dir] and [ES_Impl] exclusively deals with electronic signatures, the new legal framework [eIDAS_Reg] and [eIDAS_Impl] has a considerably **broader scope,** amongst other especially by introducing the new notion of electronic seals. But the SSCD PP standards were based on the more limited scope of the old legal framework and have electronic signatures in focus. This situation gives rise to questions about if and how the newly introduced or extended notions and use cases are affected by the old SSCD PP standards, i.e. which requirements of the existing SSCD PP standards nevertheless can and have to be applied to them in certifications. This situation is analyzed in more detail in chapter 2.1 of this document.

- The SSCD PP standards **reference and cite** the **obsolete legal documents** [ES_Dir] and [ES_Impl], which makes it hard to understand the relationship between the detailed technical and security requirements given in the PPs and the corresponding legal requirements applicable today as those are specified in [eIDAS_Reg] and [eIDAS_Impl]. The implications of this situation are analyzed in chapter 2.2 of this document.
- Another relevant recent evolution in the domain of Common Criteria (CC) and specifically in SOG-IS is the introduction and subsequent further development and regular maintenance of the so-called **'SOG-IS Crypto Catalogue'**, i.e. the JIWG supporting document 'SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms' [SOGIS_C]. This catalogue was not available at the time as the PPs were set up and standardized, but on the other hand the application of this catalogue is indirectly required by the legal framework [eIDAS_Reg] and [eIDAS_Impl] via advice from the respective EU Commission's expert group. Implications from this catalogue on the application of the SSCD PP standards in the context of [eIDAS_Reg] and [eIDAS_Impl] are further analyzed in chapter 2.3 of this document.
- The evolvement and changes in the Common Criteria (CC) 'background' standard over the time as well as references to different CC origins (here: ISO, CCRA) and versions have to be taken into account. This concerns on the one hand the EU Regulation [eIDAS_Reg] and [eIDAS_Impl] where explicitly the use of an ISO CC standard differing from the CCRA CC version that the SSCD PP standards are partly based on is required. Furthermore, the ISO CC version prescribed by [eIDAS_Impl] and the CCRA / ISO CC version referenced in the SSCD PP standards meanwhile were as well superseded by a further newer CCRA CC version / revision. All in all, a mixture of different CC origins and versions is given and has to be handled. This sometimes provokes uncertainties regarding the question of conformance to the SSCD PP standards as well as to [eIDAS_Reg] and [eIDAS_Impl], and in particular in case the most recent **CC version** is used for a product's certification as this is usually required by the national certification schemes. This issue is addressed in more detail in chapter 2.4 of this document.
- Some **SSCD PP-internal inconsistencies** as well as **inconsistencies between the different SSCD PPs** concerning the conformance claim to more than one of these PPs at the same time (in particular, when taking PPs from the two different PP clusters, refer to chapter 1.1) have been discovered after the SSCD PPs' standardization and certification. Chapter 2.5 of this document provides guidance on how to cope with these issues.

1.3 Purpose, Objectives and Structure of the Document

7 This document explicitly addresses qualified electronic signature/seal creation devices (QSCD) on base of [eIDAS_Reg, Article 30 (1), (3a)] and the related requirements outlined in [eIDAS_Impl]. Other devices and their certification according to [eIDAS_Reg, Article 30 (3b)] are out of scope for this document.

8 The document at hand primarily strives to clarify the issues described in the previous chapter 1.2, assisting developers, evaluators and certifiers in the correct and meaningful application of the SSCD PP standards by providing suitable interpretations.

9 The following chapter 2 provides more detailed information on the issues identified and briefly described in chapter 1.2. In general, the respective subchapters present a problem and issue description followed by a section for agreed interpretation, if applicable. For clarity, the issue and agreed interpretation sections are colored in blue and indicated by a corresponding text mark (see entries '*Issue'*, '*Agreed Interpretation'*, '*Agreed Additional Interpretation*').

10 In the longer term, this document might also be used as a starting point for the preparation of a revised set of PP standards, further improving the match between the PPs and the legal framework of [eIDAS_Reg] and [eIDAS_Impl].

1.4 Notes

11 The current version of the document refers to the Regulation (EU) No 910/2014 and the Commission Implementing Decision (EU) 2016/650 of the European Parliament. At present, these regulations are under revision, and hence this document will be adapted accordingly as soon as the revised regulations are available.

12 Furthermore, for maintaining the document to remain up-to-date and applicable, the intended transition of SOG-IS to the EU CC Scheme and of the Common Criteria to a new ISO/IEC 15408 and ISO/IEC 18045 version might make a further corresponding adaptation of the document necessary.

2 Interpretations

2.1 Scope of eIDAS Regulation vs Scope of Electronic Signatures Directive

13 As indicated by its title, the old legal framework [ES_Dir] / [ES_Impl] had a comparatively restricted scope: its objective was to 'establish a legal framework for electronic signatures and certain certification services' [ES_Dir, Article 1]. Note that only certification services directly associated to the creation and use of electronic signatures were considered. The new legal framework [eIDAS_Reg] / [eIDAS_Impl] addresses a much broader scope, covering not only electronic signatures but also several additional or extended topics, concepts and objectives. Paraphrased from [eIDAS_Reg, Article 1], the topics, concepts and objectives of the new legislation are the following (numbering in parentheses added here):

(X.) establishment of a legal framework for electronic signatures

(A.) specification of rules for recognition of electronic identification means

(B.) specification of rules for trust services

(C.) establishment of a legal framework for

(C.1) electronic seals

(C.2) electronic time stamps

(C.3) electronic documents

(C.4) electronic registered delivery services

(C.5) certificate services for website authentication

14 Due to this much more extensive scope, [eIDAS_Reg] specifies a diverse set of new requirements on the legal level, many of which do not have counterparts in [ES_Dir], refer to (A.), (B.) and (C.) including (C.1) to (C.5). However, regarding electronic signatures, a clear compatibility relationship between the two legal frameworks was intended by the legislator, as can be seen both by comparing the requirements specified in the old and new legal documents and their annexes, and by the fact that the old SSCD PP standards were deemed sufficient for prescribing corresponding technical and security requirements through the Commission Implementing Decision [eIDAS_Impl].

15 In view of this situation the question arises which implications and issues for the applicability of the SSCD PP standards are to be derived. Note that the SSCD PP standards were set up in relationship to the old legal framework [ES_Dir] / [ES_Impl] and now are required to be used in different areas within the new legal framework [eIDAS_Reg] / [eIDAS_Impl].

2.1.1 Electronic Signatures

16 ***Issue:***

17 Both the old legal framework [ES_Dir] / [ES_Impl] and the new legal framework [eIDAS_Reg] / [eIDAS_Impl] cover electronic signatures, devices for creating them, and associated services. However, there are differences between the two frameworks, both regarding their scopes and on detail level. Are the SSCD PP standards that were

written in the context of the old legal framework fully applicable in security evaluations of electronic signature creation devices according to the new legal framework?

18 ***Agreed Interpretation:***

19 Regarding the technical requirements on which a security evaluation has to be based, [eIDAS_Reg, Article 30 (3)] stipulates that (leaving aside exceptional cases)

20 'The certification […] shall be based on […] (a) a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in the list established in accordance with the second subparagraph […]',

21 where the referenced subparagraph reads

22 'The Commission shall, by means of implementing acts, establish a list of standards for the security assessment of information technology products referred to in point (a) […].'

23 Concretely, Commission Implementing Decision [eIDAS_Impl] fulfils this requirement and references in its Annex both methodology standards (here: ISO/IEC 15408, ISO/IEC 18045) as well as technical and security standards to base the security evaluation upon, more detailed the SSCD PP standards [PP_1, PP_2, PP_3, PP_4, PP_5, PP_6]. This decision is motivated in [eIDAS_Impl, (4)] as follows:

24 'The European Committee for Standardisation (CEN) has developed […] standards for qualified electronic signature and seals creation devices, where the electronic signature creation data or electronic seal creation data is held in an entirely but not necessarily exclusively user-managed environment. These standards are considered suitable for the assessment of conformity of such devices with the relevant requirements set out in Annex II to Regulation (EU) No 910/2014.'

25 [eIDAS_Impl, Article 1] exhibits additional strictness compared to [eIDAS_Reg, Article 30 (3)] by stipulating that the entire list of standards documented in [eIDAS_Impl, Annex] applies to the certification of qualified electronic signature creation devices (or qualified electronic seal creation devices).

26 Therefore, the legislator's intent is interpreted in such a way that the SSCD PP standards' requirements fully apply to devices for electronic signature creation under [eIDAS_Reg]. Of course, as the scope of the SSCD PP standards matches the scope of the old legal framework only, their detailed requirements are restricted to that scope as well.

