ID&TRUST

IDENTITY APPLET V3.4/QSCD

QUALIFIED ELECTRONIC SIGNATURE COMPLIANT WITH IAS ECCV2 AND EIDAS

SECURITY TARGET

COMMON CRITERIA / ISO 15408

EAL4+

2020

Classification: Public

Revision History

Version	Date	Information
V1.00	18.08.2020	Final version
V1.01	16.09.2020	Minor modification
V1.02	13.10.2020	Update references Minor modification in section 1.4.2

Table of Contents

List of Tables

1. ST Introduction

1 This section provides document management and overview information that are required a potential user of the TOE to determine, whether the TOE fulfils its requirements.

2 Throughout this document, the term QSCD refers to Qualified Signature Creation Device.

3 The TOE is a composite TOE. The Common Criteria Mandatory Technical Document Composite product evaluation for Smart Cards and similar devices [8] contains all the relevant information about the methodology to handle such a TOE. The developer followed the direction of the mandatory document, and so should any relevant parties participate in the evaluation and certification of the TOE.

1.1. ST Reference

4 Title: Security Target IDentity Applet v3.4/QSCD - Qualified electronic signature compliant with IAS ECCv2 and eIDAS

5 TOE: IDentity Applet v3.4/QSCD on NXP JCOP 4 P71

6 Author: ID&Trust Ltd.

7 Version number: v1.02

8 Date: 13.10.2020

9 The Security Target defines the security requirements of a Qualified Signature Creation Device (QSCD) for the generation of signature-creation data (SCD) and the creation of qualified electronic signatures. Additionally, the TOE of this ST supports its authentication as QSCD by the certificate generation application (CGA) of the Certification service provider (CSP) and a trusted communication with this CGA for protection of signature verification data (SVD) generated and exported by the TOE and imported by CGA.

The TOE may implement additional functions and security requirements e.g. for editing and displaying the data to be signed (DTBS), but these additional functions and security requirements are not subject of this Security Target

10 Keywords: Security Target, Common Criteria, qualified signature-creation device, QSCD, electronic signature, digital signature

1.2. TOE Reference

11 The Security Target refers to the product “ID&Trust IDentity Applet Suite v3.4” for CC evaluation.

12 TOE Name: IDentity Applet v3.4/QSCD on NXP JCOP 4 P71

13 TOE short name: IDentity Applet v3.4/QSCD

14 TOE Identification Data: IDentity Applet/QSCD v3.4.7470

15 The TOE name and the TOE identification data constitute the accurate TOE reference.

16 Evaluation Criteria: [4]

17 Evaluation Assurance Level: EAL 4 augmented by AVA_VAN.5

18 Developer: ID&Trust Ltd.

19 Evaluation Sponsor: NXP Semiconductors Netherlands B.V. 5656, AG Eindhoven, High Tech Campus 60

20 Keywords: Qualified Signature-Creation Device, QSCD, electronic signature, digital signature

1.3. TOE Overview

21 The TOE comprises:

I. Underlying platform of the TOE, which is evaluated by Brightsight and certified by TÜV Rheinland Nederland B.V.

Evaluation assurance level: EAL6 augmented by ASE_TSS.2 and ALC_FLR.1.

CC Certification number: NSCIB-CC-180212-CR2

Long platform name: JCOP 4 P71

Short name: JCOP 4

It consists of:

a) Micro Controller (a secure smart card controller from NXP from the SmartMX3 family);
b) IC Dedicated Software (MC FW Micro Controller Firmware and Crypto Library);
c) IC Embedded Software JCOP4 (Java Card Virtual Machine, Runtime Environment, Java Card API);
d) Global Platform (GP) Framework;

II. the Application Part of the TOE:

ID&Trust IDentity Applet Suite v3.4/QSCD;

III. the associated guidance documentation [5], [6].

1.3.1. TOE usage and major security features

22 The TOE addressed by the current ST is a Qualified Signature Creation Device (QSCD) representing a contact or contactless smart card which is able to generate signature creation data (SCD) and create qualified electronic signatures. The TOE protects the SCD and ensures that only an authorized signatory can use it.

23 The TOE meets all the following requirements as defined in the [23] (article 26):

a) it is uniquely linked to the signatory;

b) it is capable of identifying the signatory;

c) it is created using means that the signatory can maintain under his sole control;

d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

24 IDentity Applet is a highly configurable eID solution. It is able to satisfy multiple different application requirements even within a single applet instance. The Application part of the TOE, the applet functionalities are distributed according to the following table:

Application	Function	Standard	Protection Profile
IDentity/PKI	Flexible PKI token	CEN TS 14890-1/2 IAS-ECC 1.0.1 [22]	-
IDentity/IAS	European card for e-Services and National e-ID applications	CEN/TS 15480-2 [21] IAS-ECC 1.0.1 [22]	-
IDentity/QSCD	Qualified Signature Creation Device	CEN/TS 15480-2 [21] IAS-ECC 1.0.1[22] REGULATION (EU) No 910/2014 [23] BSI TR-03117 [26]	[18] [19]
IDentity/IDL	International Driving License	ISO/IEC 18013	BSI-CC-PP-0055 [15]
IDentity/EDL	European Driving License	2012/383/EC	-
IDentity/eVR	Electronic Vehicle Registration	1999/37/EC	-
IDentity/eHC	Electronic Health Insurance	CEN/CWA 15794	-
IDentity/BAC	Basic Access Control (BAC)	ICAO Doc 9303 [13]	BSI-CC-PP-0055 [15]
IDentity-J	Basic Access Control (BAC) Password Authenticated Connection Establishment (PACE)	ICAO Doc 9303 [13]	JISEC500 [29] JISEC499 [30]
IDentity/PACE-EAC1	Password Authenticated Connection Establishment (PACE) Extended Access Control v1 (EAC1)	ICAO Doc 9303 [13] ICAO TR-SAC [14] BSI TR-03110 v2.21 [9], [10], [11], [12]	BSI-CC-PP-0068-V2-2011 [17] BSI-CC-PP-0056-V2-2012 [16]
IDentity/eIDAS	Password Authenticated Connection Establishment (PACE) Extended Access Control v2 (EAC2)	ICAO TR-SAC [14] BSI TR-03110 v2.21 [9], [10], [11], [12]	BSI-CC-PP-0087 [20]

1. Table Applet functionalities

25 All the functions are supplied by the applet “ID&Trust IDentity Applet Suite Version 3.4”, the behaviour of the applet changes according to the configuration applied during the personalization phase of IDentity Applet life cycle, and the environmental behaviour of the usage phase.

The scope of the current ST is only concerned with applet behaviour of configuration: IDentity/QSCD.

26 For the TOE, beside the QSCD application other applications may be present on the Platform. They are not relevant for the current ST and do not infer the Security Functions of the TOE. The TOE utilises the evaluation of the underlying Platform.

27 Part of the TOE is the associated guidance documentation, the IDentity Applet Suite v3.4 Administrator's Guide [5] and IDentity Applet Suite v3.4 User's Guide [6].

28 The intended customer of the product the Card Issuer, who is in charge of the issuance of the product to the smartcard holders.

1.3.2. TOE type

29 The TOE is the Smart Card Integrated Circuit with Dedicated Software, Embedded Software and IDentity Applet v3.4/QSCD.

1.3.3. Non-TOE hardware/software/firmware

30 There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application.

1.4. TOE Description

1.4.1. Product type

31 The TOE is a Smart Card Integrated Circuit with Dedicated Software, Embedded Software and IDentity Applet 3.4/QSCD.

1.4.2. Components of the TOE

32 **Micro Controller**

The Micro Controller is a secure smart card controller from NXP from the SmartMX3 family. The Micro Controller contains a co-processor for symmetric cipher, supporting DES operations and AES, as well as an accelerator for asymmetric algorithms. The Micro Controller further contains a physical random number generator. The supported memory technologies are volatile (Random Access Memory (RAM)) and non-volatile (Read Only Memory (ROM) and FLASH) memory. Access to all memory types is controlled by a Memory Management Unit (MMU) which allows to separate and restrict access to parts of the memory.

IC dedicated software - Micro Controller Firmware

The Micro Controller Firmware is used for testing of the Micro Controller at production, for booting of the Micro Controller after power-up or after reset, for configuration of communication devices and for writing data to non-volatile memory.

IC dedicated software - Crypto Library

The Crypto Library provides implementations for symmetric and asymmetric cryptographic operations, hashing, the generation of hybrid deterministic and hybrid physical random numbers and further tools like secure copy and compare. The supported asymmetric cryptographic operations are ECC and RSA. These algorithms use the Public Key Crypto Coprocessor (PKCC) of the Micro Controller for the cryptographic operations.

Micro Controller, IC dedicated software (Micro Controller Firmware, Crypto Library) are covered by the following certification:

Certification ID: BSI-DSZ-CC-1040-2019-MA-01

Evaluation

Level:	EAL6+ ALC_FLR.1 and ASE_TSS.2 according to Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-00084-2014.

IC Embedded Software

Certification ID:	NSCIB-CC-180212-CR2

JCOP4 consists of Java Card Virtual Machine (JCVM), Java Card Runtime Environment (JCRE), Java Card API (JCAPI), Global Platform (GP) framework, Configuration Module, etc.

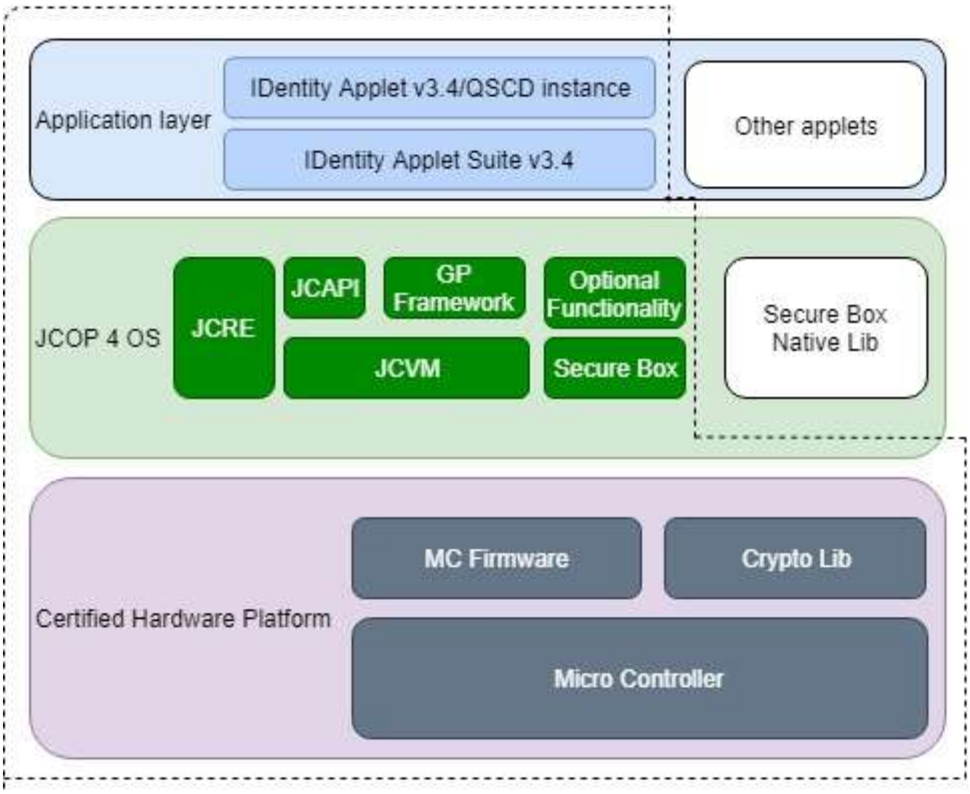
OS Name:	JCOP 4 Operating System
Applied OS configuration:	Banking & Secure ID
Product Identification:	JCOP 4 v4.7 R1.00.4
Evaluation Level:	CC EAL 6+ with ASE_TSS.2, ALC_FLR.1 according to Java Card System – Open Configuration Protection Profile, version 3.0.5, Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI, BSI-CC-PP-0099-2017).
Platform UGD:	[27]

IDentity Applet – accomplishing IDentity application

Product name:	ID&Trust IDentity Applet Suite
Version:	3.4
Applet name:[1]	IDentity Applet V3.4/QSCD
TOE Guidance Documentation[2]:	IDentity Applet Suite v3.4 Administrator's Guide [5]
	IDentity Applet Suite v3.4 User's Guide [6]

33 The logical architecture of the TOE:

[1] The applet is provided in cap file format.
[2] The AGD documents provided in electronic document format.



1. Figure TOE Boundaries

The TOE is a composite TOE and the dashed line denotes the whole TOE. The underlying certified hardware platform and JCOP 4 OS are marked with purple and green. In this ST the common short name of certified hardware platform and JCOP 4 OS is Platform.

The blue box marks the application layer. The ID&Trust IDentity Applet Suite v3.4 could be loaded in the Flash. During the creation phase an instance is created in the Flash and after several configuration steps it will be personalized as IDentity Applet v3.4/QSCD. For details please see: section 1.4.5 TOE life cycle and [5].

The boxes marked with white are not certified.

1.4.3. Operation of the TOE

34 The TOE is an QSCD which can generate the SCD/SVD key pair.

35 The IDentity Applet v3.4/QSCD is linked to a card reader/writer (card terminal) via the HW and physical interfaces of the smart card. The smart card has contact type and contactless type interfaces.

36 The TOE may be applied to a contact type card reader/writer or to a contactless card reader/writer. The card reader/writer either is an intelligent device having the capability to use the TOE or it is connected to a computer such as a personal computer and allows application programs (APs) to use the TOE.

37 The contact types interface of the TOE:

- Contact type (ISO/IEC 7816-3 complaint);
- Contactless type (ISO/IEC 14443 complaint);

38 The TOE is designed and produced in a secure environment.

39 A functional overview of the TOE in its distinct operational environments:

- The preparation environment, where it interacts with a certification service provider through a certificate-generation application (CGA) to obtain a certificate for the signature verification data (SVD) corresponding with signature creation data (SCD) the TOE has generated. The TOE can export the SVD through a trusted channel allowing the CGA to check the authenticity of the SVD. The initialization environment interacts further with the TOE to personalize it with the initial value of the reference-authentication data (RAD)
- The signing environment where it interacts with a signer through a signature-creation application (SCA) to sign data after authenticating the signer as its signatory. The signature-creation application provides the unique representation of data to be signed, thereof (DTBS/R) as input to the TOE signature-creation function and obtains the resulting digital signature.
- The management environments where it interacts with the user or an QSCD-Provisioning service provider to perform management operations, e.g. for the signatory to reset a blocked RAD. A single device, e.g. a smart card terminal, may provide the required secure environment for management and signing

40 The signing environment, the management environment and the preparation environment are secure and protect data exchanged with the TOE.

41 The TOE stores signature creation data and reference authentication data. The TOE may store multiple instances of SCD. In this case the TOE provides a function to identify each SCD and the SCA can provide an interface to the signer to select an SCD for use in the signature creation function of the QSCD. The TOE protects the confidentiality and integrity of the SCD and restricts its use in signature creation to its signatory. The digital signature created by the TOE may be used to create a qualified electronic signature as defined in Article 25 of [23]. Determining the state of the certificate as qualified is beyond the scope of this document.

42 The signature creation application is assumed to protect the integrity of the input it provides to the TOE signature creation function as being consistent with the user data authorized for signing by the signatory. Unless implicitly known to the TOE, the SCA indicates the kind of the signing input (as DTBS/R) it provides and computes any hash values required. The TOE may augment the DTBS/R with signature parameters it stores and then computes a hash value over the input as needed by the kind of input and the used cryptographic algorithm.