2.1.2 New eIDAS Concepts

27 Beside their applicability to electronic signature creation devices, the SSCD PP standards' requirements cannot and do not immediately apply to the new topics, concepts and objectives introduced within [eIDAS_Reg]. However, in specific cases they can indeed apply – namely, if and wherever the new legal framework [eIDAS_Reg] / [eIDAS_Impl] makes specific provisions that imply their applicability.

28 ***Issue:***

29 To what extent do the requirements in the SSCD PP standards apply to the topics, concepts and objectives newly introduced in [eIDAS_Reg]?

30 ***Agreed Interpretation:***

31 The SSCD PP standards' requirements do not apply to those topics, concepts and objectives within the Regulation [eIDAS_Reg] that had not been defined and covered equivalently in [ES_Dir], unless [eIDAS_Reg] makes specific provisions that imply their applicability. Concretely, the SSCD PP standards' requirements do not apply to the following topics newly defined in [eIDAS_Reg]:

(A.) electronic identification means

(C.2) electronic time stamps

(C.3) electronic documents

(C.4) electronic registered delivery services

(C.5) certificate services for website authentication

32 Consequently, no detailed interpretations for the previously listed topics are necessary.

33 Note: The associated trust services (B.) are discussed further down in chapter 2.1.5.

34 There is one newly defined topic for which [eIDAS_Reg] makes specific provisions that imply applicability of the SSCD PP standards and for which corresponding interpretation is needed: (C.1) electronic seals. For interpretation details refer to the following chapter 2.1.3.

2.1.3 Electronic Seals

35 Regarding the new concept of electronic seals (C.1 above), [eIDAS_Reg, Article 39] explicitly stipulates that all legal and, by implication, technical and security requirements that the regulation specifies for qualified electronic signature creation devices and their certification are to be applied analogously (‘mutatis mutandis’, i.e. ‘with the necessary modifications’) to qualified electronic seal creation devices and their certification as well.

2.1.3.1 Principal Interpretation for Electronic Seals and Associated ‘Necessary Modifications’

36 ***Issue:***

37 To what extent do the requirements in the SSCD PP standards apply to electronic seals?

38 ***Agreed Interpretation:***

39 By [eIDAS_Reg, Article 39 (2)], the legislator stipulated that the requirements of [eIDAS_Reg, Article 30] applying to the certification of devices for electronic signature creation shall apply analogously (‘mutatis mutandis’, i.e. ‘with the necessary modifications’) to devices for electronic seal creation.

40 As [PP_1, PP_2, PP_3, PP_4, PP_5, PP_6] fully apply to devices for electronic signature creation under [eIDAS_Reg] (see chapter 2.1.1), this is interpreted as the legislator’s intent to have [PP_1, PP_2, PP_3, PP_4, PP_5, PP_6] applied to the furthest possible extent to devices for electronic seal creation as well. Hereby, the legislator chose to refer to these existing standards rather than trigger the creation of revised standards in which the modifications would be made explicit. Therefore, the ‘mutatis mutandis’ stipulations are interpreted in such a way that the ‘necessary modifications’ are to be applied only

virtually by the reader, i.e. during reading the standards. This simple and efficient mode is possible because the concepts ‘electronic signature’ and ‘electronic seal’, although legally different, are practically equivalent w.r.t. the technical and security details.

41 The following mapping table details the ‘necessary modifications’ according to [eIDAS_Reg, Article 3 (32), Article 39 (1), (2), (3), Article 40] that are to be applied in the manner just described within the relevant parts of the SSCD PP texts in order to render these texts applicable in the context of electronic seals. A small number of additional refinements will be added to this principal interpretation in Table 1 below based on the analysis in the following subchapters.

42

Original Term in SSCD PPs	**Substituted Term for the Context of Electronic Seals**	**Remark**
(digital/electronic) signature	(electronic) seal	Exception: This substitution does not apply where the text addresses digital/electronic signatures occurring within qualified certificates.
signatory	seal creator (legal person)	
under sole control	with a high level of confidence under sole control	Refer to [eIDAS_Reg, Article 36 (c)] (and correcting an obvious error in the text ‘with a high level of confidence under its control’ of this clause). Refer as well to the considerations in section 2.1.3.6 which motivate the additional entry ‘with a high level of confidence’ because of a legal person that might be instantiated by several natural persons.
Original Abbreviation in SSCD PPs	**Original Meaning in SSCD PPs**	**Substitution (in the context of electronic seals)**
SSCD	secure signature creation device	secure seal creation device
SCD	signature creation data	seal creation data
SVD	signature validation data	seal validation data
SCA	signature creation application	seal creation application

43 Table 1: Basic ‘necessary modifications’

2.1.3.2 ST Modifications concerning Electronic Seals

44 ***Issue:***

45 Considering a TOE that supports electronic seal creation: In order to correctly model all aspects pertinent to electronic seal creation, is the ST author obliged to include specific text where the 'necessary modifications' (for all SSCD PP text sections and entries affected by the 'mutatis mutandis' stipulations of [eIDAS_Reg, Article 3 (32), Article 39 (1), (2), (3), Article 40]) are explicitly done, because the SSCD PPs formally deal with electronic signature creation only?

46 ***Agreed Interpretation:***

47 As the legislator stipulated that all requirements for qualified electronic signature creation devices are to be applied analogously to qualified electronic seal creation devices as well, the differences between electronic signatures and electronic seals are primarily legal, and the technical and security related differences do not affect the TOE itself but only its environment (see next interpretation), this additional effort would not be justified. It is sufficient if the descriptive parts of the ST (in particular, ST Introduction including TOE Overview and TOE Description, TOE Summary Specification) clearly state that the TOE is intended to be (also) used as a device for electronic seal creation and that all requirements stated in the ST applying to electronic signature creation are deemed to apply to electronic seal creation analogously, with the interpretations given in this document.

2.1.3.3 Electronic Signatures vs Electronic Seals: Role of External Entities

48 ***Issue:***

49 Apart from requirements to the TOE itself, the SSCD PPs also address within their security models objectives for, assumptions about and policies that affect entities external to the TOE which are associated with electronic signature creation. They e.g. make statements about certification services and about the CGA. Do these objectives, assumptions and policies apply in an analogous manner to external entities that are associated with electronic seal creation?

50 ***Agreed Interpretation:***

51 These objectives, assumptions and policies are the logical foundation based on which the technical and security requirements of the SSCD PPs are derived or justified. Therefore they have to continue to apply - with the 'necessary modifications' (refer to chapter 2.1.3.1). In specific cases, additional interpretations apply, too, which are presented in the following subchapters of this document.

2.1.3.4 Electronic Signatures vs Electronic Seals: Natural and Legal Persons

52 An electronic seal is, according to the Regulation [eIDAS_Reg], basically an electronic signature whose owner and creator is not a natural person (i.e. a human user, also called 'signatory' in the Regulation), but a legal person (i.e. an organization). [eIDAS_Reg, Article 3 (24)] defines the 'creator of a seal' as 'a legal person who creates an electronic seal' in a completely analogous way to [eIDAS_Reg, Article 3 (9)] which defines a 'signatory' as 'a natural person who creates an electronic signature'. This analogy is present in the same spirit throughout all parts of the Regulation dealing with electronic

seals, i.e. the ‘creator of a seal’ creating an electronic seal replaces the ‘signatory’ creating an electronic signature. It works fine on the legal level of the Regulation but poses some questions on the technical level of the SSCD PP texts when attempting to apply them analogously to qualified electronic seal creation, as prescribed by [eIDAS_Reg, Article 39].

53 The problem is that in practice a legal person cannot act by itself but only through humans acting on its behalf. Therefore, in order to create an electronic seal, some natural person within the organization embodying the legal person intending to create the seal, authorized to do this on the legal person’s behalf, will execute the seal creation process. This person will do this using an electronic seal creation device which according to [eIDAS_Reg, Article 39] needs to fulfil the requirements imposed by the existing SSCD PP standards analogously. However, crucially and in contrast to the situation with electronic signatures, the organization often will have the need to designate and authorize more than one individual for the task of seal creation.

54 The Regulation [eIDAS_Reg] with its Commission Implementing Decision [eIDAS_Impl] completely abstracts from the necessity to have individuals acting on behalf of a legal person. The SSCD PP standards do not contain a concept of electronic seals and of legal persons at all but instead only know abstract user roles such as ‘signatory’ and ‘administrator’. Unfortunately, neither [eIDAS_Reg] / [eIDAS_Impl] nor the SSCD PP standards provide more details or constraints on how to cope with this situation. In chapter 2.1.3.6 possible scenarios for the creation of electronic seals by a legal person with one or several natural persons acting on behalf of that legal person will be discussed.

2.1.3.5 Interpretations for Organisational Security Policies, Assumptions and Security Objectives for the TOE Operational Environment

55 The issues just described in the preceding subchapters do not affect the internal workings of the electronic signature/seal creation and corresponding devices from a technical point of view – on this level, there are no technical differences between electronic signature creation and electronic seal creation. But, they do affect the electronic signature/seal creation devices’ operating environment.

56 ***Issue:***

57 From the (semi-formal) parts of a PP, it is the Organisational Security Policies (OSP), the Assumptions and the Security Objectives for the TOE operational environment (OE) which impose requirements on the operating environment and on how the TOE is to be used within it. For electronic seal creation and related devices, are there any ‘necessary modifications’ on the OSPs, Assumptions and OEs as these are specified in the SSCD PP standards to be performed? How do they look like?

58 ***Agreed Interpretation:***

59 The following Table 2 addresses the Organisational Security Policies (OSP), the Assumptions and the Security Objectives for the TOE operational environment (OE) as these are specified by the SSCD PP standards and outlines the important specifics after execution of the ‘necessary modifications’. In addition, the table provides detailed interpretations for some of these items that are motivated by practical scenarios for the creation of electronic seals and which are described in chapter 2.1.3.6.

60 The first three columns in Table 2 list the original OSPs, Assumptions, and OEs in the SSCD PPs including their title, content and references to the SSCD PPs. The fourth column presents a modified version of the respective items' original text according to the [eIDAS_Reg] 'mutatis mutandis' analogous application stipulation. Hereby, some substitutions have additional text in brackets, at the interest of clarity.

61 The fifth column provides information on specific motivations for the modifications, in particular additional interpretations that were needed to clarify specific application scenarios which themselves are documented in chapter 2.1.3.6.

62

OSP / Assumption / OE Title	**Original Text in SSCD PPs**	**References to SSCD PPs** (context in which inter-pretations apply)	**Necessary Modifications for Electronic Seals** ([eIDAS_Reg, Article 3 (32), Article 39 (1), (2), (3), Article 40])	**Additional Interpretations**
P.CSP_QCert Qualified certificate	The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. the directive, Article 2, Clause 9, and Annex I) for the SVD generated by the SSCD. The certificates contain at least the name of the **signatory** and the SVD matching the SCD implemented in the TOE under **sole control** of the **signatory**. The CSP ensures that the use of the TOE as SSCD is evident with **signatures** through the certificate or other publicly available information.	PP-0059 [PP_2], PP-0075 [PP_3]: 6.3.1 PP-0071 [PP_4], PP-0072 [PP_5], PP-0076 [PP_6]: (6.3)	The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate for the SVD generated by the SSCD. The certificates contain at least the name of the **seal creator (legal person) [and, where applicable, registration number as stated in the official records]** and the SVD matching the SCD implemented in the TOE **with a high level of confidence under sole control** of the **seal creator (legal person)**. The CSP ensures that the use of the TOE as SSCD is evident with **[electronic] seals** through the	Note: Refer to [eIDAS_Reg, Annex III (c)].

			certificate or other publicly available information.	
P.QSign Qualified electronic signatures	The **signatory** uses a **signature** creation system to sign data with an advanced **electronic signature** (cf. the directive, Article 1, Clause 2), which is a qualified electronic **signature** if it is based on a valid qualified certificate **(according to the directive Annex I)12).** The DTBS are presented to the **signatory** and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic **signature** created with a SCD implemented in the SSCD that the **signatory** maintain under their **sole control** and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.	PP-0059 [PP_2], PP-0075 [PP_3]: 6.3.2 PP-0071 [PP_4], PP-0072 [PP_5], PP-0076 [PP_6]: (6.3)	The **seal creator (legal person)** uses a **seal** creation system to sign data with an advanced **electronic seal**, (cf. [eIDAS_Reg, Article 36]) which is a qualified electronic **seal** if it is based on a valid qualified certificate **[for electronic seals]** (according to **[eIDAS_Reg, Annex III]**). The DTBS are presented to the **seal creator (legal person)** and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic **seal** created with a SCD implemented in the SSCD that the **seal creator (legal person)** maintain **with a high level of confidence** under their **sole control** and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.	#1: The signatory is a legal person. In practice, the electronic seal creation process is executed by a natural person authorized to create electronic seals on the authority of a legal person.
P.Sigy_SSCD TOE as secure signature creation device	The TOE meets the requirements for an SSCD laid down in **Annex**	PP-0059 [PP_2], PP-0075 [PP_3]: 6.3.3	The TOE meets the requirements for an SSCD laid down in	

	III of the directive [1]. This implies the SCD is used for **digital signature creation** under **sole control of the signatory** and the SCD can practically occur only once.	PP-0071 [PP_4], PP-0072 [PP_5], PP-0076 [PP_6]: (6.3)	**[eIDAS_Reg, Annex II]**. This implies the SCD is used for **electronic seal creation with a high level of confidence** under **sole control of the seal creator (legal person)** and the SCD can practically occur only once.	
P.Sig_Non-Repud Non-repudiation of signatures	The lifecycle of the SSCD, the SCD and the SVD shall be implemented in a way that the **signatory** is not able to deny having **signed** data if the **signature** is successfully verified with the SVD contained in their unrevoked certificate.	PP-0059 [PP_2], PP-0075 [PP_3]: 6.3.4 PP-0071 [PP_4], PP-0072 [PP_5], PP-0076 [PP_6]: (6.3)	The lifecycle of the SSCD, the SCD and the SVD shall be implemented in a way that the **seal creator (legal person)** is not able to deny having **created a seal on** data if the **seal** is successfully verified with the SVD contained in their unrevoked certificate.	(#1) #2: Non-repudiation is interpreted to apply on the level of the legal person. If multiple natural persons are authorized to execute electronic seal creation on the authority of a legal person using a shared SSCD instance, individual accountability is not enforced by the SSCD.
A.SCA Trustworthy signature creation application	The **signatory** uses only a trustworthy SCA. The SCA generates and sends the DTBS/R of the data the **signatory** wishes to **sign** in a form appropriate for **signing** by the TOE.	PP-0059 [PP_2], PP-0075 [PP_3]: 6.4.2 PP-0071 [PP_4], PP-0072 [PP_5], PP-0076 [PP_6]: (6.4)	The **seal creator (legal person)** uses only a trustworthy SCA. The SCA generates and sends the DTBS/R of the data the **seal creator (legal person)** wishes to **create a seal on** in a form appropriate for **seal creation** by the TOE.	(#1)

A.CSP Secure SCD/SVD management by CSP	The CSP uses only a trustworthy SCD/SVD generation device and ensures that this device can be used by authorised user only. The CSP ensures that the SCD generated practically occurs only once, that generated SCD and SVD actually correspond to each other and that SCD cannot be derived from the SVD. The CSP ensures the confidentiality of the SCD during generation and export to the TOE, does not use the SCD for creation of any **signature** and irreversibly deletes the SCD in the operational environment after export to the TOE.	PP-0059 [PP_2]: - PP-0075 [PP_3]: 6.4.3 PP-0071 [PP_4], PP-0072 [PP_5]: - PP-0076 [PP_6]: (6.4)	The CSP uses only a trustworthy SCD/SVD generation device and ensures that this device can be used by authorised user only. The CSP ensures that the SCD generated practically occurs only once, that generated SCD and SVD actually correspond to each other and that SCD cannot be derived from the SVD. The CSP ensures the confidentiality of the SCD during generation and export to the TOE, does not use the SCD for creation of any **[electronic] seal** and irreversibly deletes the SCD in the operational environment after export to the TOE.	#3: 'Export to the TOE' is interpreted to allow for export to multiple SSCD instances if the SSCD is intended to be used for electronic seal creation.
OE.Signatory Security obligation of the signatory	The **signatory** shall check that the SCD stored in the SSCD received from SSCD-provisioning service is in non-operational state. The **signatory** shall keep their VAD confidential.	PP-0059 [PP_2]: 7.2.8 PP-0075 [PP_3]: 7.2.12 PP-0071 [PP_4], PP-0072 [PP_5], PP-0076 [PP_6]: (7.2.1)	The **seal creator (legal person)** shall check that the SCD stored in the SSCD received from SSCD-provisioning service is in non-operational state. The **seal creator (legal person)** shall keep their VAD confidential.	(#1) #4: Confidentiality of VAD is interpreted to apply on the level of the legal person, i.e. the group of persons authorized for electronic seal creation, and knowledge of the VAD shall be kept strictly within this group.