43 The TOE stores signatory reference authentication data to authenticate a user as its signatory. The RAD is a password e.g. PIN. The TOE protects the confidentiality and integrity of the RAD. The TOE may provide a user interface to directly receive verification authentication data (VAD) from the user, alternatively, the TOE receives the VAD from the signature creation application. If the signature creation application handles, is requesting or obtaining a VAD from the user, it is assumed to protect the confidentiality and integrity of this data.

44 A certification service provider and a QSCD-provisioning service provider interact with the TOE in the secure preparation environment to perform any preparation function of the TOE required before control of the TOE is given to the legitimate user. These functions may include:

- initializing the RAD,
- generating a key pair,
- storing personal information of the legitimate user.

45 The TOE and the CGA communicate through a trusted channel in order to protect the integrity and authenticity of the SVD exported from the TOE.

46 The TOE supports Certificate Request Signature (CRS) to provide evidence about the validity of the SVD for the CGA. The CRS also proves that the SVD belongs to the TOE.

The CRS key pair is generated separately from the SCD/SVD key pair on the TOE, but in case the generation the latter key pair the TOE signs the SVD with the private key of CRS. So, the CGA is able to verify the validity of the SVD by checking the CRS.

1.4.4. TOE Definition

47 The TOE is a combination of hardware and software configured to securely create, use and manage signature-creation data (SCD). The QSCD protects the SCD during its whole life cycle as to be used in a signature-creation process solely by its signatory.

48 The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the electronic signature.

49 The TOE provides the following functions:

(1) to generate signature-creation data (SCD) and the correspondent signature-verification data (SVD),
(2) to export the SVD for certification through a trusted channel to the CGA,
(3) to prove the identity as QSCD to external entities,
(4) to optionally, receive and store certificate info,
(5) to switch the TOE from a non-operational state to an operational state, and
(6) if in an operational state, to create digital signatures for data with the following steps:
  (a) select an SCD if multiple are present in the QSCD,
  (b) authenticate the signatory and determine its intent to sign,
  (c) receive the unique representation of data to be signed thereof (DTBS/R),
  (d) apply an appropriate cryptographic signature-creation function using the selected SCD to the DTBS/R.

50 The TOE may implement its function for digital signature creation to also conform to the specifications in ETSI TS 101 733 **(**CAdES**)** and ETSI TS 101 903 (XAdES) and ETSI TS 102 778 (PAdES). In this case the TOE may provide additional supporting functions, e.g. to support receiving and/or validating a time stamp.

51 The TOE is prepared for the signatory's use by

(1) generating at least one SCD/SVD pair, and
(2) personalizing for the signatory by storing in the TOE:
  (a) the signatory's reference authentication data (RAD)
  (b) optionally, certificate info for at least one SCD in the TOE.

52 After preparation, the SCD shall be in a non-operational state. Upon receiving a TOE, the signatory shall verify its non-operational state and change the SCD state to operational.

53 After preparation the intended, legitimate user should be informed of the signatory's verification authentication data (VAD) required for use of the TOE in signing. If the VAD is a password or PIN, providing this information shall protect the confidentiality of the corresponding RAD. There is a special VAD, which can be used only once in the TOE lifetime, the Signature Transport PIN, which has to be changed to Signature PIN in order to create digital signatures.

54 If the use of an SCD is no longer required, then it can be destroyed (e.g. overwritten) as well as the associated certificate info, if any exists.

1.4.5. TOE life cycle

1.4.5.1. General

55 The TOE lifecycle distinguishes stages for development production, preparation and operational use.

56 **1. Application note (from ST Author)**

The IDentity Applet Life cycle has the following phases, which differ from the whole TOE Lifecycle:

- IDentity Applet

LOADED (Creation phase)

- IDentity Instance

Personalization Phase

SELECTABLE (Configuration Phase)

CONFIGURED (Initialization Phase)

Operational Phase

PERSONALIZED

LOCKED

BLOCKED

These phases are detailed in the ID&Trust Identity Applet Suite Administrator's Guide [5]. These states and phases are presented here, because of informational reasons, to serve better understanding.

57 The development phase comprises the development and production of the TOE. The development phase is subject of the evaluation according to the assurance lifecycle (ALC) class. The development phase ends with the delivery of the TOE to the QSCD-provisioning service.

58 **2. Application note (from ST Author)**

The delivery procedures between ID&Trust (applet developer) and the manufacturer:

1. The IDentity Applet Developer develops a new version of the IDentity Applet v3.4/QSCD.
2. After the new version is tested a new release is issued and stored in configuration management system.
3. The new version of the IDentity Applet v3.4 is sent to as required by [27].

59 The operational usage of the TOE comprises the preparation stage and the operational use stage. The TOE operational use stage begins when the signatory has obtained both the VAD and the TOE. Enabling the TOE for signing requires at least one set of SCD stored in its memory.

60 The lifecycle may allow generation of SCD or SCD/SVD key pairs after delivery to the signatory as well.

1.4.5.2. Preparation stage

61 An QSCD-provisioning service provider having accepted it from a manufacturer prepares the TOE for use and delivers it to its legitimate user. The preparation phase ends when the legitimate user of the TOE, having received it from an QSCD provisioning service enables if an SCD it holds for use in signing.

62 During preparation of the TOE, as specified above, an QSCD-provisioning service provider performs the following tasks:

(1) Obtain information on the intended recipient of the device as required for the preparation process and for identification as a legitimate user of the TOE.
(2) Generate a PIN and/or obtain a biometric sample of the legitimate user, store this data as RAD in the TOE and prepare information about the VAD for delivery to the legitimate user.
(3) The TOE generating an SCD/SVD pair.
(4) Generate a certificate for at least one SCD as follows:
    a. Initializes the security functions in the TOE for the identification as QSCD, for the proof of this QSCD identity to external entities, and for the protected export of the SVD.
    b. Links the identity of the TOE as QSCD and the identity of the legitimate user as potential applicant for certificates for SVD generated by the TOE.
(5) Optionally, present certificate info to the QSCD.
(6) Deliver the TOE and the accompanying VAD info to the legitimate user.

63 The SVD certification task (third list item above) of an QSCD-provisioning service provider as specified in this ST may support a centralized, pre-issuing key generation process, with at least one key generated and certified, before delivery to the legitimate user. Alternatively, or additionally, that task may support key generation by the signatory after delivery and outside the secure preparation environment. A TOE may support both key generation processes, for example with a first key generated centrally and additional keys generated by the signatory in the operational use stage.

64 Data required for inclusion in the SVD certificate at least includes ([23] **Annex** I):

(a) the SVD which correspond to SCD under the control of the signatory;
(b) the name of the signatory or a pseudonym, which is to be identified as such;
(c) an indication of the beginning and end of the period of validity of the certificate.

The data included in the certificate may have been stored in the QSCD during personalization.

65 Before initiating the actual certificate signature, the certificate-generating application verifies the SVD received from the TOE by:

(1) establishing the sender as genuine QSCD
(2) establishing the integrity of the SVD to be certified as sent by the originating QSCD,
(3) establishing that the originating QSCD has been personalized for the legitimate user,
(4) establishing correspondence between SCD and SVD, and
(5) an assertion that the signing algorithm and key size for the SVD are approved and appropriate for the type of certificate.

66 The proof of correspondence between an SCD stored in the TOE and an SVD may be implicit in the security mechanisms applied by the CGA. Optionally, the TOE may support a function to provide an explicit proof of correspondence between an SCD it stores and an SVD realized by self-certification. Such a function may be performed implicitly in the SVD export function and may be invoked in the preparation environment without explicit consent of the signatory[3].

67 Prior to generating the certificate, the certification service provider shall assert the identity of the signatory specified in the certification request as the legitimate user of the TOE.

1.4.5.3. Operational use stage

68 In this lifecycle stage, the signatory can use the TOE to create advanced/qualified electronic signatures.

69 The TOE operational use stage begins when the signatory has obtained both the VAD and the TOE. Enabling the TOE for signing requires at least one set of SCD stored in its memory.

70 The signatory can also interact with the QSCD to perform management tasks, e.g. reset a RAD value or use counter if the password/PIN in the reference data has been lost or blocked. Such management tasks require a secure environment.

71 The signatory can render an SCD in the TOE permanently unusable. Rendering the last SCD in the TOE permanently unusable ends the life of the TOE as QSCD.

72 The TOE may support functions to generate additional signing keys. If the TOE supports these functions it shall support further functions to securely obtain certificates for the new keys. For an additional key the signatory may be allowed to choose the kind of certificate (qualified, or not) to obtain for the SVD of the new key. The signatory may also be allowed to choose some of the data in the certificate request for instance to use a pseudonym instead of the legal name in the certificate[4]. If the conditions to obtain a qualified certificate are met the new key can also

[3] Self-certification of the SVD is effectively computing a digital signature with the corresponding SCD. A signing operation requires explicit sole signatory control, this specific case, if supported, provides an exception to this rule as, before being delivered to the signatory, such control is evidently impossible.

[4] The certificate request in this case will contain the name of the signatory as the requester, as for instance it may be signed by the signatory's existing SCD.

be used to create advanced electronic signatures. The optional TOE functions for additional key generation and certification may require additional security functions in the TOE and an interaction with the QSCD-Provisioning service provider in an environment that is secure.

73 In the usage phase, SCD/SVD generation by the TOE and SVD export from the TOE may take place in the preparation stage and/or in the operational use stage. The TOE then provides a trusted channel to the CGA protecting the integrity of the SVD.

Before generating the certificate including the SVD exported from the TOE, the CGA additionally establishes:

(1) the identity of the TOE as QSCD,
(2) that the originating QSCD has been personalized for the applicant for the certificate as legitimate user, and
(3) the correspondence between SCD stored in the QSCD and the received SVD.

74 The TOE life cycle as QSCD ends when all SCD stored in the TOE are destructed. This may include deletion of the corresponding certificates.

1.4.6. TOE security functions

75 The following TOE ensured security functions are the most significant for its operational use:

76 - Only entities possessing authorization can get access to the use of the signature creation data stored on the TOE and use functionality of card,

77 - Verifying authenticity and integrity as well as securing confidentiality of data in the communication channel (trusted channel) between the TOE and the CGA connected,

78 - Self-protection of the TOE security functionality and the data stored inside.

79 - The TOE supports Certificate Request Signature (CRS) to provide evidence about the validity of the SVD for the CGA.

80 - Post-issuance SCD/SVD key pair generation and certificate generation for R.Admin, if EAC2 is applied.

81 Above mentioned functions are described below informally, and in detail in section 7.1.

2. Conformance Claims

2.1. CC Conformance Claim

82 This Security Target is conforming to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April [2].
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017 [3]

83 As follows

Part 2 extended (see Chapter 5 Extended components definition)

Part 3 conformant.

84 The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017 [4]

has been taken into account.

2.2. PP Claim, Package Claim

85 This Security Target claims strict conformance to the following PPs:

Title:	**Protection profiles for secure signature creation device — Part 2: Device with key generation**
Standard ID:	EN 419211-2:2013
CC version:	3.1 (revision 4)
Assurance level:	The minimum assurance level for this PP is EAL4 augmented with AVA_VAN.5
Title:	**Protection profiles for Secure signature creation device — Part 4: Device with key generation and trusted communication with certificate generation application**
Standard ID:	EN 419211-4:2013
CC version:	3.1 (revision 4)
Assurance Level:	The minimum assurance level for this PP is EAL4 augmented with AVA_VAN.5.

86 This ST is conforming to assurance package EAL4 augmented with AVA_VAN.5 defined in [3].

2.3. Conformance rationale

87 The ST is built on the PPs referenced above, which according to the certifications conform to the CC version stated above.

88 This ST is conformant with Common Criteria Part 2 [2] extended due to additional components as stated in [18], and [19].

89 This ST is conformant to Common Criteria Part 3 [3].

90 The current ST refines the Assets, threats, objectives and SFR of [18] and [19].

91 The Security Target claims **strict conformance** to two PPs: [18] and [19].

92 The Target of Evaluation (TOE) is Qualified Signature Creation Device (QSCD) for the generation of signature-creation data (SCD) and the creation of qualified electronic signatures. It fulfils requirements of [23]. The Security Target refers to the QSCD compliant configurations of the IDentity Applet Suite v3.4. The IDentity Applet v3.4/QSCD is a Java Card Application used exclusively on the Platform, which is a CC EAL6+ certified product.

The TOE is thus **consistent** with the **TOE type** in the PP.

3. Application note (from ST author)

The [18] and [19] reference to Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, but it was repealed. Legislation in force [23] do not influence the security aspects of the current ST.

The new regulation does not know the Secure Signature Creation Device (SSCD), but it introduced the Qualified Signature Creation Device (QSCD) concept. For the aspect of security and the current ST it means only changing in the name, so in the current ST the QSCD is used instead of SSCD, but it does not affect the strict conformance to [18] and [19].

93 The **security problem definition** of this security target is **consistent** with the statement of the security problem definition in the PPs, as the security target claims strict conformance to the PPs and no other threats.

94 The **security objectives** of the TOE of this security target are **consistent** with the statement of the security objectives in the PPs as the security target claims strict conformance to the PPs.

95 The security objectives for the operational environment in this security target include all security objectives for the operational environment from the PPs.

The security objectives do not affect the strict conformance.

96 The **security requirements** of this security target are **consistent** with the statement of the security requirements in the PPs as the security target claims strict conformance to the PP. All assignments and selections of the security functional requirements are defined in the PP section 9.1 and in this security target section 6.1.

2.4. Statement of compatibility

2.4.1. Security Functionalities

97 The following table contains the security functionalities of the [7] and of this ST, showing which Functionality correspond to the Platform-ST and which has no correspondence. This statement is compliant to the requirements of [8].

98 A classification of TSFs of the [7] has been made. Each TSF has been classified as ‘relevant’ or ‘not relevant’ for this ST.

Platform Security Functionality	Corresponding TOE Security Functionality	Relevant/Not relevant	Remarks
SF.JCVM	TSF.Platform TSF.AppletparameterSign	Relevant	Java Card Virtual Machine

Platform Security Functionality	Corresponding TOE Security Functionality	Relevant/Not relevant	Remarks
SF.CONFIG	-	Not relevant	Configuration Management
SF.OPEN	TSF.Platform	Relevant	Card Content Management
SF.CRYPTO	TSF.Authenticate TSF.CryptoKey TSF.AppletparameterSign TSF.Platform	Relevant	Cryptographic Functionality
SF.RNG	TSF.Authenticate TSF.CryptoKey TSF.TrustedChannel TSF.Platform	Relevant	Random Number Generator
SF.DATA_STORAGE	TSF.AccessControl TSF.Authenticate TSF.CryptoKey TSF.AppletparameterSign TSF.Platform	Relevant	Secure Data Storage
SF.PUF	-	Not relevant	User Data Protection using PUF
SF.EXT_MEM	-	Not relevant	External Memory
SF.OM	TSF.AppletparameterSign TSF.Platform	Relevant	Java Object Management
SF.MM	-	Not relevant	Memory Management
SF.PIN	TSF.AccessControl TSF.Authenticate TSF.CryptoKey TSF.AppletparameterSign TSF.Platform	Relevant	PIN Management
SF.PERS_MEM	TSF.AppletparameterSign TSF.Platform	Relevant	Persistent Memory Management
SF.SENS_RES	-	Not relevant	Sensitive Result
SF.EDC	TSF.AppletparameterSign TSF.Platform	Relevant	Error Detection Code API
SF.HW_EXC	TSF.Platform	Relevant	Hardware Exception Handling
SF.RM	-	Not relevant	Restricted Mode
SF.PID	-	Not relevant	Platform Identification
SF.SMG_NSC	TSF.Platform	Relevant	No Side-Channel
SF.ACC_SBX	-	Not relevant	Secure Box
SF.MOD_INVOC	-	Not relevant	Module Invocation

2. Table Classification of Platform-TSFs

99 All the above Platform-TSFs which are indicated as relevant are relevant for this ST.

100 **4. Application note (by the ST author)**

The TSF.Platform Security functionality in the above list represents functionalities which are not directly used in the IDentity Applet v3.4/QSCD, they are implicitly invoked by calls to the Platform, respectively the JCOP operating system. These functions are called altogether as TSF.Platform.