				Hint: The confidentiality requirement for the VAD with its interpretation in #4 should be addressed accordingly in the QSCD's guidance documentation.
OE.HID_-VAD Protection of the VAD	If an external device provides the human interface for user authentication, this device shall ensure confidentiality and integrity of the VAD as needed by the authentication method employed from import through its human interface until import through the TOE interface. In particular, if the TOE requires a trusted channel for import of the VAD, the HID shall support usage of this trusted channel.	PP-0059 [PP_2]: 7.2.5 PP-0075 [PP_3]: 7.2.9 PP-0071 [PP_4]: (7.2.1) PP-0072 [PP_5], PP-0076 [PP_6]: (split into OE.HID_-TC_VAD_-Exp and OT.TOE_-TC_VAD_-Imp)	(no modifications needed)	#5: A technical intermediation layer enabling several authorized natural persons to share a single SSCD used by a legal person for creating electronic seals is regarded as an external device providing an HID here, too (i.e., this OE applies to it).
OE.HID_TC_VAD_Exp Trusted channel of HID for VAD export	The HID provides the human interface for user authentication. The HID will ensure confidentiality and integrity of the VAD as needed by the authentication method employed including export to the TOE by means of a trusted channel.	PP-0072 [PP_5], PP-0076 [PP_6]: 7.2.2	(no modifications needed)	#6: A technical intermediation layer enabling several authorized natural persons to share a single SSCD used by a legal person for creating electronic seals is regarded as an HID here, too (i.e., this OE applies to it).

OE.SCD_-Unique Uniqueness of the signature creation data	The CSP shall ensure the cryptographic quality of the SCD/SVD pair, which is generated in the environment, for the qualified or advanced electronic **signature**. The SCD used for **signature** creation shall practically occur only once, i.e. the probability of equal SCDs shall be negligible, and the SCD shall not be reconstructable from the SVD.	PP-0075 [PP_3]: 7.2.4 PP-0076 [PP_6]: (7.2.1)	The CSP shall ensure the cryptographic quality of the SCD/SVD pair, which is generated in the environment, for the qualified or advanced electronic **seal**. The SCD used for **[electronic] seal** creation shall practically occur only once, i.e. the probability of equal SCDs shall be negligible, and the SCD shall not be reconstructable from the SVD.	#7: Uniqueness is interpreted to apply on the level of the single SSCD instance, i.e. to express a requirement regarding the level of cryptographic quality of a generated key pair such that the event of by-chance creation of exactly the same key pair in an unrelated SSCD instance has negligible probability. Multiple SSCD instances are allowed to share the same SCD/SVD pair if and only if all of these SSCDs are to be used for creating electronic seals for one and the same legal person.

63 Table 2: Electronic seals: ‘necessary modifications’ and additional interpretations for OSPs, Assumptions and OEs

2.1.3.6 Scenarios for Electronic Seal Creation by Authorized Natural Persons

64 In the following, possible practical scenarios for the execution of the electronic seal creation process by one or multiple authorized persons on behalf of a legal person are discussed. Important differences to the baseline scenario of the electronic signature creation in which a single natural person directly operates a single SSCD instance to which this individual has exclusive access are identified, and interpretations from Table 2 relevant to the respective scenario are highlighted.

65 When different persons are allowed to execute the electronic seal creation process on behalf of an organization (legal person), the question of individual accountability and its technical enforcement may become important. In the case of electronic signatures, even though the SSCD PP standards do not explicitly mention it, individual accountability is always automatically enforced by the non-repudiation requirement

(P.Sig_Non-Repud) together with the fact that the signatory is a natural person according to [eIDAS_Reg, Article 3 (9)] and has to keep the VAD of the SSCD confidential (OE.Signatory). In some of the following scenarios for electronic seal creation however, this automatic enforcement no longer works. The analysis will cover this aspect as well, so additional measures can be arranged for where individual accountability is essential.

66 Note that unless an ST explicitly constrains an SSCD used for electronic seal creation to a subset of the following scenarios, it has to be assumed that the SSCD will be used in all possible scenarios.

67 **a) 1 authorized person / 1 dedicated SSCD containing an SCD/SVD key pair / direct operation / exclusive access**

68 **Scenario:** Electronic seal creation where exactly one natural person is authorized to act on behalf of the legal person for creating electronic seals. This authorized person uses and directly operates exactly one SSCD dedicated to this task. No other natural person has access to this SSCD.

69 Note: Unfortunately, this scenario is of limited practical value: Organizations have a need to limit their dependency on the availability of individual persons and will therefore often want to authorize multiple natural persons for the task of creating electronic seals, resulting in the additional scenarios described below.

70 **Differences:** No significant differences to the baseline scenario. Individual accountability remains implicitly enforced.

71 ***Agreed Additional Interpretation:***

72 Refer to chapter 2.1.3.5, Table 2: P.QSign.#1.

73 **b) N authorized persons / 1 dedicated SSCD containing an SCD/SVD key pair / direct operation / non-exclusive access**

74 **Scenario:** Electronic seal creation where multiple authorized persons share a single SSCD instance, so each of them is individually able to create an electronic seal on behalf of the legal person, by directly interacting with the device. Thus, access to the device is non-exclusive, but restricted to the group of authorized persons.

75 **Differences:** Shared access to one and the same SSCD implies that the VAD needs to be known to all authorized persons. (Note: The hypothetical alternative of having multiple, user-specific VAD/RAD pairs for one and the same SCD/SVD key pair[1] is not supported by the SSCD PP standards and would conflict with the non-repudiation requirement). Individual accountability for electronic seal creation is no longer enforced by the SSCD – if needed, this has to be enforced by other suitable means (such as by an additional, personalized authentication mechanism in the SCA, or by organizational means such as a four-eyes-principle).

[1] The SSCD PPs do support having multiple SCD/SVD key pairs in one SSCD instance, each of them having one associated RAD/VAD pair. However, in the context of this discussion, making use of this capability is equivalent to considering N SSCD instances with one key pair each.

76 ***Agreed Additional Interpretation:***

77 Refer to chapter 2.1.3.5, Table 2: P.QSign.#1, P.Sig_Non-Repud.#2, OE.Signatory.#4.

78 **c) N authorized persons / 1 dedicated SSCD containing an SCD/SVD key pair / indirect operation / no access**

79 **Scenario:** Electronic seal creation where a single SSCD instance is employed for seal creation but this SSCD is not operated directly by any human user – in fact, the natural persons authorized for creating electronic seals do not even have physical access to the device. Instead, the SSCD is controlled by a technical intermediation layer such as an authorization service, triggering electronic seal creation on the SSCD only after successful authentication and authorization by one or several of the individuals authorized for electronic seal creation have been received and validated. E.g., an authorization scheme might require simultaneous authorization by two persons.

80 **Differences:** No significant differences to the baseline scenario, based on the approach that the technical intermediation layer both plays the role of the HID (in OE.HID_TC_VAD_Exp) and fills the 'Signatory' user role of the SSCD. Note also that the SSCD PPs do not formally constrain the 'Signatory' user role of the SSCD to be filled by a human user, and they mention that the 'Signatory' user may use the SSCD 'on behalf of the natural or legal person or entity they represent'. Individual accountability for seal creation is no longer enforced by the SSCD, but the technical intermediation layer can be required to solve this problem where necessary.

81 ***Agreed Additional Interpretation:***

82 Refer to chapter 2.1.3.5, Table 2: P.QSign.#1, P.Sig_Non-Repud.#2, OE.HID_VAD.#5 (in the context of [PP_2, PP_3, PP_4]), or OE.HID_TC_VAD_Exp.#6 (in the context of [PP_5, PP_6]).

83 **d) N authorized persons / N dedicated SSCDs all containing the same SCD/SVD key pair / direct operation / exclusive access**

84 **Scenario:** Electronic seal creation where one dedicated SSCD is used per each person authorized for electronic seal creation on behalf of the legal person. Each person directly operates and has exclusive access to exactly one dedicated SSCD. Using key import, all SSCDs used for creating the electronic seals receive, and then effectively share, the same SCD/SVD key pair. Note: This scenario only applies to SSCDs supporting key import, i.e. in the context of [PP_3] and [PP_6].

85 **Differences:** No significant differences to the baseline scenario on the level of each single SSCD instance. Individual accountability is no longer guaranteed by the SSCD; if needed, it would need to be enforced by organizational means or by technical measures within the SCA.

86 ***Agreed Additional Interpretation:***

87 Refer to chapter 2.1.3.5, Table 2: P.QSign.#1, A.CSP.#3, OE.SCD_Unique.#7.

88 **e) N authorized persons / N dedicated SSCDs each containing a unique SCD/SVD key pair / direct operation / exclusive access**

89 **Scenario:** Electronic seal creation where a dedicated SSCD is used by each of the persons authorized to create electronic seals on behalf of the legal person. Each person directly operates and has exclusive access to exactly one dedicated SSCD. Each SSCD instance contains a unique SCD/SVD key pair, i.e. no two pairs are equal.

90 Note: This scenario may cause practical problems due to the fact that multiple variants of an electronic seal would exist for the same legal person, and would need to be recognized externally to belong to the same legal person. Also, the individual having executed the electronic seal creation process might be unintentionally identifiable outside the organization owning the electronic seal, which might conflict with data protection regulations. Note that pseudonyms cannot be used to alleviate the latter problem because unlike for electronic signatures, [eIDAS_Reg] does not allow for pseudonyms to be used in connection with electronic seals.

91 **Differences:** No significant differences to the baseline scenario. Individual accountability remains implicitly enforced by each SSCD.

92 ***Agreed Additional Interpretation:***

93 Refer to chapter 2.1.3.5, Table 2: P.QSign.#1.

2.1.4 Advanced Electronic Signatures and Seals

94 Even though the new legal framework [eIDAS_Reg] / [eIDAS_Impl] generally extends the old legal framework [ES_Dir] / [ES_Impl] by covering new topics, concepts and objectives there is one perspective in which the new framework can be seen as weaker (less restrictive) than the old one: Where the old framework specifies legal, technical and security requirements for ‘secure signature-creation devices’ used for creation of ‘advanced electronic signatures’ [ES_Dir (15)], the new one more narrowly specifies the requirements to only apply to ‘qualified electronic signature creation devices’ [eIDAS_Reg, Article 29, 30, 31] and ‘qualified electronic seal creation devices’ [eIDAS_Reg, Article 39]. Interpreting this literally, devices used exclusively for the creation of advanced but not qualified electronic signatures are legally not required by [eIDAS_Reg] to fulfil the requirements of [eIDAS_Reg, Annex II]. Also, [eIDAS_Impl, Article 1] only stipulates requirements to ‘the certification of qualified electronic signature creation devices or qualified electronic seal creation devices’ - concretely, that the SSCD PP standards are to be applied therein. Therefore, no applicability to the more general categories of devices for advanced signature creation or devices for advanced seal creation is stipulated. As, however, certifications based on the SSCD PP standards discussed here are normally being done for products that intend to support the creation of qualified electronic signatures/seals, this conclusion is expected to have very limited practical relevance.

95 ***Issue:***

96 In the new legal framework of [eIDAS_Reg] / [eIDAS_Impl], requirements applying to signature/seal creation devices and associated trust services are only specified for qualified electronic signatures/seals. The case of advanced electronic signatures/seals

that are not qualified is not covered. To what extent does this influence the applicability of the SSCD PP standards?

97 ***Agreed Interpretation:***

98 For the evaluation of qualified electronic signature/seal creation devices, the reduced domain to which the requirements specified by [eIDAS_Reg] / [eIDAS_Impl] formally apply is immaterial. As qualified electronic signature/seal creation devices are the class of products targeted in practical certifications, only this class will be considered further in this document - and in this context, the full applicability of the SSCD PP standards is evident.

2.1.5 eIDAS Trust Services

99 Apart from secure signature creation devices, for which detailed technical and security requirements are specified in the form of SFRs and SARs, the SSCD PP standards also lay down basic requirements on the behavior of 'certification services' associated with the creation and use of electronic signatures. As these services are not part of the TOE but part of its operating environment, their behavior is only coarsely specified in the form of Organisational Security Policies and Security Objectives for the TOE. In the new legal framework [eIDAS_Reg], those certification services are subsumed under the new and broader concept of 'trust services', the scope of which far extends the area of electronic signatures and also covers services associated to other new topics and concepts introduced in [eIDAS_Reg].

100 In order to analyze to what extent the SSCD PP requirements on certification services are still applicable under [eIDAS_Reg], it is necessary to determine their equivalent in the terminology of the new legal framework [eIDAS_Reg] / [eIDAS_Impl]. For this purpose, the trust services (B.) are categorized into subcategories (B.1) to (B.5) which are discussed in detail in the following.

101 **(B.1) Trust services associated with electronic signatures and equivalent to 'certification services' according to [ES_Dir]**

102 For these trust services, the requirements in the SSCD PP standards are evidently applicable. Although [eIDAS_Reg] / [eIDAS_Impl] formally address only 'qualified electronic signature creation devices or qualified electronic seal creation devices' and prescribe to use the SSCD PP standards in their certification, it can be safely assumed that carrying over the SSCD PP requirements to associated services was intended by the legislator as well. Without those requirements being satisfied, the conditions for the certificate being valid and applicable would not be fulfilled, so the certification would be pointless.

103 ***Issue:***

104 To what extent do the requirements in the SSCD PP standards apply to trust services associated with electronic signatures that are equivalent to 'certification services' as defined in [ES_Dir]?

105 ***Agreed Interpretation:***

106 For trust services associated to the creation and use of electronic signatures that are equivalent to 'certification services' as defined in [ES_Dir], the requirements documented in the SSCD PP standards immediately apply.

107 **(B.2) Trust services associated with electronic signatures and not equivalent to 'certification services' according to [ES_Dir]**

108 As the new legal framework [eIDAS_Reg] / [eIDAS_Impl] is intended by the legislator to extend the old legal framework [ES_Reg] / [ES_Impl] for electronic signatures, such trust services associated to electronic signatures that conflict with 'certification services' according to [ES_Dir] are not to be expected and were not found during an analysis of the documents.

109 ***Issue:***

110 None.

111 ***Agreed Interpretation:***

112 Therefore, here no detailed interpretations are necessary.

113 **(B.3) Trust services associated with electronic seals and analogous to 'certification services' according to [ES_Dir]**

114 For these trust services, the requirements in the SSCD PP standards are applicable since the legislator documented the intent to treat electronic seals in a completely analogous manner to electronic signatures.

115 ***Issue:***

116 To what extent do the requirements in the SSCD PP standards apply to trust services associated with electronic seals that are analogous to 'certification services' as defined in [ES_Dir]?

117 ***Agreed Interpretation:***

118 For trust services associated to the creation and use of electronic seals that are analogous to 'certification services' as defined in [ES_Dir], the requirements documented in the SSCD PP standards apply consequentially due to [eIDAS_Reg, Article 39].

119 **(B.4) Trust services associated with electronic seals and not analogous to 'certification services' according to [ES_Dir]**

120 As the new legal framework [eIDAS_Reg] / [eIDAS_Impl] is intended by the legislator to extend the old legal framework [ES_Reg] / [ES_Impl] for electronic signatures and furthermore in a similar manner then to electronic seals as for electronic signatures, such trust services associated to electronic seals that conflict with 'certification services' according to [ES_Dir] are not to be expected and were not found during an analysis of the documents.

121 ***Issue:***

122 None.

123 ***Agreed Interpretation:***

124 Therefore, here no detailed interpretations are necessary.

125 **(B.5) Trust services associated with other topics and concepts newly covered in [eIDAS_Reg]**

126 This concerns the topics electronic identification means, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication. As there are no equivalents to these concepts within [ES_Dir] and the SSCD PP standards, their requirements are not relevant here.

127 ***Issue:***

128 None.

129 ***Agreed Interpretation:***

130 Therefore, no detailed interpretations for the trust services associated to identification means, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication as defined in [eIDAS_Reg] are provided here.

2.1.6 Summary of Scope-related Interpretations

131 The following Table 3 provides an overview of all the scope-related interpretations collected above.

132

Tag	Topic / Concept from [eIDAS_Reg]	Relevance for SSCD PPs
(X.)	electronic signatures (associated trust services are covered in (B.))	Yes
(A.)	electronic identification means	No
(B.)	trust services:	
(B.1)	trust services associated with electronic signatures and equivalent to ‘certification services’ according to [ES_Dir]	Yes
(B.2)	trust services associated with electronic signatures and **not** equivalent to ‘certification services’ according to [ES_Dir]	No
(B.3)	trust services associated with electronic seals and analogous to ‘certification services’ according to [ES_Dir]	Yes
(B.4)	trust services associated with electronic seals and **not** analogous to ‘certification services’ according to [ES_Dir]	No
(B.5)	trust services applying to other topics and concepts newly covered in [eIDAS_Reg]	No
(C.)	New concepts in [eIDAS_Reg]:	
(C.1)	electronic seals	Yes

	(associated trust services are covered in (B.))	
(C.2)	electronic time stamps	No
(C.3)	electronic documents	No
(C.4)	electronic registered delivery services	No
(C.5)	certificate services for website authentication	No

133 Table 3: Overview of scope-related interpretations

2.2 Obsolete References

134 As described in the introduction, the SSCD PP standards reference and cite (only) the outdated legal documents [ES_Dir] and [ES_Impl] of the old legal framework. This makes it hard to understand the relationship between the detailed technical and security requirements given in the PPs and the corresponding legal requirements applicable today, i.e. the ones of [eIDAS_Reg] and [eIDAS_Impl] in the new legal framework. However, there are two reasons why these outdated references do not pose any factual problems during QSCD evaluations:

- As already stated, a clear compatibility-based relationship between the two legal frameworks given by [ES_Dir] / [ES_Impl] and [eIDAS_Reg] / [eIDAS_Impl] was intended by the legislator, as can be seen both by comparing the requirements specified in the old and new legal documents and their annexes, and by the fact that the old SSCD PP standards were deemed sufficient for prescribing corresponding technical and security requirements through [eIDAS_Impl]. A detailed analysis shows that for each obsolete reference to [ES_Dir] / [ES_Impl] in the SSCD PP standards a sufficiently equivalent text in the new legislation [eIDAS_Reg] / [eIDAS_Impl] exists. Please note that in some cases relevant content is now distributed over different locations within the legal documents, so more than one actual reference might be needed for a replacement. Of course, this argument only applies to the topic of electronic signatures.
- Many references to [ES_Dir] / [ES_Impl] in the SSCD PP standards have only informative character rather than play a normative role within the PPs.