2.4.2. OSPs

101 None of the OSPs of this ST are applicable to the Platform and therefore not mappable for the Platform-ST.

The OSPs from the Platform-ST [7] are not deal with any additional security components.

2.4.3. Security objectives

102 These Platform-ST objectives can be mapped to this STs objectives as shown in the following table, so they are relevant.

Objective from the Platform-ST	Objective from this ST
OT.ALARM	OT.SCD_Secrecy OT.Tamper_Resistance
OT.CIPHER	OT.Lifecycle_Security OT.SCD_Unique OT.SCD_SVD_Corresp OT.SCD_Secrecy
OT.COMM_AUTH	OT.Lifecycle_Security OT.Sig_Secure OT.TOE_QSCD_Auth
OT.COMM_CONFIDENTIALITY	OT.Lifecycle_Security OT.Sig_Secure OT.TOE_QSCD_Auth OT.TOE_TC_SVD_Exp
OT.COMM_INTEGRITY	OT.Lifecycle_Security OT.Sig_Secure OT.TOE_QSCD_Auth OT.TOE_TC_SVD_Exp
OT.GLOBAL_ARRAYS_CONFID	OT.SCD_Secrecy OT.Sigy_SigF
OT.KEY-MNGT	OT.Lifecycle_Security OT.SCD_Unique OT.SCD_SVD_Corresp OT.SCD_Secrecy OT.Sig_Secure OT.TOE_QSCD_Auth OT.TOE_TC_SVD_Exp OT.Sigy_SigF
OT.OPERATE	OT.SCD_Secrecy OT.Tamper_Resistance OT.Sigy_SigF
OT.PIN-MNGT	OT.SCD_SVD_Corresp OT.SCD_Secrecy OT.Sig_Secure OT.Sigy_SigF OT.DTBS_Integrity_TOE OT.Lifecycle_Security OT.SCD_Secrecy OT.Sig_Secure
OT.REALLOCATION	OT.SCD_Secrecy OT.Sigy_SigF
OT.RESOURCES	OT.SCD_Secrecy OT.Tamper_Resistance
OT.RND	OT.TOE_QSCD_Auth
OT.RNG	OT.TOE_QSCD_Auth
OT.SCP.IC	OT.SCD_Secrecy OT.Tamper_Resistance OT.EMSEC_Design OT.Tamper_ID

Objective from the Platform-ST	Objective from this ST
OT.SCP.RECOVERY	OT.SCD_Secrecy OT.Tamper_Resistance
OT.SCP.SUPPORT	OT.Lifecycle_Security OT.SCD_Unique OT.SCD_SVD_Corresp OT.SCD_Secrecy OT.Sig_Secure OT.TOE_QSCD_Auth OT.TOE_TC_SVD_Exp
OT.SID_MODULE	OT.SCD_Secrecy
OT.TRANSACTION	OT.SCD_Secrecy OT.Sigy_SigF

3. Table Mapping of security objectives for the TOE

103 The following Platform-ST objectives are not relevant for or cannot be mapped to the TOE of this ST:

- OT.FIREWALL
- OT.GLOBAL_ARRAYS_INTEG
- OT.NATIVE
- OT.SENSITIVE_RESULTS_INTEG
- OT.OBJ-DELETION
- OT.APPLI-AUTH
- OT.DOMAIN-RIGHTS
- OT.CARD-MANAGEMENT
- OT.IDENTIFICATION
- OT.SEC_BOX_FW
- OT.CARD-CONFIGURATION
- OT.ATTACK-COUNTER
- OT.RESTRICTED-MODE

cannot be mapped because these are out of scope.

104 The objectives for the operational environment can be mapped as follows:

Security Objectives for the environment of the [7]	Classification of OE	Comments
OE.APPLET	CfPOE	Covered by ALC class
OE.PROCESS_SEC_IC	CfPOE	Covered by the Platform's certification and ALC class
OE.VERIFICATION	CfPOE	Covered by ALC class
OE.CODE-EVIDENCE	CfPOE	Covered by ALC class
OE.USE_DIAG	SgOE	OE.Dev_Prov_Service
OE.USE_KEYS	SgOE	OE.HID_VAD
OE.APPS-PROVIDER	CfPOE	Covered by ALC class
OE.VERIFICATION-AUTHORITY	CfPOE	Covered by ALC class
OE.KEY-CHANGE	CfPOE	Covered by ALC class
OE.SECURITY-DOMAINS	CfPOE	Covered by ALC class

Table 4 Mapping of security objectives of the environment

105 There is no conflict between security objectives of this ST and the Platform-ST.

2.4.4. Security requirements

106 The Security Requirements of the Platform-ST can be mapped as follows:

Platform SFR	Corresponding TOE SFR	Category of Plaform's SFR	Remarks
FAU_ARP.1	FPT_PHP.3	RP_SFR-MECH	FAU_ARP.1 facilitate to protect the TOE as required by FPT_PHP.3
FAU_SAS.1[SCP]	-	IP_SFR	-
FCO_NRO.2[SC]	-	IP_SFR	-
FCS_CKM.1	FCS_CKM.1	RP_SFR-SERV	FCS.CKM.1 of the Platform is applied to generate SVD/SVD keypair.
FCS_CKM.4	FCS_CKM.4	RP_SFR-SERV	FCS.CKM.4. of the Platform is applied to destroy SCD.
FCS_COP.1	FCS_COP.1	RP_SFR-SERV	FCS_COP.1[ECSignature] is applied to generate digital signature (EC) FCS_COP.1[RSASignaturePKCS1] is applied to generate signature (RSA). FCS_COP.1[SHA] is applied, if the last part of the hash calculation is executed on the TOE. FCS_COP.1[ECSignature] or
	FDP_DAU.2/SVD	RP_SFR-SERV	FCS_COP.1[RSASignaturePKCS1] are applied (depends on the selected algorithm) for FDP_DAU.2/SVD
	FIA_API.1	RP_SFR-SERV	In case active authentication the FCS_COP.1[ECSignature] and FCS_COP.1[RSASignaturePKCS1] could be applied.
FCS_RNG.1	FIA_API.1	RP_SFR-SERV	In case Symmetric Authentication method to generate secure random the FCS_RNG.1 is applied.
	FTP_ITC.1/SVD	RP_SFR-SERV	In case Symmetric Authentication method to generate secure random the FCS_RNG.1 is applied to provide trusted channel.
FCS_RNG.1[HDT]	-	IP_SFR	-
FDP_ACC.1[EXT-MEM]	-	IP_SFR	-
FDP_ACF.1[SD]	-	IP_SFR	
FDP_ACC.1[SD]	-	IP_SFR	-

Platform SFR	Corresponding TOE SFR	Category of Plaform's SFR	Remarks
FDP_ACF.1[FIREWALL]	-	IP_SFR	-
FDP_ACC.2[FIREWALL]	-	IP_SFR	-
FDP_ACC.2[ADEL]	-	IP_SFR	-
FDP_ACC.2[Secure Box]	-	IP_SFR	-
FDP_ACC.2[RM]	-	IP_SFR	-
FDP_ACF.1[ADEL]	-	IP_SFR	-
FDP_ACF.1[EXT-MEM]	-	IP_SFR	-
FDP_ACF.1[Secure Box]	-	IP_SFR	-
FDP_ACF.1[RM]	-	IP_SFR	-
FDP_IFC.1[JCVM]	-	IP_SFR	-
FDP_IFC.2[SC]	-	IP_SFR	-
FDP_IFC.2[CFG]	-	IP_SFR	-
FDP_IFC.1[MODULAR-DESIGN]	-	IP_SFR	-
FDP_IFF.1[JCVM]	-	IP_SFR	-
FDP_IFF.1[SC]	-	IP_SFR	-
FDP_IFF.1[CFG]	-	IP_SFR	-
FDP_IFF.1[MODULAR-DESIGN]	-	IP_SFR	-
FDP_ITC.2[CCM]	-	IP_SFR	-
FDP_RIP.1[OBJECTS]	-	IP_SFR	-
FDP_RIP.1[ABORT]	-	IP_SFR	-
FDP_RIP.1[APDU]	-	IP_SFR	-
FDP_RIP.1[bArray]	-	IP_SFR	-
FDP_RIP.1[GlobalArray_Refined]	-	IP_SFR	-
FDP_RIP.1[KEYS]	FDP_RIP.1	RP_SFR-MECH	FDP_RIP.1[KEYS] is applied to destroy the SCD in the transient memory.
FDP_RIP.1[TRANSIENT]	-	IP_SFR	-
FDP_RIP.1[ADEL]	-	IP_SFR	-
FDP_RIP.1[ODEL]	-	IP_SFR	-
FDP_ROL.1[FIREWALL]	-	IP_SFR	-
FDP_ROL.1[CCM]	-	IP_SFR	-
FDP_SDI.2[DATA]	FDP_SDI.2/Persistent	RP_SFR-MECH	FDP_SDI.2[DATA] is applied to protect SCD against integrity errors.
	FDP_SDI.2/DTBS	RP_SFR-MECH	FDP_SDI.2[DATA] is applied to protect DTBS against integrity errors.
	FPT_TST.1	RP_SFR-MECH	FDP_SDI.2[DATA] checks the integrity of RAD.
FDP_SDI.2[SENSITIVE_RESULT]	-	IP_SFR	-
FDP_UIT.1[CCM]	-	IP_SFR	-

Platform SFR	Corresponding TOE SFR	Category of Plaform's SFR	Remarks
FIA_AFL.1[PIN]	FIA_AFL.1	RP_SFR-SERV	FIA_AFL.1[PIN] is applied to protect the PIN code against authentication errors.
FIA_ATD.1[AID]	-	IP_SFR	-
FIA_ATD.1[MODULAR-DESIGN]	-	IP_SFR	-
FIA_UID.1[SC]	-	IP_SFR	-
FIA_UID.1[CFG]	-	IP_SFR	-
FIA_UID.1[RM]	-	IP_SFR	-
FIA_UID.2[AID]	-	IP_SFR	-
FIA_UID.1[MODULAR-DESIGN]	-	IP_SFR	-
FIA_USB.1[AID]	-	IP_SFR	-
FIA_USB.1[MODULAR-DESIGN]	-	IP_SFR	-
FIA_UAU.1[SC]	-	IP_SFR	-
FIA_UAU.2[RM]	-	IP_SFR	-
FIA_UAU.4[SC]	-	IP_SFR	-
FMT_MSA.1[JCRE]	-	IP_SFR	-
FMT_MSA.1[JCVM]	-	IP_SFR	-
FMT_MSA.1[ADEL]	-	IP_SFR	-
FMT_MSA.1[SC]	-	IP_SFR	-
FMT_MSA.1[EXT-MEM]	-	IP_SFR	-
FMT_MSA.1[SecureBox]	-	IP_SFR	-
FMT_MSA.1[CFG]	-	IP_SFR	-
FMT_MSA.1[SD]	-	IP_SFR	-
FMT_MSA.1[RM]	-	IP_SFR	-
FMT_MSA.1[MODULAR-DESIGN]	-	IP_SFR	-
FMT_MSA.2[FIREWALL-JCVM]	-	IP_SFR	-
FMT_MSA.3[FIREWALL]	-	IP_SFR	-
FMT_MSA.3[JCVM]	-	IP_SFR	-
FMT_MSA.3[ADEL]	-	IP_SFR	-
FMT_MSA.3[EXT-MEM]	-	IP_SFR	-
FMT_MSA.3[SecureBox]	-	IP_SFR	-
FMT_MSA.3[CFG]	-	IP_SFR	-
FMT_MSA.3[SD]	-	IP_SFR	-
FMT_MSA.3[SC]	-	IP_SFR	-
FMT_MSA.3[RM]	-	IP_SFR	-
FMT_MSA.3[MODULAR-DESIGN]	-	IP_SFR	-
FMT_MTD.1[JCRE]	-	IP_SFR	-
FMT_MTD.3[JCRE]	-	IP_SFR	-
FMT_SMF.1	-	IP_SFR	-
FMT_SMF.1[ADEL]	-	IP_SFR	-
FMT_SMF.1[EXT-MEM]	-	IP_SFR	-

Platform SFR	Corresponding TOE SFR	Category of Plaform's SFR	Remarks
FMT_SMF.1[Secure Box]	-	IP_SFR	-
FMT_SMF.1[CFG]	-	IP_SFR	-
FMT_SMF.1[SD]	-	IP_SFR	-
FMT_SMF.1[SC]	-	IP_SFR	-
FMT_SMF.1[RM]	-	IP_SFR	-
FMT_SMF.1[MODULAR-DESIGN]	-	IP_SFR	-
FMT_SMR.1	-	IP_SFR	-
FMT_SMR.1[INSTALLER]	-	IP_SFR	-
FMT_SMR.1[ADEL]	-	IP_SFR	-
FMT_SMR.1[CFG]	-	IP_SFR	-
FMT_SMR.1[SD]	-	IP_SFR	-
FMT_SMR.1[MODULAR-DESIGN]	-	IP_SFR	-
FPR_UNO.1	-	IP_SFR	-
FPT_EMSEC.1	FPT_EMS.1	RP_SFR-MECH	FPT_EMS.1 matches the FPT_EMSEC.1 of the Platform.
FPT_FLS.1	FPT_FLS.1	RP_SFR-MECH	FPT_FLS.1 of the Platform ensures the secure state of the TOE as required by FPT_FLS.1
FPT_FLS.1[INSTALLER]	-	IP_SFR	-
FPT_FLS.1[ADEL]	-	IP_SFR	-
FPT_FLS.1[ODEL]	-	IP_SFR	-
FPT_FLS.1[CCM]	-	IP_SFR	-
FPT_FLS.1[MODULAR-DESIGN]	-	IP_SFR	-
FPT_TDC.1	-	IP_SFR	-
FPT_RCV.3[INSTALLER]	-	IP_SFR	-
FPT_PHP.3	FPT_PHP.1	RP_SFR-MECH	FPT_PHP.3 of the Platform covers the requirement of FPT_PHP.3
	FPT_PHP.3	RP_SFR-MECH	FPT_PHP.3 matches the FPT_PHP.3 of the Platform.
FTP_ITC.1[SC]	-	IP_SFR	-
ADV_SPM.1	-	IP_SFR	-

5. Table Mapping of Security requirements

2.5. Assurance requirements

107 This ST requires EAL 4 according to Common Criteria V3.1 R5 augmented by AVA_VAN.5.

108 The Platform-ST [7] requires EAL 6 according to Common Criteria V3.1 R5 augmented by: ASE_TSS.2 and ALC_FLR.1.

109 As EAL 6 covers all assurance requirements of EAL 4 all non-augmented parts of this ST will match to the Platform-ST [7] assurance requirements.