135 ***Issue:***

136 None.

137 ***Agreed Interpretation:***

138 The obsolete references in the SSCD PP standards do not necessitate any more detailed interpretations within this document.

2.3 Suitable Cryptographic Algorithms for QSCD

139 To ensure that the electronic signatures/seals generated by a qualified electronic signature/seal creation device are reliably protected against forgery, suitable cryptographic algorithms, key lengths and hash functions build the prerequisite for the security of the certified product and its usage.

140 At the time of preparation of the Commission Implementing Decision [eIDAS_Impl] this issue was not harmonized at European level, and the EU Member States were supposed to cooperate for agreement on cryptographic algorithms, key lengths and hash functions to be used in qualified electronic signature/seal creation devices (refer to [eIDAS_Impl, (8)]).

141 Furthermore, the SSCD PP standards require the ST author to consult with specified entities as responsible for accreditation and supervision of the evaluation process to select the admissible cryptographic algorithms, related relevant parameters and applicable standards. The following occurrences are among others of relevance:

- SSCD PP Part 2 [PP_2], Application Note 4: 'Member states of the European Union have specified entities as responsible for accreditation and supervision of the evaluation process for products conforming to this standard and for determining admissible algorithms and algorithm parameters (the directive: 1.1b and 3.4). The ST writer shall consult with these entities to learn of admissible algorithms and cryptographic key sizes and other parameters or applicable standards.'
- SSCD PP Part 3 [PP_3], Application Note 5: 'The ST writer shall perform the missing operations in the element FCS_COP.1.1. The ST writer should consult the notified body or the certification body for the admissible algorithms, cryptographic key sizes and other parameters for algorithms, and standards for digital signature creation by SSCD. The operations in the element FCS_COP.1.1 shall be appropriate for the SCD imported according to FTP_ICT.1/SCD.'

142 ***Issue:***

143 Did the EU Member States agree on cryptographic mechanisms, key lengths and corresponding standards? Which role does the agreement play in the context of the certification of qualified electronic signature/seal creation devices?

144 ***Agreed Interpretation:***

145 For the generation of qualified electronic signatures/seals the qualified electronic signature/seal creation device (QSCD) has to use cryptographic algorithms and related relevant parameters (e.g. key size) in accordance with the so-called 'SOG-IS Crypto Catalogue', i.e. the JIWG supporting document 'SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms' [SOGIS_C]. The application of this catalogue is based on the advice of the respective EU Commission's expert group. If the product is intended for use in accordance with the eIDAS Regulation [eIDAS_Reg] and Commission Implementing Decision [eIDAS_Impl] only agreed cryptographic mechanisms according to [SOGIS_C] shall be used. The usage of cryptographic mechanisms (including related relevant parameters) that are classified neither as 'recommended' nor as 'legacy' in [SOGIS_C] is not allowed.

146 The cryptographic mechanisms (including relevant parameters) chosen for the QSCD are part of the product's security certification according to the CC and SSCD PP standards.

147 Additionally to be considered for use of the cryptographic mechanisms (including relevant parameters) are their corresponding validity deadlines as those are outlined in [SOGIS_C] and in the certification or qualification report for the QSCD product. Future updates of the 'SOG-IS Crypto Catalogue' [SOGIS_C] that occur after certification of

the QSCD may shorten or extend the validity time frame of cryptographic mechanisms or parameters. This may need actions for the usage of the product to be taken.

2.4 Application of CC Version for Certification of QSCD

148 In the Commission Implementing Decision [eIDAS_Impl] the technical requirements which a qualified electronic signature/seal creation device (QSCD) has to fulfil to be compliant to the Regulation [eIDAS_Reg] are stated. According to [eIDAS_Impl, Annex] the QSCD has to be evaluated and certified according to Common Criteria (CC) using the ISO standards ISO/IEC 15408 and ISO/IEC 18045 in their 2008/2009 versions [ISO_15408, ISO_18045] (including their related technical corrigenda).

149 The SSCD PP standards required for the certification of qualified electronic signature/seal creation devices by [eIDAS_Impl, Annex] on the other hand refer partially to CCRA CC Version 3.1 Revision 4 [CC31_R4, CEM31_R4] and/or Revision 3 [CC31_R3, CEM31_R3] as well as in parts to the ISO CC standards [ISO_15408, ISO_18045].

150 Hereby, it should be noted that the referenced versions of the ISO CC standards [ISO_15408, ISO_18045] (together with their related technical corrigenda) are on content level fully compatible with the CCRA CC Version 3.1 Revision 4 [CC31_R4, CEM31_R4].

151 ***Issue:***

152 Is a certification of a qualified electronic signature/seal creation device (QSCD) according to CCRA CC Version 3.1 Revision 5 [CC31_R5, CEM31_R5] acceptable w.r.t. the Commission Implementing Decision [eIDAS_Impl]?

153 ***Agreed Interpretation:***

154 A certification of a QSCD according to CCRA CC Version 3.1 Revision 5 w.r.t. the Commission Implementing Decision [eIDAS_Impl] is acceptable because of the reasoning outlined in the following:

155 The main differences between CCRA CC Version 3.1 Revision 3 and [ISO_15408, ISO_18045] / CCRA CC Version 3.1 Revision 4 address the following aspects:

- CC Part 1: In [CC31_R4, Part 1] changes for conformance claims of type ‘strict conformance’ and ‘demonstrable conformance’ were formally incorporated on base of a corresponding agreed Change Proposal that previously already was applied for PPs and STs.
- CC Part 2: In [CC31_R4, Part 2] no changes occurred.
- CC Part 3: In [CC31_R4, Part 3] no changes were done.
- CEM: In [CEM31_R4] the changes for ‘strict conformance’ and ‘demonstrable conformance’ performed in CC Part 1 were taken over to CEM accordingly.

156 The main differences between [ISO_15408, ISO_18045] / CCRA CC Version 3.1 Revision 4 and CCRA CC Version 3.1 Revision 5 can be summarized as follows:

- CC Part 1: In [CC31_R5, Part 1] a new modularization concept for Protection Profiles (consisting of base PPs, PP modules and PP

configurations) that was originally set up and experienced as an Addendum to the CCRA CC was incorporated.

- CC Part 2: In [CC31_R5, Part 2] no changes occurred.
- CC Part 3: In [CC31_R5, Part 3] the new class 'ACE: Protection Profile Configuration evaluation' was introduced to address the new modularization concept for Protection Profiles. Furthermore, some slight issues in the context of ASE_INT, ASE_CCL and ADV_TDS were clarified and corrected.
- CEM: In [CEM31_R5] the new class ACE in Part 3 was filled with corresponding work units, and the further slight changes in Part 3 were taken over to CEM accordingly.

157 The security level of [CC31_R3, CEM31_R3], [ISO_15408, ISO_18045] / [CC31_R4, CEM31_R4] and [CC31_R5, CEM31_R5] can be therefore regarded as equivalent, and the changes made for [CC31_R5, CEM31_R5] (starting from [CC31_R3, CEM31_R3] via [CC31_R4, CEM31_R4]) do not raise any conflict, neither in view of the requirements on a security certification of a QSCD according to Common Criteria nor in view of the application of the SSCD PP standards as base for such certifications.

2.5 PP Inconsistencies

158 Some inconsistencies within single SSCD PPs and as well between the different PPs have been discovered after their standardization and certification. The following two major issues were identified:

- Insufficient coverage of the objective OT_Lifecycle_Security by SFRs
- Inconsistencies and problems when combining the SSCD PP Part 2 [PP_2] and SSCD PP Part 3 [PP_3] within a 'strict conformance' claim of a ST in a single product certification

2.5.1 Insufficient Coverage of OT.Lifecycle_Security

159 PP Part 2 [PP_2] and PP Part 3 [PP_3] prescribe the following objective for the TOE:

160 OT.Lifecycle_Security:

'The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall securely destroy the SCD on demand of the signatory.'

161 The objective OT.Lifecycle_Security is accompanied by the following Application Note in PP Part 2 [PP_2] and PP Part 3 [PP_3]:

'The TOE shall keep the confidentiality of the SCD at all times, in particular during SCD/SVD generation, signature creation operation, storage and secure destruction.'