2.6. Analysis

110 Overall there is no conflict between security requirements of this ST and the Platform-ST [7].

3. Security Problem Definition

3.1. Assets, users and threat agents

111 The Common Criteria define assets as entities that the owner of the TOE presumably places value upon. The term “asset” is used to describe the threats in the operational environment of the TOE.

3.1.1. Assets and objects

SCD

Signature Creation Data

112 Private key used to perform an electronic signature operation. The confidentiality, integrity and signatory’s sole control over the use of the SCD must be maintained.

SVD

Signature Verification Data

113 Public key linked to the SCD and used to perform digital signature verification. The integrity of the SVD when it is exported must be maintained.

DTBS and DTBS/R

Data to be Sign

114 Set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the digital signature must be maintained.

3.1.2. User and subjects acting for users

User

115 End user of the TOE who can be identified as Administrator or Signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.

Signatory

116 User who hold the TOE and use it on his own behalf or on behalf of the natural or legal person or entity they represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as signatory.

Administrator

117 User who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator.

3.1.3. Threat agents

Attacker

118 Human or process acting on their behalf located outside the TOE. The main goal of the attacker is to access the SCD or to falsify the electronic signature. The attacker has got a high attack potential and knows no secret.

3.2. Threats

T.SCD_Divulg

Storing, copying, and releasing of the signature creation data

119 An attacker stores or copies the SCD outside the TOE. An attacker can obtain the SCD during generation, storage and use for signature creation in the TOE.

T.SCD_Derive

Derive the signature creation data

120 An attacker derives the SCD from publicly known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data exported outside the TOE, which is a threat against the secrecy of the SCD.

T.Hack_Phys

Physical attacks through the TOE interfaces

121 An attacker interacts physically with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD and DTBS.

T.SVD_Forgery

Forgery of the signature verification data

122 An attacker forges the SVD presented by the CSP to the CGA. This results in loss of SVD integrity in the certificate of the signatory.

T.SigF_Misuse

Misuse of the signature creation function of the TOE

123 An attacker misuses the signature creation function of the TOE to create SDO for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

T.DTBS_Forgery

Forgery of the DTBS/R

124 An attacker modifies the DTBS/R sent by the SCA. Thus the DTBS/R used by the TOE for signing does not match the DTBS the signatory intended to sign.

T.Sig_Forgery

Forgery of the electronic signature

125 An attacker forges a signed data object, maybe using an electronic signature which has been created by the TOE, and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature created by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

3.3. Organizational Security Policies

P.CSP_QCert

Qualified certificate

126 The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. the [23], article 3, clause 14, and Annex **I**) for the SVD generated by the QSCD. 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 QSCD is evident with signatures through the certificate or other publicly available information.

P.QSign

Qualified electronic signatures

127 The signatory uses a signature creation system to sign data with an advanced electronic signature (cf. the [23], article 3, clause 15), which is a qualified electronic signature if it is based on a valid qualified certificate (according to the [23] Annex I)[5]. The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the QSCD. The QSCD creates the electronic signature created with a SCD implemented in the QSCD that the signatory maintains under his sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

P.Sigy_QSCD

TOE as Qualified signature creation device

128 The TOE meets the requirements for an QSCD laid down in Annex II of the [23]. This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once.

P.Sig_Non-Repud

Non-repudiation of signatures

129 The life cycle of the QSCD, 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.

3.4. Assumptions

A.CGA

Trustworthy certification generation application

130 The CGA protects the authenticity of the signatory’s name or pseudonym and the SVD in the (qualified) certificate by an advanced electronic signature of the CSP.

A.SCA

Trustworthy signature creation application

131 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.

---

[5] It is a non-qualified advanced electronic signature if it is based on a non-qualified certificate for the SVD.

4. Security Objectives

4.1. Security Objectives for the TOE

OT.Lifecycle_Security

Lifecycle security

132 The TOE shall detect flaws during the initialization, personalization and operational usage. The TOE shall securely destroy the SCD on demand of the signatory

133 **5. Application note (taken from application note 1 from [18]):**

The TOE may contain more than one set of SCD. 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 QSCD e.g. after the (qualified) certificate for the corresponding SVD has been expired.

OT.SCD/SVD_Auth_Gen

Authorized SCD/SVD generation

134 The TOE shall provide security features to ensure that authorized users only may invoke the generation of the SCD and the SVD.

OT.SCD_Unique

Uniqueness of the signature creation data

135 The TOE shall ensure the cryptographic quality of an SCD/SVD pair it creates as suitable for the advanced or qualified electronic signature. The SCD used for signature creation shall practically occur only once and shall not be reconstructable from the SVD. In that context ‘practically occur once’ means that the probability of equal SCDs is negligible.

OT.SCD_SVD_Corresp

Correspondence between SVD and SCD

136 The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE. This includes unambiguous reference of a created SVD/SCD pair for export of the SVD and in creating an electronic signature creation with the SCD.

OT.SCD_Secrecy

Secrecy of the signature creation data

137 The secrecy of an SCD (used for signature creation) shall be reasonably assured against attacks with a high attack potential.

138 **6. Application note (taken from application note 2 from [18])**

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

OT.Sig_Secure

Cryptographic security of the electronic signature

139 The TOE shall create digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD shall not be reconstructable using the digital signatures or any other data exportable from the TOE. The digital signatures shall be resistant against these attacks, even when executed with a high attack potential.

OT.Sigy_SigF

Signature creation function for the legitimate signatory only

140 The TOE shall provide the digital signature creation function for the legitimate signatory only and protects the SCD against the use of others. The TOE shall resist attacks with high attack potential.

OT.DTBS_Integrity_TOE

DTBS/R integrity inside the TOE

141 The TOE must not alter the DTBS/R. As by definition of the DTBS/R this may consist of the DTBS themselves, this objective does not conflict with a signature creation process where the TOE hashes the provided DTBS (in part or entirely) for signature creation.

OT.EMSEC_Design

Provide physical-emanation security

142 The TOE shall be designed and built in such a way as to control the production of intelligible emanations within specified limits.

OT.Tamper_ID

Tamper detection

143 The TOE shall provide system features that detect physical tampering of its components, and uses those features to limit security breaches

OT.Tamper_Resistance

Tamper resistance

144 The TOE shall prevent or resist physical tampering with specified system devices and components.

OT.TOE_QSCD_Auth

Authentication proof as QSCD

145 The TOE shall hold unique identity and authentication data as QSCD and provide security mechanisms to identify and to authenticate itself as QSCD.

OT.TOE_TC_SVD_Exp

TOE Trusted channel for SVD export

146 The TOE shall provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA. The TOE shall enable the CGA to detect alteration of the SVD exported by the TOE.

4.2. Security Objectives for the Operational Environment

OE.SVD_Auth

Authenticity of the SVD

147 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 QSCD of the signatory and the SVD in the qualified certificate.

OE.CGA_Qcert

Generation of qualified certificates

148 The CGA shall generate a qualified certificate that includes (amongst others)

(a) the name of the signatory controlling the TOE,
(b) the SVD matching the SCD stored in the TOE and being under sole control of the signatory,
(c) the advanced signature of the CSP.

The CGA shall confirm with the generated qualified certificate that the SCD corresponding to the SVD is stored in a QSCD.

OE.Dev_Prov_Service

Authentic QSCD provided by QSCD-provisioning service

149 The QSCD Provisioning Service handles authentic devices that implement the TOE, prepares the TOE for proof as QSCD to external entities, personalises the TOE for the legitimate user as signatory, links the identity of the TOE as QSCD with the identity of the legitimate user, and delivers the TOE to the signatory. Note: This objective replaces OE.QSCD_Prov_Service from the [18], which is possible as it does not imply any additional requirements for the operational environment when compared to OE.QSCD_Prov_Service (OE.Dev_Prov_Service is a subset of OE.QSCD_Prov_Service).

OE.HID_VAD

Protection of the VAD

150 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.

OE.DTBS_Intend

SCA sends data intended to be signed

151 The signatory shall use a trustworthy SCA that

- generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE,
- sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE,
- attaches the signature produced by the TOE to the data or provides it separately.

152 **7. Application note (taken from application note 3 from [18])**

The SCA should be able to support advanced electronic signatures. Currently, there exist three formats defined by ETSI recognized as meeting the requirements needed by advanced electronic signatures: CAdES, XAdES and PAdES. These three formats mandate to include the hash of the signer's public key certificate in the data to be signed. In order to support for the mobility of the signer, it is recommended to store the certificate info on the QSCD for use by SCA and identification of the corresponding SCD if more than one SCD is stored on the QSCD.

OE.DTBS_Protect

SCA protects the data intended to be signed

153 The operational environment shall ensure that the DTBS/R cannot be altered in transit between the SCA and the TOE. In particular, if the TOE requires a trusted channel for import of the DTBS/R, the SCA shall support usage of this trusted channel.

OE.Signatory

Security obligation of the Signatory

154 The Signatory checks that the SCD stored in the QSCD received from QSCD-provisioning service is in non-operational state. The signatory shall keep their VAD confidential

OE.CGA_QSCD_Auth

Pre-initialisation of the TOE for QSCD authentication

155 The CSP shall check by means of the CGA whether the device presented for application of a (qualified) certificate holds unique identification as QSCD, successfully proved this identity as QSCD to the CGA, and whether this identity is linked to the legitimate holder of the device as applicant for the certificate.

OE.CGA_TC_SVD_Imp

CGA trusted channel for SVD import

156 The CGA shall detect alteration of the SVD imported from the TOE with the claimed identity of the QSCD.

The developer prepares the TOE by pre-initialisation for the delivery to the customer (i.e. the QSCD provisioning service) in the development phase not addressed by a security objective for the operational environment. The QSCD Provisioning Service performs initialisation and personalisation as TOE for the legitimate user (i.e. the Device holder). If the TOE is delivered to the Device holder with SCD the TOE is a QSCD. This situation is addressed by OE.QSCD_Prov_Service except the additional initialisation of the TOE for proof as QSCD and trusted channel to the CGA. If the TOE is delivered to the Device holder without a SCD the TOE will be a QSCD only after generation of the first SCD/SVD pair. Because this SCD/SVD pair generation is performed by the signatory in the operational use stage the TOE provides additional security functionality addressed by OT.TOE_QSCD_Auth and OT.TOE_TC_SVD_Exp. But this security functionality must be initialised by the QSCD Provisioning Service as described in OE.Dev_Prov_Service. Therefore, this ST substitutes OE.QSCD_Prov_Service (from [18]) by OE.Dev_Prov_Service allowing generation of the first SCD/SVD pair after delivery of the TOE to the Device holder and requiring initialisation of security functionality of the TOE. Nevertheless the additional security functionality must be used by the operational environment as described in OE.CGA_QSCD_Auth and OE.CGA_TC_SVD_Imp. This approach does not weaken the security objectives of and requirements to the TOE but enforce more security functionality of the TOE for additional method of use. Therefore, it does not conflict with the CC conformance claim to the [18].

4.3. Security Objectives Rationale

157 The following table provides an overview for security objectives coverage.

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_QSCD_Auth	OT.TOE_TC_SVD_Exp	OE.CGA_Qcert	OE.SVD_Auth	OE.Dev_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory	OE.CGA_QSCD_Auth	OE.CGA_TC_SVD_Imp
T.SCD_Divulg	-	-	-	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_QSCD_Auth	OT.TOE_TC_SVD_Exp	OE.CGA_Qcert	OE.SVD_Auth	OE.Dev_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory	OE.CGA_QSCD_Auth	OE.CGA_TC_SVD_Imp
T.SCD_Derive	-	X	-	-	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
T.Hack_Phys	-	-	-	-	X	-	-	-	X	X	X	-	-	-	-	-	-	-	-	-	-	-
T.SVD_Forgery	-	-	-	X	-	-	-	-	-	-	-	-	X	-	X	-	-	-	-	-	-	X
T.SigF_Misuse	X	-	-	-	-	-	X	X	-	-	-	-	-	-	-	-	X	X	X	X	-	-
T.DTBS_Forgery	-	-	-	-	-	-	-	X	-	-	-	-	-	-	-	-	-	X	X	-	-	-
T.Sig_Forgery	-	-	X	-	-	X	-	-	-	-	-	-	-	X	-	-	-	-	-	-	-	-
P.CSP_QCert	X	-	-	X	-	-	-	-	-	-	-	X	-	X	-	-	-	-	-	-	X	-
P.QSign	-	-	-	-	-	X	X	-	-	-	-	-	-	X	-	-	-	X	-	-	-	-
P.Sigy_QSCD	X	X	X	-	X	X	X	X	X	-	X	X	X	-	-	X	-	-	-	-	X	X
P.Sig_Non-Repud	X	-	X	X	X	X	X	X	X	X	X	X	X	X	X	X	-	X	X	X	X	X
A.CGA	-	-	-	-	-	-	-	-	-	-	-	-	-	X	X	-	-	-	-	-	-	-
A.SCA	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	X	-	-	-	-

6. Table Mapping of security problem definition to security objectives

4.4. Security Objectives Sufficiency

Countering of threats by security objectives

158 **T.SCD_Divulg (***Storing, copying, and releasing of the signature-creation data***)** addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in recital (18) of **the Directive**. This threat is countered by OT.SCD_Secrecy, which assures the secrecy of the SCD used for signature creation.

159 **T.SCD_Derive (***Derive the signature creation data***)** deals with attacks on the SCD via public known data produced by the TOE, which are the SVD and the signatures created with the SCD. OT.SCD/SVD_Auth_Gen counters this threat by implementing cryptographically secure generation of the SCD/SVD-pair. OT.Sig_Secure ensures cryptographically secure electronic signatures.

160 **T.Hack_Phys (***Exploitation of physical vulnerabilities***)** deals with physical attacks exploiting physical vulnerabilities of the TOE. OT.SCD_Secrecy preserves the secrecy of the SCD. OT.EMSEC_Design counters physical attacks through the TOE interfaces and observation of TOE emanations. OT.Tamper_ID and OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tampering attacks.

161 **T.SVD_Forgery** (*Forgery of the signature verification data*) deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate. T.SVD_Forgery is addressed by OT.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature

creation with the SCD, and OE.SVD_Auth that ensures the integrity of the SVD exported by the TOE to the CGA and verification of the correspondence between the SCD in the QSCD of the signatory and the SVD in the input it provides to the certificate generation function of the CSP. Additionally T.SVD_Forgery is addressed by OT.TOE_TC_SVD_Exp, which ensures that the TOE sends the SVD in a verifiable form through a trusted channel to the CGA, as well as by OE.CGA_TC_SVD_Imp, which provides verification of SVD authenticity by the CGA.

162 **T.SigF_Misuse** (*Misuse of the signature creation function of the TOE*) addresses the threat of misuse of the TOE signature creation function to create SDO by others than the signatory to create an electronic signature on data for which the signatory has not expressed the intent to sign, as required by paragraph 1(c) of Annex III. OT.Lifecycle_Security (Lifecycle security) requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure destruction of the SCD, which may be initiated by the signatory. OT.Sigy_SigF (Signature creation function for the legitimate signatory only) ensures that the TOE provides the signature creation function for the legitimate signatory only. OE.DTBS_Intend (Data intended to be signed) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign and OE.DTBS_Protect counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE. OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. If the SCA provides a human interface for user authentication, OE.HID_VAD (Protection of the VAD) provides confidentiality and integrity of the VAD as needed by the authentication method employed. OE.Signatory ensures that the signatory checks that an SCD stored in the QSCD when received from an QSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the signatory becomes control over the QSCD. OE.Signatory ensures also that the signatory keeps their VAD confidential.