162 There are several SFRs in the two PPs that are traced back to and cover this objective OT.Lifecycle_Security. FCS_CKM.4.1 for instance requires that the cryptographic keys shall be destroyed in accordance with a specified cryptographic key destruction method. However, there are no SFRs in the PP Part 2 [PP_2] and PP Part 3 [PP_3] mapped which explicitly state that the destruction of the SCD shall be done on demand of the signatory. In particular, no policies controlling the access to the SCD destruction function are

given. Hence, the objective OT.Lifecycle_Security does not seem to be fully covered by the SFR tracings. The next sections address solutions for providing sufficient coverage of the objective on ST level and concerning further CC aspects.

163 ***Issue:***

164 How should this issue of insufficient coverage of the objective OT.Lifecycle_Security by SFRs be addressed during the QSCD certification according to the SSCD PP Part 2 [PP_2] or Part 3 [PP_3] respectively?

165 ***Agreed Interpretation:***

166 The mechanism for the destruction of the SCD on demand of the signatory belongs to the TOE's security functionality and shall therefore be considered by the developer and evaluation body throughout the whole certification procedure for the QSCD.

167 The following sections describe four proposals on how this issue can be solved whereby the rules for strict conformance as required by the SSCD PPs are respected.

168 Hereby, the requirement 'key destruction *on demand of the signatory*' is interpreted according to the Application Note 1 related to OT.Lifecycle_Security in [PP_2] and [PP_3] in that way that the signatory himself is explicitly able to initiate and perform the key destruction. The way of key destruction by an administrator on request of the signatory is not deemed to be sufficient in the sense of the PPs. A corresponding information on this interpretation should be provided by the QSCD's guidance documentation.

169 Furthermore, it should be taken into account that control over the SCD destruction e.g. via authentication mechanisms may cause problems if using the user verification mechanism via RAD/VAD for this objective as such data in common view are explicitly and exclusively assigned to the signature functionality of the QSCD.

170 **1) Solution via key generation / key import by the signatory**

171 In case that the TOE offers the possibility for the signatory to generate a new SCD with overwriting the old SCD or to import a new SCD with replacing the old SCD (i.e. the subject S.User with the security attribute 'Role' set to 'R.Sigy' is as well assigned the security attribute 'SCD/SVD Management' set to 'authorised') the requirement 'The TOE shall securely destroy the SCD on demand of the signatory.' in OT.Lifecycle_Security is sufficiently fulfilled in view of the Application Note 1 related to OT.Lifecycle_Security:

'[…] There is no need to destroy the SCD in case of repeated SCD generation. The signatory shall be able to destroy the SCD stored in the SSCD, e.g. after the (qualified) certificate for the corresponding SVD has been expired.' ([PP_2], chapter 7.1.2)

respectively

'[…] There is no need to destroy the SCD in case of repeated SCD import. The signatory shall be able to destroy the SCD stored in the SSCD, e.g. after the (qualified) certificate for the corresponding SVD has been expired.' ([PP_3], chapter 7.1.2)

172 **2) Solution via change of security attributes by the signatory**

173 In case the TOE is implemented in such a way that the SFR FMT_MSA.1/Signatory that is mapped to OT.Lifecycle_Security offers the signatory the possibility to change

the security attribute ‘SCD operational’ from the value ‘yes’ to ‘no’ (even if this case is not explicitly discussed in the PPs) this could be interpreted in view of the SFR FDP_RIP.1 and the objective OT.SCD_Secrecy as the de-allocation of the storage used for the SCD including destruction of the SCD.

174 According to the Application Note accompanying the objective OT.Lifecycle_Security in the PPs, ‘the TOE shall keep the confidentiality of the SCD at all times, in particular during SCD/SVD […] secure destruction’. Furthermore, FDP_RIP is mapped to OT.SCD_Secrecy. Setting the SCD to non-operational state means that the SCD is no longer usable, and this together with the overall secrecy of the SCD is interpreted as (logical) de-allocation. Please take into account that FDP_RIP.1 does not necessarily require physical destruction.

175 Via these considerations the requirement ‘The TOE shall securely destroy the SCD on demand of the signatory.’ in OT.Lifecycle_Security is deemed as sufficiently fulfilled.

176 **3) Solution via Application Note**

177 The ST author adds an Application Note to FCS_CKM.4.1 which states that the destruction of the SCD is done at least on demand of the signatory.

178 In the Application Note, the ST author may use the subjects and security attributes from the SSCD PP Part 2 or Part 3 respectively, Table 2 to describe the access control policy w.r.t the SCD destruction in a more precise way, e.g. ‘S.User with the security attribute ‘Role’ set to ‘R.Sigy’ is allowed to destroy the SCD.’

179 The mechanism for the SCD destruction is considered in the ST section ‘TOE Summary Specification’ (TSS) within the description of the TSF and the related rationale for the mapping to the SFRs.

180 All ST additions arising in this context are evaluated by the evaluation body according to the ASE Common Criteria methodology.

181 The additional functionality ‘SCD destruction on demand of the signatory’ added by the Application Note has to be evaluated by the evaluation body in the framework of the QSCD's product evaluation during all relevant Common Criteria evaluation activities (e.g. concerning the aspects guidance, TOE design, testing, vulnerability analysis etc.).

182 **4) Solution via additional and modified SFRs**

183 The ST author adapts already in the PPs existing SFRs and adds additional SFRs in order to adequately supplement the missing modelling of the TOE’s security functionality for the destruction of the SCD on demand of the signatory.

184 The following two SFRs are added to the ST beyond the SFRs that are already contained in the SSCD PP Part 2 or Part 3 respectively:

- FDP_ACC.1/SCD_Destruction
- FDP_ACF.1/SCD_Destruction

185 FDP_ACC.1/SCD_Destruction Subset access control

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ SCD_Destruction	The TSF shall enforce the SCD Destruction SFP[2] on 1) subjects: S.User; 2) objects: SCD; 3) operations: SCD destruction[3].

186 FDP_ACF.1/SCD_Destruction Security attribute based access control

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/ SCD_Destruction	The TSF shall enforce the SCD Destruction SFP[4] to objects based on the following: 1) subjects: S.User associated with the security attribute 'Role'; 2) objects: SCD associated with the security attribute 'SCD identifier'[5].
FDP_ACF.1.2/ SCD_Destruction	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: S.User with the security attribute 'Role' set to [selection: R.Admin, R.Sigy] is allowed to destroy the SCD[6].
FDP_ACF.1.3/ SCD_Destruction	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[7].
FDP_ACF.1.4/ SCD_Destruction	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[8].

Accompanied is this new SFR by the

'Application Note: The ST writer shall perform the operation in the element FDP_ACF.1.2/SCD_Destruction according to the access control rules provided by the TOE for SCD destruction. In FDP_ACF.1.2/ SCD_Destruction at least the selection of R.Sigy has to be performed.'

[2] [assignment: *access control SFP*]
[3] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[4] [assignment: *access control SFP*]
[5] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
[6] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[7] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[8] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to object*]

187 The following SFR of the SSCD PP Part 2 or Part 3 respectively is extended in the ST in order to cover the additional SCD destruction operation:

- FMT_MSA.3.1: The 'SCD Destruction SFP' is added to FMT_MSA.3.1.

188 The following tracings from Table 4 in the SSCD PP Part 2 or Part 3 respectively are supplemented in the ST:

- FDP_ACC.1/SCD_Destruction is mapped to OT.Lifecycle_Security.
- FDP_ACF.1/SCD_Destruction is mapped to OT.Lifecycle_Security.

189 The rationale for the TOE security requirements sufficiency in the SSCD PP Part 2 or Part 3 respectively, section 9.3.2 is extended at least with the following statement: 'The SCD destruction is controlled by the TSF according to FDP_ACC.1/SCD_Destruction and FDP_ACF.1/SCD_Destruction.'

190 The mechanism for the SCD destruction is considered in the ST section 'TOE Summary Specification' (TSS) within the description of the TSF and the related rationale for the mapping to the SFRs.

191 Since the proposed supplements and adaptations of SFRs are not part of the SSCD PPs and their certification these SFRs including their related ST aspects in the SPD, Objectives for the TOE and its environment, SFRs, TSS etc. have to be evaluated by the evaluation body in the framework of the QSCD's product evaluation during all relevant Common Criteria evaluation activities. This affects not only the ST, but as well concerns the aspects guidance, TOE design, testing, vulnerability analysis etc.

2.5.2 Inter-PP Inconsistencies

192 SSCD PP Part 2 [PP_2] covers the security functionality of an SSCD with onboard key generation whereas SSCD PP Part 3 [PP_3] addresses the security functionality of an SSCD with key import. Hence, there are several parts of these two PPs that differ in their scope and on content level, in particular this concerns the Security Problem Definition (SPD), the Security Objectives for the TOE and its operational environment, the Security Functional Requirements (SFR), including related rationales.

193 Some differences between the PPs thus result from the different functional scope of the corresponding TOE. In [PP_2] for instance, the objective 'OT.SCD/SVD_Auth_Gen: Authorised SCD/SVD generation' has to be enforced by the TOE. In contrast, in [PP_3] the same objective, here now called 'OE.SCD/SVD_Auth_Gen: Authorised SCD/SVD generation' has to be enforced by the environment because the key generation is done by the certification service provider and not by the TOE.

194 However, the PPs [PP_2] and [PP_3] also exhibit differences that are not clearly related to the differing scopes (onboard key generation vs key import). Some elements of the Security Problem Definition have the same ID on both sides but subtly different content, such as:

- [PP_2]: OE.SVD_Auth: 'The operational environment shall ensure the **integrity** of the SVD sent to the CGA of the CSP. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.'

- [PP_3]: OE.SVD_Auth: 'The operational environment shall ensure the **authenticity** of the SVD sent to the CGA of the CSP. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.'

195 All such differences in the Security Problem Definition, the Security Objectives for the TOE and its operational environment and the Security Functional Requirements have an impact on further parts of the PPs [PP_2] and [PP_3] as e.g. tracings/mappings and related rationales. If the TOE is intended to support the onboard key generation as well as the key import, both PPs [PP_2] and [PP_3] have to be applied and claimed. However, due to the identified differences the combination may cause (formal) problems w.r.t. the 'strict conformance' required by both PPs.

196 As the SSCD PP Part 2 [PP_2] is (as text copy) incorporated into the SSCD PP Part 4 [PP_4] and SSCD PP Part 5 [PP_5] as well as the SSCD PP Part 3 [PP_3] is (as text copy) incorporated into the SSCD PP Part 6 [PP_6], the inconsistency problems between [PP_2] and [PP_3] transfer to [PP_4], [PP_5] and [PP_6] accordingly.

197 Note: Internal inconsistencies in the PP cluster consisting of the SSCD PP Part 2 [PP_2], the SSCD PP Part 4 [PP_4] and the SSCD PP Part 5 [PP_5] are not known. The same holds for the PP cluster consisting of the SSCD PP Part 3 [PP_3] and the SSCD PP Part 6 [PP_6]. 'Strict conformance' claims of a TOE to several PPs inside a single PP cluster should therefore show no problem.

198 ***Issue:***

199 SSCD PP Part 2 [PP_2] and SSCD PP Part 3 [PP_3] show some inconsistencies in their Security Problem Definition, Security Objectives for the TOE and its operational environment and Security Functional Requirements (including tracings/mappings and related rationales) lying beyond those differences that are caused by the PPs' different scopes (i.e. TOE with onboard key generation and TOE with key import). How is it feasible to claim conformance to both PPs in one product certification without running in (formal) problems with the 'strict conformance' claim that is required by both PPs?

200 ***Agreed Interpretation:***

201 An easy solution to solve the issue previously described is given by the following approach:

202 The TOE and its related ST outlines two configurations, one configuration for the SSCD with onboard key generation and a second configuration for the SSCD with key import. Hereby, providing two configurations does not necessarily mean or require that e.g. at the time point of production, delivery or installation of the TOE a decision for one of the two configurations has to be taken and afterwards the TOE is restricted in its operational phase to the respective chosen configuration. A TOE that provides both configurations for parallel use in its operational phase is possible, and as a specific implementation solution it is allowed to bind the configuration to the respective SCD and its origin (i.e. TOE internal generation / external generation with import).

203 Each configuration claims 'strict conformance' to the SSCD PP(s) of the respective relevant PP cluster. To ease the ASE evaluation activities it is recommended to organize the ST according to these two configurations and assign the respective SSCD PPs' contents to the configurations. The configuration aspect should as well be followed in all further evaluation evidences and activities, and in particular the ST and the TOE related user guidance documentation should clearly address and clarify the respective

configuration scope, boundary and usage (including usage constraints/obligations, if applicable).

3 Abbreviations

CC	Common Criteria
CEM	Common Criteria Evaluation Methodology
CCRA	Common Criteria Recognition Arrangement
CGA	Certificate Generation Application
DTBS	Data To Be Signed
DTBS/R	DTBS Representation
eIDAS	electronic IDentification, Authentication and trust Services
EU	European Union
HID	Human Interface Device
JIL	Joint Interpretation Library
OE	Security Objective for the TOE Operational Environment
OSP	Organisational Security Policy
PP	Protection Profile
QSCD	Qualified Electronic Signature/Seal Creation Device
RAD	Reference Authentication Data
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SCD	Signature Creation Data
SFR	Security Functional Requirement
SOG-IS	Senior Officials Group Information Systems Security
SSCD	Secure Signature Creation Device
ST	Security Target
SVD	Signature Verification/Validation Data
TOE	Target Of Evaluation
TSS	TOE Summary Specification
VAD	Verification Authentication Data

For further abbreviations refer to the SSCD PP standards [PP_1, PP_2, PP_3, PP_4, PP_5, PP_6] and to the Common Criteria.

Note on the abbreviation ‘QSCD’:

For better readability of this document, the terms ‘qualified electronic signature creation device’ and ‘qualified electronic seal creation device’ are put together and jointly abbreviated by using the term ‘QSCD’, as far as no distinction between signatures and seals on content level is necessary. Note that for the notification of QSCDs according to [eIDAS_Reg, Article 31] a differentiation like ‘QSigCD’ for ‘qualified electronic signature creation device’ and

'QSealCD' for 'qualified electronic seal creation device' might be made. However, this is irrelevant for the purpose and content of the interpretation document at hand.

4 References

[ES_Dir] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 2000-01-19, Official Journal of the European Union

[ES_Impl] Commission Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council, 2003-07-15, Official Journal of the European Union

[eIDAS_Reg] 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, 2014-08-28, Official Journal of the European Union

[eIDAS_Impl] 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, 2016-04-26, Official Journal of the European Union

[ISO_15408] ISO/IEC 15408-1:2009 – Information technology – Security techniques – Evaluation criteria for IT security – Part 1, ISO, 2009

ISO/IEC 15408-2:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 2, ISO, 2008

ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3, ISO, 2008

[ISO_18045] ISO/IEC 18045:2008: Information technology – Security techniques – Methodology for IT security evaluation, ISO, 2008

[CC31_R3] Common Criteria for Information Technology Security Evaluation, Version 3.1

Part 1: Introduction and general model, Revision 3, July 2009

Part 2: Security functional components, Revision 3, July 2009

Part 3: Security assurance components, Revision 3, July 2009

http://www.commoncriteriaportal.org

[CEM31_R3] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 3, July 2009

http://www.commoncriteriaportal.org

[CC31_R4] Common Criteria for Information Technology Security Evaluation, Version 3.1

Part 1: Introduction and general model, Revision 4, September 2012

Part 2: Security functional components, Revision 4, September 2012

Part 3: Security assurance components, Revision 4, September 2012

http://www.commoncriteriaportal.org

[CEM31_R4] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 4, September 2012

http://www.commoncriteriaportal.org

[CC31_R5] Common Criteria for Information Technology Security Evaluation, Version 3.1

Part 1: Introduction and general model, Revision 5, April 2017

Part 2: Security functional components, Revision 5, April 2017

Part 3: Security assurance components, Revision 5, April 2017

http://www.commoncriteriaportal.org

[CEM31_R5] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 5, April 2017

http://www.commoncriteriaportal.org

[PP_1] Protection profiles for secure signature creation device – Part 1: Overview, CEN/ISSS –- Information Society Standardization System, EN 419211-1:2014, 2016-06-30

[PP_2] BSI-CC-PP-0059-2009-MA-02, Protection profiles for Secure signature creation device – Part 2: Device with key generation, CEN/ISSS – Information Society Standardization System, EN 419211-2:2013, 2016-06-30

[PP_3] BSI-CC-PP-0075-2012-MA-01, Protection profiles for secure signature creation device – Part 3: Device with key import, CEN/ISSS – Information Society Standardization System, EN 419211-3:2013, 2016-06-30

[PP_4] BSI-CC-PP-0071-2012-MA-01, Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application, CEN/ISSS – Information Society Standardization System, EN 419211-4:2013, 2016-06-30

[PP_5] BSI-CC-PP-0072-2012-MA-01, Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application, CEN/ISSS – Information Society Standardization System, EN 419211-5:2013, 2016-06-30

[PP_6] BSI-CC-PP-0076-2013-MA-01, Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted channel to signature creation application, CEN/ISSS – Information Society Standardization System, EN 419211-6:2014, 2016-06-30

[SOGIS_C] SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms, current version