163 **T.DTBS_Forgery (***Forgery of the DTBS/R***)** addresses the threat arising from modifications of the data sent as input to the TOE's signature creation function that does not represent the DTBS as presented to the signatory and for which the signature has expressed its intent to sign. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.DTBS_Intend, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE, and by means of OE.DTBS_Protect, which ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE. The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by ensuring the integrity of the DTBS/R inside the TOE.

164 **T.Sig_Forgery (***Forgery of the electronic signature***)** deals with non-detectable forgery of the electronic signature. OT.Sig_Secure, OT.SCD_Unique and OE.CGA_Qcert address this threat in general. OT.Sig_Secure (*Cryptographic security of the electronic signature*) ensures by means of robust cryptographic techniques that the signed data and the electronic signature are securely linked together. OT.SCD_Unique ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance. OE.CGA_Qcert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision concerning a forged signature.

Enforcement of OSPs by security objectives

165 **P.CSP_QCert** (*CSP generates qualified certificates*) provides that the TOE and the SCA may be employed to sign data with (qualified) electronic signatures, as defined by the Regulation[23], paragraph (63). Regulation [23], recital Article 29 refers to QSCDs to ensure the functionality of advanced signatures. The OE.CGA_Qcert addresses the requirement of qualified (or advanced) electronic signatures as being based on qualified (or non-qualified) certificates. According to OT.TOE_QSCD_Auth the copies of the TOE will hold unique identity and authentication data as QSCD and provide security mechanisms enabling the CGA to identify and to authenticate the TOE as QSCD to prove this identity as QSCD to the CGA. The OE.CGA_QSCD_Auth ensures that the CSP checks the proof of the device presented of the applicant that it is a QSCD. The OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE to the CGA corresponds to the SCD stored in the TOE and used

by the signatory. The OT.Lifecycle_Security ensures that the TOE detects flaws during the initialisation, personalisation and operational usage.

166 **P.QSign (***Qualified electronic signatures***)** provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate. OT.Sigy_SigF ensures signatory's sole control of the SCD by requiring the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others. OT.Sig_Secure ensures that the TOE creates electronic signatures, which cannot be forged without knowledge of the SCD through robust encryption techniques. OE.CGA_Qcert addresses the requirement of qualified or non-qualified electronic certificates building a base for the electronic signature. OE.DTBS_Intend ensures that the SCA provides only those DTBS to the TOE, which the signatory intends to sign.

167 **P.Sigy_QSCD** (*TOE as Qualified signature creation device*) requires the TOE to meet Annex III of the regulation. The paragraph 1(a) of Annex III is ensured by OT.SCD_Unique requiring that the SCD used for signature creation can practically occurs only once. The OT.SCD_Secrecy OT.Sig_Secure and OT.EMSEC_Design and OT.Tamper_Resistance address the secrecy of the SCD (cf. paragraph 1(a) of Annex III). OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(b) of Annex III by the requirements to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE. OT.Sigy_SigF meets the requirement in paragraph 1(c) of Annex III by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others. OT.DTBS_Integrity_TOE meets the requirements in paragraph 2 of Annex III as the TOE must not alter the DTBS/R. The usage of SCD under sole control of the signatory is ensured by OT.Lifecycle_Security, OT.SCD/SVD_Auth_Gen and OT.Sigy_SigF.

168 **OE.Dev_Prov_Service** (*Authentic QSCD provided by QSCD Provisioning Service*) ensures that the legitimate user obtains a TOE sample as an authentic, initialised and personalised TOE from an QSCD Provisioning Service through the TOE delivery procedure. If the TOE implements SCD generated under control of the QSCD Provisioning Service the legitimate user receives the TOE as QSCD. If the TOE is delivered to the legitimate user without SCD in the operational phase he or she applies for the (qualified) certificate as the Device holder and legitimate user of the TOE. The CSP will use the TOE security feature (addressed by the security objectives OT.TOE_QSCD_Auth and OT.TOE_TC_SVD_Exp to check whether the device presented is a QSCD linked to the applicant as required by OE.CGA_QSCD_Auth and the received SVD is sent by this QSCD as required by OE.CGA_TC_SVD_Imp. Thus, the obligation of the QSCD provision service for the first SCD/SVD pair is complemented in an appropriate way by the CSP for the SCD/SVD pair generated outside the secure preparation environment.

169 **P.Sig_Non-Repud (***Non-repudiation of signatures***)** deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in their certificate valid at the time of signature creation. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, that ensure the aspects of signatory's sole control over and responsibility for the electronic signatures generated with the TOE.

170 **OE.Dev_Prov_Service** ensures that the signatory uses an authentic TOE, initialised and personalised for the signatory. OE.CGA_Qcert ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory.

171 **OE.SVD_Auth** and **OE.CGA_Qcert** require the environment to ensure authenticity of the SVD as being exported by the TOE and used under sole control of the signatory. OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE. OT.SCD_Unique provides that the signatory's SCD can practically occur just once.

172 **OE.Signatory** ensures that the signatory checks that the SCD, stored in the QSCD received from an QSCD provisioning service is in non-operational state (i.e. the SCD cannot be used

before the signatory becomes into sole control over the QSCD). The TOE security feature addressed by the security objectives OT.TOE_QSCD_Auth and OT.TOE_TC_SVD_Exp supported by OE.Dev_Prov_Service enables the verification whether the device presented by the applicant is a QSCD as required by OE.CGA_QSCD_Auth and the received SVD is sent by the device holding the corresponding SCD as required by OE.CGA_TC_SVD_Imp. OT.Sigy_SigF provides that only the signatory may use the TOE for signature creation. As prerequisite OE.Signatory ensures that the signatory keeps their VAD confidential. OE.DTBS_Intend, OE.DTBS_Protect and OT.DTBS_Integrity_TOE ensure that the TOE generates electronic signatures only for a DTBS/R that the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig_Secure ensure that only this SCD may generate a valid electronic signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE OT.Lifecycle_Security (Lifecycle security), OT.SCD_Secrecy (Secrecy of the signature creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection) and OT.Tamper_Resistance (Tamper resistance) protect the SCD against any compromise.

Upkeep of assumptions by security objectives

173 **A.SCA (***Trustworthy signature creation application***)** establishes the trustworthiness of the SCA with respect to generation of DTBS/R. This is addressed by OE.DTBS_Intend *(Data intended to be signed*) which ensures that the SCA generates the DTBS/R of the data that have been presented to the signatory as DTBS and which the signatory intends to sign in a form which is appropriate for being signed by the TOE.

174 **A.CGA (***Trustworthy certification generation application***)** establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by OE.CGA_Qcert *(Generation of qualified certificates*), which ensures the generation of qualified certificates, and by OE.SVD_Auth (*Authenticity of the SVD*), which ensures the protection of the integrity of the received SVD and the verification of the correspondence between the SVD and the SCD that is implemented by the QSCD of the signatory.

5. Extended Component Definition

175 The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation. The definition of the family FPT_EMS is taken from the *Protection Profile Secure Signature Creation Device [18]*.

176 The additional family FIA_API (a sensitive family of the Class FIA (Identification and authentication). This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity. The definition of the family FIA_API is taken from the *Protection Profile Secure Signature Creation Device* [19].

FPT_EMS TOE Emanation

177 Family behaviour: This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMS TOE Emanation — 1

178 FPT_EMS.1 TOE Emanation has two constituents:
FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
FPT_EMS.1.2 Interface Emanation requires not emit interface emanation enabling access to TSF data or user data.

179 Management: FPT_EMS.1 There are no management activities foreseen.

180 Audit: FPT_EMS.1 There are no actions identified that must be auditable if **FAU_GEN** (*Security audit data generation*) is included in a protection profile or security target.

181 **FPT_EMS.1** *TOE Emanation*

Hierarchical to: No other components

Dependencies: No dependencies.

182 FPT_EMS.1.1

The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

183 FPT_EMS.1.2

The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

FIA_API Authentication Proof of Identity

184 Family behaviour: This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.

Component levelling:

FIA_API Authentication Proof of Identity	—	1

185 FIA_API.1 Authentication Proof of Identity.

186 Management: FIA_API.1 The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

187 Audit: There are no actions defined to be auditable.

188 **FIA_API.1** *Authentication Proof of Identity*

Hierarchical to: No other components

Dependencies: No dependencies.

189 FIA_API.1.1

The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: authorized user or role].

6. Security Requirements

6.1. TOE Security Functional Requirements

6.1.1. Use of requirement specifications

190 Common Criteria allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration.* Each of these operations is used in this ST and the underlying PP. The footnotes in this ST indicate the operations of the PP and the ST as well.

191 A **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is either (i) denoted by the word "refinement" in **bold** text and the added or changed words are in bold text, or (ii) included in text as **bold** text and marked by a footnote. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

192 A **selection** operation is used to select one or more options provided by the CC or the underlying PP in stating a requirement. A selection that has been made is indicated as underlined text and the original text of the component is given by a footnote.

193 An **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment that that has been made is indicated as double underlined text and the original text of the component is given by a footnote.

194 An **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

6.1.2. Cryptographic support (FCS)

195 **8. Application note (taken from application note 4 from [18])**

Applied.

FCS_CKM.1

Cryptographic key generation (from [18])

196 Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

197 FCS_CKM.1.1

The TSF shall generate an **SCD/SVD** pair in accordance with a specified cryptographic key generation algorithm RSA or ECDSA[6] and specified cryptographic key sizes 1024-4096 or 160-521 bits[7] or that meet the following: [7][8]

198 **9. Application note (taken from application note 5 from [18])**

Applied.

199 **10. Application note (from the ST author)**

The underlying Platform supports RSA, RSA-CRT and ECDSA generation algorithms and cryptographic key sizes 1024 bits to 4096 (RSA) and 160 bits to 521 bits (ECDSA) with equal security measures. However, to fend off attackers with high attack potential an adequate key length must be used.

---

[6] [assignment: *cryptographic key generation algorithm*]
[7] [assignment*: cryptographic key sizes*]
[8] [assignment*: list of standards*]

FCS_CKM.4

Cryptographic key destruction (from [18])

200 Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

201 FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physically overwriting the keys in a randomized manner[9] that meets the following: none.[10]

202 **11. Application note (taken from application note 6 from [18])**

Applied.

FCS_COP.1

Cryptographic operation (from [18])

203 Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

204 FCS_COP.1.1

The TSF shall perform digital signature creation[11] in accordance with a specified cryptographic algorithm RSA according to RSASSA-PKCS1-v1_5, RSASSA-PSS with key sizes 2048-4096 bits or ECDSA according to ISO14883-3 with key sizes 160-521[12,13] that meet the following: [24][27][14].

205 **12. Application note (taken from application note 7 from [18])**

Applied.

206 **13. Application note (from the ST author)**

The underlying Platform supports RSA, RSA-CRT and ECDSA digital signature algorithms and cryptographic key sizes 2048 bits to 4096 bits (RSA) and 160 bits to 521 bits (ECDSA) with equal security measures. However, to fend off attackers with high attack potential an adequate key length must be used.

6.1.3. User data protection (FDP)

207 The security attributes and related status for the subjects and objects are:

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin – S.User acts as S.Admin R.Sigy – S.User acts as S.Sigy

[9] [assignment: *cryptographic key destruction method*]
[10] [assignment: *list of standards*]
[11] [assignment: list of cryptographic operations]
[12] [assignment: *cryptographic algorithm*]
[13] [assignment: *cryptographic key sizes*]
[14] [assignment: *list of standards*]

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	SCD/SVD Management	authorized, not authorized
SCD	SCD Operational	no, yes
SCD	SCD Identifier	arbitrary value
SVD	(This ST does not define security attributes for SVD)	(This ST does not define security attributes for SVD)

7. Table Subjects and security attributes for access control

208 **14. Application note (taken from application note 8 from [18])**

Applied.

FDP_ACC.1/Signature_Creation

Subset access control (from [18])

209 Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

210 FDP_ACC.1.1/Signature_Creation

The TSF shall enforce the Signature Creation SFP[15] on

(1) subjects: S.User,

(2) objects: DTBS/R, SCD,

(3) operations: signature creation.[16]

FDP_ACC.1/SCD/SVD_Generation

Subset access control (from [18])

211 Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

212 FDP_ACC.1.1/SCD/SVD_Generation

The TSF shall enforce the SCD/SVD_Generation_SFP[17] on

(1) subjects: S.User,

(2) objects: SCD, SVD,

(3) operations: generation of SCD/SVD pair[18]

FDP_ACF.1/SCD/SVD_Generation

Security attribute based access control (from [18])

213 Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

[15] [assignment: *access control SFP*]
[16] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[17] [assignment: *access control SFP*]
[18] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

214 FDP_ACF.1.1/SCD/SVD_Generation

The TSF shall enforce the SCD/SVD_Generation_SFP[19] to objects based on the following: the user S.User is associated with the security attribute "SCD/SVD Management"[20].

215 FDP_ACF.1.2/SCD/SVD_Generation_SFP

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 "SCD / SVD Management" set to "authorized" is allowed to generate SCD/SVD pair[21]

216 FDP_ACF.1.3/SCD/SVD_Generation

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[22].

217 FDP_ACF.1.4/ SCD/SVD_Generation

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

S.User with the security attribute "SCD / SVD management" set to "not authorized" is not allowed to generate SCD/SVD pair[23].

FDP_ACC.1/SVD_Transfer

Subset access control (from [21])

218 Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

219 FDP_ACC.1.1/SVD_Transfer

The TSF shall enforce the SVD_Transfer_SFP[24] on

(1) subjects: S.User,

(2) objects: SVD

(3) operations: export[25].

FDP_ACF.1/SVD_Transfer

Security attribute based access control (from [18])

220 Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

221 FDP_ACF.1.1/SVD_Transfer

[19] [assignment: *access control SFP*]
[20] [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*]
[21] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[22] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
[23] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[24] [assignment: *access control SFP*]
[25] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

The TSF shall enforce the SVD_Transfer_SFP[26] to objects based on the following:

(1) the S.User is associated with the security attribute Role,

(2) the SVD[27].

222 FDP_ACF.1.2/SVD_Transfer

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: R.Admin[28] is allowed to export SVD[29].

223 FDP_ACF.1.3/SVD_Transfer

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[30].

224 FDP_ACF.1.4/SVD_Transfer

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[31].

225 **15. Application note (taken from application note 9 from [18])**

Applied.

FDP_ACF.1/Signature creation

Security attribute based access control (from [18])

226 Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

227 FDP_ACF.1.1/Signature_creation

The TSF shall enforce the Signature creation_SFP[32] to objects based on the following:

(1) the user S.User is associated with the security attribute "Role" and

(2) the SCD with the security attribute "SCD Operational"[33].

228 FDP_ACF.1.2/Signature_creation

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

R.Sigy is allowed to create digital signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "yes"[34].

229 FDP_ACF.1.3/Signature_creation

---

26 [assignment: *access control SFP*]

27 [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*]

28 [selection: R.Admin, R.Sigy]

29 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]].

30 [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]

31 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

32 [assignment: *access control SFP*]

33 [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*]

34 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[35].

230 FDP_ACF.1.4/Signature_creation

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

S.User is not allowed to create digital signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no"[36].

FDP_DAU.2/SVD

Data Authentication with Identity of Guarantor (from [19])

231 Hierarchical to: FDP_DAU.1 Basic Data Authentication

Dependencies: FIA_UID.1 Timing of identification

232 FDP_DAU.2.1/SVD

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of SVD[37].

233 FDP_DAU.2.2/SVD

The TSF shall provide CGA[38] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

16. Application note (from the ST author)

The TOE supports Certificate Request Signature (CRS) to provide evidence about the validity of the SVD for the CGA. CRS also proves that the SVD belongs to the TOE.

FDP_RIP.1

Subset residual information protection (from [18])

234 Hierarchical to: No other components.

Dependencies: No dependencies.

235 FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the **overwrite or** deallocation of the resource from[39] the following objects: SCD[40].

236 **17. Application note (from the ST author)**

The TOE overwrites the previous SCD in case a new key pair generation.

237 The following data persistently stored by the TOE shall have the user data attribute "integrity checked persistent stored data":

1. SCD
2. SVD (if persistently stored by the TOE).

---

[35] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
[36] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[37] [assignment: list of objects or information types]
[38] [assignment: list of subjects]
[39] [selection: *allocation of the resource to, deallocation of the resource from*]
[40] [assignment: *list of objects*]

238 The DTBS/R temporarily stored by the TOE has the user data attribute "integrity checked stored data":

FDP_SDI.2/Persistent

Stored data integrity monitoring and action (from [18])

239 Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies

240 FDP_SDI.2.1/Persistent

The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[41] on all objects, based on the following attributes: integrity checked stored data[42].

241 FDP_SDI.2.2/Persistent

Upon detection of a data integrity error, the TSF shall

(1) prohibit the use of the altered data

(2) inform the S.Sigy about integrity error[43].

FDP_SDI.2/DTBS

Stored data integrity monitoring and action (from [18])

242 Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

243 FDP_SDI.2.1/DTBS

The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[44] on all objects, based on the following attributes: integrity checked stored DTBS[45].

244 FDP_SDI.2.2/DTBS

Upon detection of a data integrity error, the TSF shall

(1) prohibit the use of the altered data

(2) inform the S.Sigy about integrity error[46].

245 **18. Application note (taken from application note 10 from [18])**

Applied.

246 **19. Application note (from the ST author)**

There is no stored DTBS in the TOE, because the card only receives and immediately signs hash (DTBS/R), not the DTBS.

---

41 [assignment: *integrity errors*]
42 [assignment: *user data attributes*]
43 [assignment: *action to be taken*]
44 [assignment: *integrity errors*]
45 [assignment: *user data attributes*]
46 [assignment: *action to be taken*]

6.1.4. Identification and authentication (FIA)

FIA_UID.1

Timing of identification (from [18])

247 Hierarchical to: No other components.

Dependencies: No dependencies.

248 FIA_UID.1.1

The TSF shall allow

(1) Self-test according to FPT_TST.1,

(2) none[47][48]

on behalf of the user to be performed before the user is identified.

249 FIA_UID.1.2

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

250 **20. Application note (taken from application note 11 from [18])**

Applied.

FIA_UAU.1

Timing of authentication (from [19])

251 Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

252 FIA_UAU.1.1

The TSF shall allow

(1) self-test according to FPT_TST.1,

(2) identification of the user by means of TSF required by FIA_UID.1,

(3) establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD, [49][50]

(4) none[51][52]

on behalf of the user to be performed before the user is authenticated.

253 FIA_UAU.1.2

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

254 **21. Application note (taken from application note 1 from [19])**

Applied.

---

[47] [assignment: *list of TSF-mediated actions*]
[48] [assignment: *list of additional TSF-mediated actions]*
[49] [assignment: *list of TSF-mediated actions*]
[50] [assignment: *list of additional TSF-mediated actions]*
[51] [assignment: *list of TSF-mediated actions*]
[52] [assignment: *list of additional TSF-mediated actions]*

FIA_API.1

Authentication Proof of Identity (from [19])

255 Hierarchical to: No other components.

Dependencies: No dependencies

256 FIA_API.1.1

The TSF shall provide a symmetric or asymmetric authentication mechanism[53] to prove the identity of the QSCD[54]

257 **22. Application note (taken from application note 2 from [19])**

Applied.

258 **23. Application note (from ST author)**

The IDentity Applet supports several kind of symmetric or asymmetric authentication mechanisms, which compliance with the followings:[21][22][26] In addition IDentity Applet supports Certificate Request Signature, which implements a high secure way to prove the identity and authenticity of the QSCD based on PKI, in addition proves the correspondence between SCD/SVD key pair in authentic way.

The authentication mechanism is depended on the configured Application Profile.

FIA_AFL.1

Authentication failure handling (from [18])

259 Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

260 FIA_AFL.1.1

The TSF shall detect when an administrator configurable positive integer within 3-15[55] [56], unsuccessful authentication attempts occur related to consecutive failed authentication attempts[57]

261 FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met[58], the TSF shall block RAD[59]

262 **24. Application note (taken from application note 13 from [18])**

Applied.

263 **25. Application note (from ST Author)**

The PUK (personal unlocking key) is an optional security function of IDentity Applet, which meet the requirements of FIA_AFL.1.1 and FIA_AFL.1.2 as described is current ST.

[53] [assignment: *authentication mechanism*]
[54] [assignment: *authorized user or rule]*
[55] [assignment: positive integer number]
[56] [selection: [assignment: positive integer number] an administrator configurable positive integer within [assignment: range of acceptable values]]
[57] [assignment: list of authentication events]
[58] [selection: met,surpassed]
[59] [assignment: list of actions]

6.1.5. Security management (FMT)

FMT_SMR.1

Security roles (from [18])

264 Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

265 FMT_SMR.1.1

The TSF shall maintain the roles R.Admin and R.Sigy[60].

266 FMT_SMR.1.2

The TSF shall be able to associate users with roles.

FMT_SMF.1

Specification of management functions (from [18])

267 Hierarchical to: No other components.

Dependencies: No dependencies

268 FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:

(1) Creation and modification of RAD,

(2) Enabling the signature-creation function,

(3) Modification of the security attribute SCD/SVD management, SCD operational,

(4) Change the default value of the security attribute SCD Identifier,

(5) Unblock the RAD[61][62].

269 **26. Application note (taken from application note 14 from [18])**

Applied.

FMT_MOF.1

Management of security functions behaviour (from [18])

270 Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions.

271 FMT_MOF.1.1

The TSF shall restrict the ability to enable[63] the functions signature-creation function[64] to R.Sigy[65].

[60] [assignment: the authorized identified roles]
[61] [assignment: *list of security management functions to be provided by the TSF*]
[62] [assignment: *list of other security management functions to be provided by the TSF*]
[63] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
[64] [assignment: *list of functions*]
[65] [assignment: *the authorized identified roles*]

FMT_MSA.1/Admin

Management of security attributes (from [18])

272 Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

273 FMT_MSA.1.1/Admin

The TSF shall enforce the SCD/SVD_Generation_SFP[66] to restrict the ability to modify, none[67] the security attributes SCD / SVD management[68] to R.Admin[69].

FMT_MSA.1/Signatory

Management of security attributes (from [18])

274 Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

275 FMT_MSA.1.1/Signatory

The TSF shall enforce the Signature-creation_SFP[70] to restrict the ability to modify[71] the security attributes SCD operational[72] to R.Sigy[73].

FMT_MSA.2

Secure security attributes (from [18])

276 Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

277 FMT_MSA.2.1

The TSF shall ensure that only secure values are accepted for SCD / SVD Management and SCD operational[74].

278 **27. Application note (taken from application note 15 from [18])**

Applied.

[66] [assignment: *access control SFP(s), information flow control SFP(s)*]
[67] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[68] [assignment: *list of security attributes*]
[69] [assignment: *the authorized identified roles*]
[70] [assignment: *access control SFP(s), information flow control SFP(s)*]
[71] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[72] [assignment: *list of security attributes*]
[73] [assignment: *the authorized identified roles*]
[74] [assignment: *list of security attributes*]

FMT_MSA.3

Static attribute initialization (from [18])

279 Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

280 FMT_MSA.3.1

The TSF shall enforce the SCD/SVD_Generation_SFP, SVD_Transfer_SFP and Signature-creation_SFP[75]to provide restrictive[76] default values for security attributes that are used to enforce the SFP.

281 FMT_MSA.3.2

The TSF shall allow the R.Admin[77] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.4

Security attribute value inheritance (from [18])

282 Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

283 FMT_MSA.4.1

The TSF shall use the following rules to set the value of security attributes:

(1) If S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute "SCD operational of the SCD" shall be set to "no" as a single operation.

(2) If S.Sigy successfully generates an SCD/SVD pair the security attribute "SCD operational of the SCD" shall be set to "yes" as a single operation.[78]

284 **28. Application note (taken from application note 16 from [18])**

Applied.

FMT_MTD.1/Admin

Management of TSF data (from [18])

285 Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

286 FMT_MTD.1.1/Admin

The TSF shall restrict the ability to create[79] the RAD[80] to R.Admin[81].

---

75 [assignment: *access control SFP, information flow control SFP*]
76 [selection, choose one of: *restrictive, permissive, [assignment: other property]*]
77 [assignment: the authorized identified roles
78 [assignment: *rules for setting the values of security attributes*]
79 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
80 [assignment: *list of TSF data*]
81 [assignment: *the authorized identified roles*]

FMT_MTD.1/Signatory

Management of TSF data (from [18])

287 Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

288 FMT_MTD.1.1/Signatory

The TSF shall restrict the ability to modify, none[82][83] the RAD[84] to R.Sigy[85].

289 **29. Application note (taken from application note 17 from [18])**

Applied.

6.1.6. Protection of the TSF (FPT)

FPT_EMS.1

TOE Emanation (from [18])

290 Hierarchical to: No other components.

Dependencies: No dependencies.

291 FPT_EMS.1.1

The TOE shall not emit variations in power consumption or timing during command execution[86] in excess of non-useful information[87] enabling access to RAD[88] and SCD[89].

292 FPT_EMS.1.2

The TSF shall ensure that unauthorized users[90] are unable to use the following interface electrical contacts[91] to gain access to RAD[92] and SCD[93].

293 **30. Application note (taken from application note 18 from [18])**

Applied.

FPT_FLS.1

Failure with preservation of secure state (from [18])

294 Hierarchical to: No other components.

Dependencies: No dependencies.

295 FPT_FLS.1.1

---

82 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
83 [assignment: other operations]
84 [assignment: *list of TSF data*]
85 [assignment: *the authorized identified roles*]
86 [assignment: *types of emissions*]
87 [assignment: specified limits]
88 [assignment*: list of types of TSF data*]
89 [assignment*: list of types of user data*]
90 [assignment: type of users]
91 [assignment: type of connection]
92 [assignment*: list of types of TSF data*]
93 [assignment*: list of types of user data*]

The TSF shall preserve a secure state when the following types of failures occur:

(1) self-test according to FPT_TST fails,

(2) none[94].

296 **31. Application note (taken from application note 19 from [18])**

Applied.

FPT_PHP.1

Passive detection of physical attack (from [18])

297 Hierarchical to: No other components.

Dependencies: No dependencies

298 FPT_PHP.1.1

The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

299 FPT_PHP.1.2

The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.3

Resistance to physical attack (from [18])

300 Hierarchical to: No other components.

Dependencies: No dependencies

301 FPT_PHP.3.1

The TSF shall resist physical manipulation and physical probing [95] to the TSF[96]by responding automatically such that the SFRs are always enforced.

302 **32. Application note (taken from application note 20 from [18])**

Applied.

FPT_TST.1

TSF testing (from [18])

303 Hierarchical to: No other components.

Dependencies: No dependencies

304 FPT_TST.1.1

The TSF shall run a suite of self-tests during initial start-up, periodically during normal operation [97] to demonstrate the correct operation of the TSF[98]

---

[94] [assignment*: list of types of failures in the TSF*]
[95] [assignment: physical tampering scenarios]
[96] [assignment: *list of TSF devices/elements*]
[97] [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions[assignment: conditions under which self-test should occur]]
[98] [selection: *[assignment: parts of TSF], the TSF*]

305 FPT_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of TSF data[99].

306 FPT_TST.1.3

The TSF shall provide authorized users with the capability to verify the integrity of TSF[100]

307 **33. Application note (taken from application note 21 from [18]**

Applied.

6.1.7. Trusted path/Channels (FTP)

FTP_ITC.1/SVD

Inter-TSF trusted channel – CGA (from [19])

308 Hierarchical to: No other components

Dependencies: No dependencies

309 FTP_ITC.1.1/SVD

The TSF shall provide a communication channel between itself and another trusted IT product **CGA** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

310 FTP_ITC.1.2/SVD

The TSF shall permit another trusted IT product[101] to initiate communication via the trusted channel.

311 FTP_ITC.1.3/SVD

The TSF **or the CGA** shall initiate communication via the trusted channel for

1. data Authentication with Identity of Guarantor according to FIA_API.1 and FDP_DAU.2/SVD.
2. none[102][103]

312 **34. Application note (taken from application note 3 and 4 from [19])**

Applied

313 **35. Application note (from ST author)**

The TOE supports to receive DTBS and RAD via trusted channel between the TOE and a terminal.

The above-mentioned functions are not certified in current ST.

[99] [selection: *[assignment: parts of TSF data], TSF data*]
[100] [selection: *[assignment: parts of TSF], TSF*]
[101] [selection: *the TSF, another trusted IT product*]
[102] [assignment: list of functions for which a trusted channel is required]
[103] [assignment: list of other functions for which a trusted channel is required]

6.2. TOE Security Assurance Requirements

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Architectural Design with domain separation and non-bypassability
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

8. Table Security Assurance Requirements: EAL4 augmented with AVA_VAN.5

6.3. Security Requirements Rationale

6.3.1. Security Requirement Coverage

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_QSCD_Auth	OT.TOE_TC_SVD_Exp
FCS_CKM.1	X	-	X	X	X	-	-	-	-	-	-	-	-
FCS_CKM.4	X	-	-	-	X	-	-	-	-	-	-	-	-
FCS_COP.1	X	-	-	-	-	X	-	-	-	-	-	-	-

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_QSCD_Auth	OT.TOE_TC_SVD_Exp
FDP_ACC.1/SCD/SVD_Generation	X	X	-	-	-	-	-	-	-	-	-	-	-
FDP_ACC.1/SVD_Transfer	X	-	-	-	-	-	-	-	-	-	-	-	X
FDP_ACC.1/Signature_Creation	X	-	-	-	-	-	X	-	-	-	-	-	-
FDP_ACF.1/SCD/SVD_Generation	X	X	-	-	-	-	-	-	-	-	-	-	-
FDP_ACF.1/SVD_Transfer	X	-	-	-	-	-	-	-	-	-	-	-	X
FDP_ACF.1/Signature creation	X	-	-	-	-	-	X	-	-	-	-	-	-
FDP_DAU.2/SVD	-	-	-	-	-	-	-	-	-	-	-	-	X
FDP_RIP.1	-	-	-	-	X	-	X	-	-	-	-	-	-
FDP_SDI.2/Persistent	-	-	-	X	X	X	-	-	-	-	-	-	-
FDP_SDI.2/DTBS	-	-	-	-	-	-	X	X	-	-	-	-	-
FIA_AFL.1	-	-	-	-	-	-	X	-	-	-	-	-	-
FIA_UAU.1	-	X	-	-	-	-	X	-	-	-	-	X	
FIA_API.1	-	-	-	-	-	-	-	-	-	-	-	X	-
FIA_UID.1	-	X	-	-	-	-	X	-	-	-	-	-	-
FMT_MOF.1	X	-	-	-	-	-	X	-	-	-	-	-	-
FMT_MSA.1/Admin	X	X	-	-	-	-	-	-	-	-	-	-	-
FMT_MSA.1/Signatory	X		-	-	-	-	X	-	-	-	-	-	-
FMT_MSA.2	X	X	-	-	-	-	X	-	-	-	-	-	-
FMT_MSA.3	X	X	-	-	-	-	X	-	-	-	-	-	-
FMT_MSA.4	X	X	-	X	-	-	X	-	-	-	-	-	-
FMT_MTD.1/Admin	X	-	-	-	-	-	X	-	-	-	-	-	-
FMT_MTD.1/Signatory	X	-	-	-	-	-	X	-	-	-	-	-	-
FMT_SMR.1	X	-	-	-	-	-	X	-	-	-	-	-	-
FMT_SMF.1	X	-	-	X	-	-	X	-	-	-	-	-	-
FPT_EMS.1	-	-	-	-	X	-	-	-	X	-	-	-	-
FPT_FLS.1	-	-	-	-	X	-	-	-	-	-	-	-	-
FPT_PHP.1	-	-	-	-	-	-	-	-	-	X	-	-	-
FPT_PHP.3	-	-	-	-	X	-	-	-	-	-	X	-	-
FPT_TST.1	X	-	-	-	X	X	-	-	-	-	-	-	-
FTP_ITC.1/SVD	-	-	-	-	-	-	-	-	-	-	-	-	X

9. Table Mapping of functional requirements to security objectives for the TOE

6.3.2. TOE Security Requirements Sufficiency

314 **OT.Lifecycle_Security** (*Lifecycle security*) is provided by the SFR for SCD/SVD generation FCS_CKM.1, SCD usage FCS_COP.1 and SCD destruction FCS_CKM.4 ensure cryptographically secure lifecycle of the SCD. The SCD/SVD generation is controlled by TSF according to FDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation. The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer. The SCD usage is ensured by access control FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_creation which is based on the security attribute secure TSF management according to FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FMT_SMF.1 and FMT_SMR.1. The test functions FPT_TST.1 provides failure detection throughout the lifecycle.

315 **OT.SCD/SVD_Auth_Gen (Authorized SCD/SVD generation)** addresses that generation of a SCD/SVD pair requires proper user authentication. The TSF specified by FIA_UID.1 and FIA_UAU.1 provide user identification and user authentication prior to enabling access to authorized functions. The SFR FDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation provide access control for the SCD/SVD generation. The security attributes of the authenticated user are provided by FMT_MSA.1/Admin, FMT_MSA.2, and FMT_MSA.3 for static attribute initialization. The SFR FMT_MSA.4 defines rules for inheritance of the security attribute “SCD operational” of the SCD.

316 OT.SCD_Unique (Uniqueness of the signature-creation data) implements the requirement of practically unique SCD as laid down in Annex III, paragraph 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1.

317 **OT.SCD_SVD_Corresp** (*Correspondence between SVD and SCD*) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1 to generate corresponding SVD/SCD pairs. The security functions specified by FDP_SDI.2/Persistent ensure that the keys are not modified, so to retain the correspondence. Moreover, the SCD Identifier allows the environment to identify the SCD and to link it with the appropriate SVD. The management functions identified by FMT_SMF.1 and by FMT_MSA.4 allow R.Admin to modify the default value of the security attribute SCD Identifier.

318 **OT.SCD_Secrecy** (*Secrecy of signature-creation data*) is provided by the security functions specified by the following SFR. FCS_CKM.1 ensures the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD. The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information.

319 The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_TST.1 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA).

320 SFR FPT_EMS.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

321 **OT.Sig_Secure** (*Cryptographic security of the digital signature*) is provided by the cryptographic algorithms specified by FCS_COP.1, which ensures the cryptographic robustness of the signature algorithms. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE and FPT_TST.1 ensure self-tests ensuring correct signature-creation.

322 **OT.Sigy_SigF** (*Signature creation function for the legitimate signatory only*) is provided by an SFR for identification authentication and access control.

323 FIA_UAU.1 and FIA_UID.1 ensure that no signature generation function can be invoked before the signatory is identified and authenticated. The security functions specified by FMT_MTD.1/Admin and FMT_MTD.1/Signatory manage the authentication function. SFR FIA_AFL.1 provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by FDP_SDI.2/DTBS ensures the integrity of stored DTBS and FDP_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature-creation process).

324 The security functions specified by FDP_ACC.1/Signature_Creation and FDP_ACF.1/Signature_creation provide access control based on the security attributes managed according to the SFR FMT_MTD.1/Signatory, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4. The SFR FMT_SMF.1 and FMT_SMR.1 list these management functions and the roles. These ensure that the signature process is restricted to the signatory. FMT_MOF.1 restricts the ability to enable the signature-creation function to the signatory. FMT_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory.

325 **OT.DTBS_Integrity_TOE** (*DTBS/R integrity inside the TOE*) ensures that the DTBS/R is not altered by the TOE. The integrity functions specified by FDP_SDI.2/DTBS require that the DTBS/R has not been altered by the TOE.

326 **OT.EMSEC_Design** (*Provide physical emanations security*) covers that no intelligible information is emanated. This is provided by FPT_EMS.1.

327 **OT.Tamper_ID** (*Tamper detection*) is provided by FPT_PHP.1 by the means of passive detection of physical attacks.

328 **OT.Tamper_Resistance** (*Tamper resistance*) is provided by FPT_PHP.3 to resist physical attacks.

329 **OT.TOE_QSCD_Auth** (*Authentication proof as QSCD*) requires the TOE to provide security mechanisms to identify and to authenticate themselves as QSCD, which is directly provided by FIA_API.1 (Authentication Proof of Identity). The SFR FIA_UAU.1 allows (additionally to the [18]) establishment of the trusted channel before (human) user is authenticated.

330 **OT.TOE_TC_SVD_Exp** (TOE trusted channel for SVD export) requires the TOE to provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA, which is directly provided by

- The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer.
- FDP_DAU.2/SVD (Data Authentication with Identity of Guarantor), which requires the TOE to provide CGA with the ability to verify evidence of the validity of the SVD and the identity of the user that generated the evidence.
- FTP_ITC.1/SVD Inter-TSF trusted channel), which requires the TOE to provide a trusted channel to the CGA.

6.4. Satisfaction of dependencies of security requirements

331 The following table provides an overview how the dependencies of the security functional requirements are solved and a justification why some dependencies are not being satisfied.

Functional requirement	Dependencies	Satisfied by
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.4]	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FDP_ACC.1/SCD/SVD_Generation	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation
FDP_ACC.1/Signature_Creation	FDP_ACF.1	FDP_ACF.1/Signature creation
FDP_ACC.1/SVD_Transfer	FDP_ACF.1	FDP_ACF.1/SVD_Transfer
FDP_ACF.1/SCD/SVD_Generation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generation, FMT_MSA.3
FDP_ACF.1/Signature_Creation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature_Creation, FMT_MSA.3
FDP_ACF.1/SVD_Transfer	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer, FMT_MSA.3
FDP_DAU.2/SVD	FIA_UID1.	FIA_UID.1
FDR_RIP.1	No dependencies	n/a
FDP_SDI.2/Persistent	No dependencies	n/a
FDP_SDI.2/DTBS	No dependencies	n/a
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	No dependencies	n/a
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_API.1	No dependencies	n/a
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD/SVD_Generation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.4	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation
FMT_MTD.1/Admin	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	No dependencies	n/a
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_EMS.1	No dependencies	n/a
FPT_FLS.1	No dependencies	n/a
FPT_PHP.1	No dependencies	n/a
FPT_PHP.3	No dependencies	n/a
FPT_TST.1	No dependencies	n/a
FTP_ITC.1/SVD	No dependencies	n/a

10. Table Functional Requirements Dependencies

6.5. Rationale for chosen security assurance requirements

332 The assurance level for this protection profile is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. The TOE described in this protection profile is just such a product. Augmentation results from the selection of:

333 AVA_VAN.5 Advanced methodical vulnerability analysis

334 The following table summarize the satisfaction of dependencies of security assurance requirements.

Assurance requirement(s)	Dependencies	Satisfied by
EAL4 package	(dependencies of EAL4 package are not reproduced here)	By construction, all dependencies are satisfied in a CC EAL package
AVA_VAN.5	ADV_ARC.1,	ADV_ARC.1,
	ADV_FSP.4,	ADV_FSP.4,
	ADV_TDS.3,	ADV_TDS.3,
	ADV_IMP.1,	ADV_IMP.1,
	AGD_OPE.1,	AGD_OPE.1,
	AGD_PRE.1,	AGD_PRE.1,
	ATE_DPT.1	ATE_DPT.1
		(all are included in EAL4 package)

11. Table Satisfaction of dependencies of security assurance requirements

335 The TOE is intended to function in a variety of signature creation systems for qualified electronic signatures. Due to the nature of its intended application, i.e., the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure.

7. TOE Summary Specification

336 This chapter gives the overview description of the different TOE Security Functions composing the TSF. The mapping in-between the TSFs and SFRs can be found in 12. Table Mapping of SFRs to mechanisms of TOE

7.1. TOE Security Functions

7.1.1. TSF.AccessControl

337 This function provides the access controls to data in the file system, initialization, personalization and pre-personalization data. During earlier life phases, when the applet may not be present yet, the Platform responsible for managing the accesses correctly.

338 The TOE provides access control mechanisms that allow the maintenance of different security roles according to FMT_SMR.1 Security roles (R.Signatory and R.Administrator) and the access control policies and functions (FDP_ACC.1/Signature_Creation, FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FDP_ACC.1/SVD_Transfer, FDP_ACF.1/SVD_Transfer and FDP_ACF.1/Signature creation).

339 Administrator role (R.Admin):

The TOE restricts the ability to the followings:

- create the RAD;
- specify alternative initial values to override the default values when an object or information is created;
- to export SVD to CGA;

The TSF.AccessControl provides that the R.Admin role is only valid in Operational phase of IDentity Applet life cycle.

340 Signatory role (R.Sigy)

The TOE restricts the ability to the followings

- enable the signature-creation function;
- modify the security attributes of SCD operational;
- modify or unblock the RAD;
- create digital signature only if the security attribute “SCD operational” is set to “yes”;

The TSF.AccessControl provides that the Signatory role is only valid in Operational phase of IDentity Applet life cycle.

341 The TSF.AccessControl ensures that nobody is allowed to read all TOE intrinsic secret cryptographic keys stored in the TOE, such as RAD, SCD.

342 The access control mechanisms allow the execution of certain security relevant actions (e.g. self-tests) without successful user authentication.

343 The TSF provides functionality for the following SFRs:

- FDP_ACC.1/Signature_Creation: It is a requirement about access control and authentication, the access control is provided by TSF.AccessControl.
- FDP_ACC.1/SCD/SVD_Generation: It is a requirement about access control and authentication, the access control is provided by TSF.AccessControl.
- FDP_ACC.1/SVD_Transfer: It is a requirement about access control and authentication, the access control is provided by TSF.AccessControl.

- FDP_ACF.1/SCD/SVD_Generation: It is a requirement about access control and authentication, the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.
- FDP_ACF.1/SVD_Transfer: It is a requirement about access control and authentication, the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.
- FDP_ACF.1/Signature_creation: It is a requirement about access control and authentication, the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.
- FIA_AFL.1 The requirement is about to detect when an administrator configurable positive integer unsuccessful authentication attempts occur related to consecutive failed authentication attempts and after that block the RAD. It is provided by TSF.Authenticate and TSF.AccessControl.
- FIA_UID.1: The requirement is about identification and authentication, what shall be accessed before and after it. It is realized by TSF.AccessControl.
- FIA_UAU.1: The requirement is about authentication, and what can be accessed before and after it. It is realized by TSF.AccessControl.
- FMT_MOF.1: This SFR requires the access control to signature-creation to the signatory and is realized TSF.AccessControl. TSF.Authenticate, and TSF.SecureManagement.
- FMT_MSA.1/Admin: Requires that the SCD/SVD generation SFP to modify query the SCD/SVD management to the Administrator. It is realized by TSF.AccessControl. TSF.Authenticate, and TSF.SecureManagement.
- FMT_MSA.1/Signatory: Requires access control restrictions to modify the SCD operational security attributes to the signatory. This is realized by TSF.AccessControl. TSF.Authenticate, and TSF.SecureManagement.
- FMT_MSA.3: Requires the capability to perform authentication controls. This is realized by TSF.AccessControl, TSF.Authenticate and TSF.SecureManagement.
- FMT_MTD.1/Admin This SFR requires RAD creation to the Signatory. It is realized by TSF.AccessControl, TSF.Authenticate and TSF.SecureManagement
- FMT_MTD.1/Signatory: This SFR requires RAD modification to the Signatory. It is realized by TSF.AccessControl, TSF.Authenticate and TSF.SecureManagement.
- FMT_SMR.1: Requires the maintenance of security roles, this is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.

7.1.2. TSF.Authenticate

344 This TSF manages the identification and authentication of the Signatory and Administrator and enforces role separation (FMT_SMR.1)

345 After activation or reset of the TOE no user is authenticated.

346 TSF-mediated actions on behalf of a user require the user's prior successful identification and authentication.

347 The Platform contains a deterministic random number generator rated DRG.3 (high) according to AIS20 that provides random numbers used for the authentication.

348 The TSF.Authenticate provides the following authentication mechanism:

Compliance to [21], [22] and [28]:

- User verification
- Device authentication mechanism:
  - Device authentication with privacy protection
  - Symmetric authentication mechanism
- Role authentication
  - Symmetric role authentication
  - Asymmetric authentication based on RSA

Compliance to [26] and [12]:

- PACE
- Terminal Authentication
- Chip Authentication

The IDentity Applet is highly configurable according to the user's needs. In current ST, the TSF.Authenticate enforces to configure in the Personalisation phase of Applet life cycle and implement in the Operational phase authentication mechanism as the follows:

Authentication of Signatory (authenticating the signer as its signatory) either by:

- User verification [28]

To proof the identity of the QSCD:

- Chip Authentication v2 [10];
- Symmetric authentication [22];
- Active Authentication [13];
- Certificate request signature.

Authentication for trusted channel between CGA and QSCD either by:

- Symmetric authentication [22];
- Terminal Authentication v2 [10].

349 This part of the TSF provides functionality for the following SFRs:

- FDP_ACF.1/SCD/SVD_Generation: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.
- FDP_ACF.1/SVD_Transfer: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.
- FDP_ACF.1/Signature_creation: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.
- FIA_AFL.1 The requirement is about to detect when an administrator configurable positive integer unsuccessful authentication attempts occur related to consecutive failed authentication attempts and after that block the RAD. It is provided by TSF.Authenticate and TSF.AccessControl.
- FIA_API.1: The requirement is about identification and authentication and it is realized by TSF.Authenticate, TSF.CryptoKey and TSF.Platform. It requires security mechanisms to identify and to authenticate themselves as QSCD (Authentication Proof of Identity).
- FMT_SMR.1: Requires the maintenance of security roles, this is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.
- FMT_SMF.1: Requires the capability to perform management functions. It is realized by TSF.Authenticate and TSF.SecureManagement.
- FMT_MOF.1: This SFR requires the access control to signature-creation to the signatory and is realized TSF.AccessControl. TSF.Authenticate, and TSF.SecureManagement.
- FMT_MSA.1/Admin: Requires that the SCD/SVD generation SFP to modify query the SCD/SVD management to the Administrator. It is realized by TSF.AccessControl. TSF.Authenticate, and TSF.SecureManagement.
- FMT_MSA.1/Signatory: Requires access control restrictions to modify the SCD operational security attributes to the signatory. This is realized by TSF.AccessControl. TSF.Authenticate, and TSF.SecureManagement.
- FMT_MSA.2 The requirement is about the necessary authentication to change the security attributes of SCD/SVD management and SCD operation values. It is provided by TSF.Authenticate and TSF.SecureManagement and TSF.Platform.

- FMT_MSA.3: Requires the capability to perform authentication controls. This is realized by TSF.AccessControl, TSF.Authenticate and TSF.SecureManagement.
- FMT_MSA.4: Requires the capability to differentiate between actions made by certain users. It is realized by TSF.Authenticate and TSF.SecureManagement.
- FMT_MTD.1/Admin This SFR requires RAD creation to the Signatory. It is realized by TSF.AccessControl, TSF.Authenticate and TSF.SecureManagement
- FMT_MTD.1/Signatory: This SFR requires RAD modification to the Signatory. It is realized by TSF.AccessControl, TSF.Authenticate and TSF.SecureManagement.

7.1.3. TSF.SecureManagement

350 All security attributes are modified in a secure way so that no unauthorised modifications are possible.

351 The TSF.SecureManagement is responsible for the secure management of the security attributes, data and functions

352 This part of the TSF provides functionality for the following SFRs:

- FMT_SMF.1: Requires the capability to perform management functions. It is realized by TSF.Authenticate and TSF.SecureManagement.
- FMT_MOF.1: This SFR requires the access control to signature-creation to the signatory and is realized TSF.AccessControl. TSF.Authenticate, and TSF.SecureManagement.
- FMT_MSA.1/Admin: Requires that the SCD/SVD generation SFP to modify query the SCD/SVD management to the Administrator. It is realized by TSF.AccessControl. TSF.Authenticate, and TSF.SecureManagement.
- FMT_MSA.1/Signatory: Requires access control restrictions to modify the SCD operational security attributes to the signatory. This is realized by TSF.AccessControl. TSF.Authenticate, and TSF.SecureManagement.
- FMT_MSA.2 The requirement is about the necessary authentication to change the security attributes of SCD/SVD management and SCD operation values. It is provided by TSF.Authenticate and TSF.SecureManagement and TSF.Platform.
- FMT_MSA.3: Requires the capability to perform authentication controls. This is realized by TSF.AccessControl, TSF.Authenticate and TSF.SecureManagement.
- FMT_MSA.4: Requires the capability to differentiate between actions made by certain users. It is realized by TSF.Authenticate and TSF.SecureManagement.
- FMT_MTD.1/Admin This SFR requires RAD creation to the Signatory. It is realized by TSF.AccessControl, TSF.Authenticate and TSF.SecureManagement
- FMT_MTD.1/Signatory: This SFR requires RAD modification to the Signatory. It is realized by TSF.AccessControl, TSF.Authenticate and TSF.SecureManagement.

7.1.4. TSF.TrustedChannel

353 The TSF is responsible for the command and response exchanges between the TOE and the external devices (e.g. CGA).

354 The cases when the TOE uses trusted channel are the following:

- SVD export (ENC+MAC)
- data Authentication with Identity of Guarantor

355 This function is responsible for confidentiality, data integrity and data authenticity. It provides functionality for:

- FTP_ITC.1/SVD: This requirement is about the Trusted Channel which is provided by the TSF.TrustedChannel and TSF.Platform.

7.1.5. TSF.CryptoKey

356 TSF.CryptoKey is responsible for providing cryptographic support to all the other TSF including secure key generation (SCD/SVD key pair), digital signature creation. In addition, it provides secure key destruction method.

357 It provides functionality for:

- FCS_CKM.1: The SFR requires generation of cryptographic keys. It is realized by TSF.CryptoKey and TSF.Platform.
- FCS_CKM.4: Requires the cryptographic key destruction according to a specified cryptographic method. This is realized by TSF.CryptoKey and TSF.Platform.
- FCS_COP.1.: Requires a use of cryptographic operation. It is provided by TSF.CryptoKey and TSF.Platform.
- FDP_DAU.2/SVD: The requirement is about to generate evidence that can be used as a guarantee of the validity of SVD for the CGA. It is realized by the TSF.CryptoKey and TSF.Platform.
- FDP_SDI.2/DTBS: Requires data integrity monitoring and prohibits the use of altered data. It is provided by TSF.CryptoKey, TSF.AppletparameterSign and TSF.Platform.
- FIA_API.1: The requirement is about identification and authentication and it is realized by TSF.Authenticate, TSF.CryptoKey and TSF.Platform. It requires security mechanisms to identify and to authenticate themselves as QSCD (Authentication Proof of Identity).

7.1.6. TSF.AppletparameterSign

358 During the IDentity Applet life cycle phases after LOADED state of the IDentity Applet the IDentity Applet becomes the default Application and reaches SELECTABLE state of IDentity Applet. This phase is called the Initialization phase of IDentity Applet. During this phase, the following steps are carried out:

- Applet configuration;
- File creation (all control parameters);
- Object creation (all control parameters and some usage parameters).

359 Certain configuration and control parameters are signed, and this signature is verified before closing the Initialization phase. Only the unsigned parameters can be changed by the Initializer. This way only those Application Profiles can be applied which are validated by the Developer and conform to the requirements. The Initialization state cannot be finished by reaching the INITIALIZED state of IDentity Applet, and the Personalization phase of IDentity Applet cannot be started without successful signature verification.

360 These signatures can be verified during the whole IDentity Applet life-cycle, thus the non-authorized changed become detectable by applying this TSF.

361 The TSF provides functionality for the following SFRs:

- FDP_SDI.2/DTBS: Requires data integrity monitoring and prohibits the use of altered data. It is provided by TSF.CryptoKey, TSF.AppletparameterSign and TSF.Platform.
- FPT_FLS.1: The requirement requires the preservation of a secure state when detecting failures. This is provided by TSF.AppletparameterSign and TSF.Platform.

- FPT_TST.1: Requires self-test and capability to verify integrity of TSF and TSF data. This is provided by TSF.AppletparameterSign and TSF.Platform.

7.1.7. TSF.Platform

362 This TSF provides functionalities (such as CryptoLibrary, random number generation, etc.) to the followings:

- generate SCD/SVD key pair;
- support digital signature generation
- provide secure key destruction method functionality;
- provide mechanism to generate random numbers (DRG.3 (high));
- prohibit the use of the altered persistent data and inform the S.Sigy about integrity error;
- insure that the TOE shall not emit variations in power consumption or timing during command execution in excess of non-useful information enabling access to secret data;
- insure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the objects of session keys and ephemeral private key;
- insure that unauthorized are unable to use electrical contacts interface to gain access to secret data;
- preserve a secure state when exposure to operating conditions causing a TOE malfunction or failure is detected during self-tests;
- implements appropriate measures to continuously counter physical manipulation and physical probing;
- run a suite of self-tests to demonstrate the correct operation of the TSF and to verify the integrity of the TSF data and stored TSF executable code.

363 The Platform provides the following security functionality:

• SF.JCVM	Java Card Virtual Machine
• SF.OPEN	Card Content Management
• SF.CRYPTO	Cryptographic Functionality
• SF.RNG	Random Number Generator
• SF.DATA_STORAGE	Secure Data Storage
• SF.OM	Java Object Management
• SF.PIN	PIN Management
• SF.PERS_MEM	Persistent Memory Management
• SF.EDC	Error Detection Code API
• SF.HW_EXC	Hardware Exception Handling
• SF.SMG_NSC	No Side-Channel

364 These provide functionality for the following SFRs:

- FCS_CKM.1: The SFR requires generation of cryptographic keys. It is realized by TSF.CryptoKey and TSF.Platform.
- FCS_CKM.4: Requires the cryptographic key destruction according to a specified cryptographic method. This is realized by TSF.CryptoKey and TSF.Platform.
- FCS_COP.1: Requires a use of cryptographic operation. It is provided by TSF.CryptoKey and TSF.Platform.
- FDP_DAU.2/SVD: The requirement is about to generate evidence that can be used as a guarantee of the validity of SVD for the CGA. It is realized by the TSF.CryptoKey and TSF.Platform.

- FDP_RIP.1: This requirement is about to make unavailable any previous information content of SCD. It is provided by TSF.Platform
- FDP_SDI.2/Persistent: Requires data integrity monitoring and prohibits the use of altered data. It is provided by TSF.Platform.
- FDP_SDI.2/DTBS: Requires data integrity monitoring and prohibits the use of altered data. It is provided by TSF.CryptoKey, TSF.AppletparameterSign and TSF.Platform.
- FIA_API.1: The requirement is about identification and authentication and it is realized by TSF.Authenticate, TSF.CryptoKey and TSF.Platform. It requires security mechanisms to identify and to authenticate themselves as QSCD (Authentication Proof of Identity).
- FMT_MSA.2 The requirement is about the necessary authentication to change the security attributes of SCD/SVD management and SCD operation values. It is provided by TSF.Authenticate and TSF.SecureManagement and TSF.Platform.
- FPT_EMS.1: Requires that the TOE does not emit variations in power consumption or timing during command execution and ensures that unauthorized users are unable to use the electrical contact interface to gain access to RAD and SCD. This is mainly realized with TSF.Platform, together with the following of JavaCard platform guidelines.
- FPT_FLS.1: The requirement requires the preservation of a secure state when detecting failures. This is provided by TSF.AppletparameterSign and TSF.Platform.
- FPT_PHP.1: Requires detection of physical attack. This is realized by TSF.Platform.
- FPT_PHP.3: Requires resistance to physical manipulation and probing to the Platform. This is realized by the TSF.Platform.
- FPT_TST.1: Requires self-test and capability to verify integrity of TSF and TSF data. This is provided by TSF.AppletparameterSign and TSF.Platform.
- FTP_ITC.1/SVD: This requirement is about the Trusted Channel which is provided by the TSF.TrustedChannel and TSF.Platform.

7.2. Fulfilment of the SFRs

TOE SFR / Security Function	TSF.AccessControl	TSF.Authenticate	TSF.SecureManagement	TSF.TrustedChannel	TSF.CryptoKey	TSF.AppletparameterSign	TSF.Platform
FCS_CKM.1	-	-	-	-	X	-	X
FCS_CKM.4	-	-	-	-	X	-	X
FCS_COP.1	-	-	-	-	X	-	X
FDP_ACC.1/Signature_Creation	X	-	-	-	-	-	-
FDP_ACC.1/SCD/SVD_Generation	X	-	-	-	-	-	-
FDP_ACF.1/SCD/SVD_Generation	X	X	-	-	-	-	-
FDP_ACC.1/SVD_Transfer	X	-	-	-	-	-	-

FDP_ACF.1/SVD_Transfer	X	X	-	-	-	-	-
FDP_ACF.1/Signature_creation	X	X	-	-	-	-	-
FDP_DAU.2/SVD	-	-	-	-	X		X
FDP_RIP.1	-	-		-	-	-	X
FDP_SDI.2/Persistent	-	-	-	-	-	-	X
FDP_SDI.2/DTBS	-	-	-	-	X	X	X
FIA_AFL.1	X	X		-	-	-	-
FIA_UID.1	X	-	-	-	-	-	-
FIA_UAU.1	X	-	-	-	-	-	-
FIA_API.1	-	X	-	-	X	-	X
FMT_SMR.1	X	X	-	-	-	-	-
FMT_SMF.1		X	X	-	-	-	-
FMT_MOF.1	X	X	X	-	-	-	-
FMT_MSA.1/Admin	X	X	X	-	-	-	-
FMT_MSA.1/Signatory	X	X	X	-	-	-	-
FMT_MSA.2	-	X	X	-	-	-	X
FMT_MSA.3	X	X	X	-	-	-	-
FMT_MSA.4	-	X	X	-	-	-	-
FMT_MTD.1/Admin	X	X	X	-	-	-	-
FMT_MTD.1/Signatory	X	X	X	-	-	-	-
FPT_EMS.1	-	-	-	-	-	-	X
FPT_FLS.1	-	-	-	-	-	X	X
FPT_PHP.1	-	-	-	-	-	-	X
FPT_PHP.3	-	-	-	-	-	-	X
FPT_TST.1	-	-	-	-	-	X	X
FTP_ITC.1/SVD	-	-	-	X	-	-	X

12. Table Mapping of SFRs to mechanisms of TOE

7.2.1. Correspondence of SFR and TOE mechanisms

365 Each TOE security functional requirement is implemented by at least one TOE mechanism. In section 7.1 the implementing of the TOE security functional requirement is described in form of the TOE mechanism.

8. Glossary and Acronyms

366 For Glossary and Acronyms please refer to the corresponding section of [18] and [19]

9. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017

[5] IDentity Applet Suite v3.4 Administrator's Guide

[6] IDentity Applet Suite v3.4 User's Guide

[7] JCOP 4 P71 4 Security Target Lite for JCOP 4 P71 / SE050 Rev. 3.7 – 2020-03-17

[8] Supporting Document Mandatory Technical Document Composite product evaluation for Smart Cards and similar devices; Version 1.5.1, May 2018

[9] BSI TR-03110-1 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 eMRTDs with BAC/PACEv2 and EACv1 - Version 2.20 26., February 2015

[10] BSI TR-03110-2 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 2 Protocols for electronic Identification, Authentication and trust Services (eIDAS) - Version 2.21, 21. December 2016

[11] BSI TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 Common Specifications – Version 2.2121. December 2016

[12] BSI TR-03110-4 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 4 Applications and Document Profiles – Version 2.21, 21. December 2016

[13] International Civil Aviation Organization (ICAO) Doc 9303 Machine Readable Travel Documents, Seventh Edition, 2015

[14] International Civil Aviation Organization (ICAO) Supplemental Access Control for Machine Readable Travel Documents, Version – 1.1, 15. April 2014

[15] Protection Profile — Machine Readable Travel Document with ICAO Application and Basic Access Control (MRTD-PP), Version 1.10, BSI-CC-PP-0055, 25.03.2009

[16] Protection Profile — Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE (EAC PP), Version 1.3.2, BSI-CC-PP-0056-V2-2012, 05.12.2012

[17] Protection Profile — Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.0, BSI-CC-PP-0068-V2-2011, 02.11.2011

[18] EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device with key generation

[19] EN 419211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application

[20] BSI: Common Criteria Protection Profile - Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use [MR.ED-PP], BSI-CC-PP-0087 version 1.01, May 20th, 2015

[21] CEN/TS 15480-2 – Identification card systems - European Citizen Card - Part 2: Logical data structures and card services

[22] European Card for e-Services and National e-ID Applications - IAS ECC, Revision 1.0.1, 21.03.2008

[23] 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] OJ L 257/73

[24] Published by Oracle. Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., May 2015.

[25] Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 2.0 28.06.2012

[26] BSI Technische Richtlinie TR-03117 eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit version 1.0

[27] JCOP 4 P71 D321 User guidance and administrator manual Rev. 3.7 – 20190531

[28] Technical report – Signature creation and administration for eIDAS token Part 1. Functional Specification – version 1.0, 2015.07.21

[29] Protection Profile for ePassport IC with SAC (BAC+PACE) and Active Authentication, version 1.0, March 8,2016, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan

[30] Protection Profile for ePassport IC with SAC (PACE) and Active Authentication, version 1.0, March 8,2016, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan