ChipDoc v3 on JCOP 4 P71 in SSCD configuration

Security Target Lite

Rev. 1.9 — 2 December 2024 **Evaluation document**

Document information

Information	Content
Keywords	Common Criteria, Security Target Lite, ChipDoc v3, SSCD
Abstract	Security Target Lite of ChipDoc v3 application on JCOP 4 P71 in SSCD configuration, which is developed and provided by NXP Semiconductors, Business Unit Identification according to the Common Criteria for Information Technology Security Evaluation Version 3.1 at Evaluation Assurance Level 5 augmented.

Revision History

Rev.	Date	Description
1.0	2020-02-24	Initial version of this Security Target Lite.
1.5	2022-06-21	Update of hardware IC and JavaCard Platform references. Added new guidance document ChipDoc V3 Application Note.Align version with ST Full.
1.6	2022-07-12	Update JCOP4 P71 ST version
1.7	2024-06-10	Update of hardware IC and JavaCard Platform references. Updated reference to guidance document ChipDoc V3 Application Note.
1.8	2024-10-31	Updated guidance document references
1.9	2024-12-02	Updated guidance document references

1 Introduction

1.1 TOE Reference and ST Reference

Table 1. TOE Reference and ST Reference

TOE Name	ChipDoc v3 on JCOP 4 P71 in SSCD configuration Version 3.0.0.52
ST Title	ChipDoc v3 on JCOP 4 P71 in SSCD configuration Security Target Lite
Version	Revision 1.9
Date	2024-12-02
Product Type	Java Card Applet
CC Version	Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 5, April 2017 (Part 1 [1], Part 2 [2] and Part 3 [3])

1.2 TOE Overview

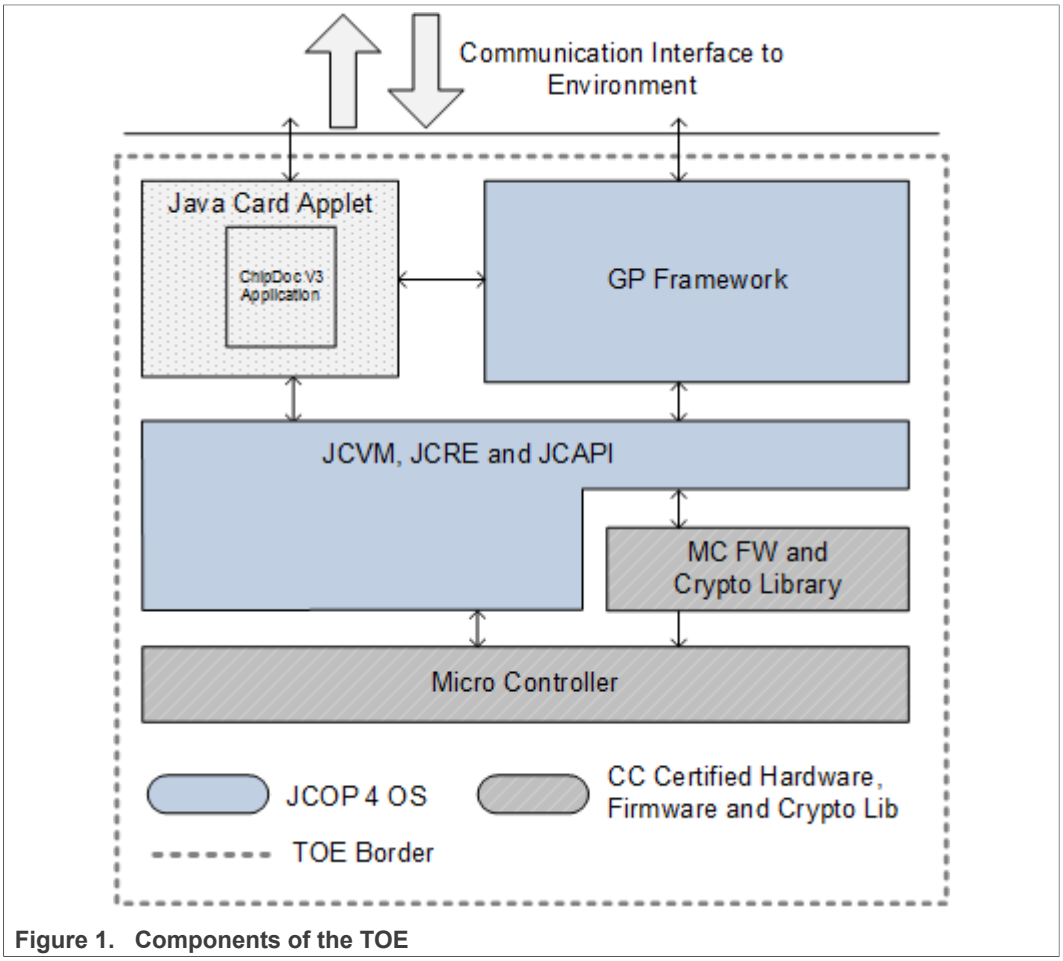

Figure 1. Components of the TOE

The TOE consists of an applet which is executed by a software stack that is stored on a Micro Controller. Figure 1 illustrates the components of the TOE, while Section 1.3.1 provides more details with respect to the dedicated components.

The TOE is delivered in open configuration, meaning that next to the interfaces provided by the SSCD application, GlobalPlatform (GP) interfaces to load and delete applications are available.

The TOE implements a Secure Signature Creation Device (SSCD) with PACE authentication in accordance with the European Directive 1999/93/EC [15] as a smart card which allows the generation and importation of signature creation data (SCD) and the creation of qualified electronic signatures. The TOE protects the SCD and ensures that only an authorized Signatory can use it.

The TOE meets all the following requirements as defined in the European Directive (article 2.2):

- it is uniquely linked to the signatory
- it is capable of identifying the signatory
- it is created using means that the signatory can maintain under his sole control
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

The TOE type is compliant with the Protection Profiles claimed according to section Section 2.2,where the conformance to the Protection Profiles is strict.

The TOE Secure Signature-Creation Device representing the SCD/SVD import, generation, SCD Storage and signature-creation components. The TOE is a personalized component, meaning that it can only be used for signature- creation by one specific user – the signatory – only.

Although the notion of SSCD types is no longer supported in the published EN's, the previous set of standards defining Secure Signature Creation device used 'Type 2' to define an SSCD that can import the SCD/SVD keys and 'Type 3' to define an SSCD which could generate it's own SCD/SVD key-pairs. This terminology is still used within industry.

Note that there is no non-TOE hardware/software/firmware that is required by the TOE.

1.3 TOE Description

1.3.1 TOE Components and Composite Certification

The certification of this TOE is a composite certification. This means that for the certification of this TOE other certifications of components which are part of this TOE are re-used. In the following sections more detailed descriptions of the components of Fig 1 are provided. In the description it is also made clear whether a component is covered by a previous certification or whether it is covered in the certification of this TOE.

1.3.1.1 Micro Controller

The Micro Controller is a secure smart card controller from NXP's SmartMX3 family. The Micro Controller contains a co-processor for symmetric cryptographic operations, supporting DES and AES, as well as an accelerator for asymmetric cryptographic 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.

The Micro Controller has been certified in a previous certification and the results are re-used for this certification. The exact reference to the previous certification is given in the following table:

Table 2. Reference to Certified Micro Controller with IC Dedicated Software and Crypto Library

Name	NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4)
Certificate	BSI-DSZ-CC-1136-V4-2024
Reference	[12]

1.3.1.2 Security IC Dedicated Software

1.3.1.2.1 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 volatile and non-volatile memory.

The Micro Controller Firmware has been certified together with the Micro Controller (refer to table Table 2) and the same references [12] as given for the Micro Controller also apply for the Micro Controller Firmware.

1.3.1.2.2 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 symmetric cryptographic operations comprise the algorithms 3DES, AES and KoreanSEED, where these algorithms use the symmetric co-processor of the Micro Controller. 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.

The Crypto Library has been certified together with the Micro Controller (refer to table Table 2) and the same references [12] as given for the Micro Controller also apply.

1.3.1.3 Security IC Embedded Software

1.3.1.3.1 JCOP 4 P71

The Operating System consists of JCVM, JCRE, JCAPI and GP framework. It is implemented according to the Java Card Specification and GlobalPlatform and has been certified in the course of a previous certification, where the results are re-used for this certification. The exact reference to the certification is given in the following table:

Table 3. Reference to certified Platform

Name	JCOP 4 P71
Configurations relevant for this TOE	JCOP 4 P71 v4.7 R1.00.4 JCOP 4 P71 v4.7 R1.01.4 JCOP 4 P71 v4.7 R1.02.4
Certificate	NSCIB-CC-2300172-01
Reference	[13]

1.3.1.3.2 ChipDoc v3 application

The ChipDoc v3 Java Card application implementing a Secure Signature Creation Device in accordance with the European Directive 1999/93/EC [15] as a smart card which allows the generation and importation of signature creation data (SCD) and the creation of qualified electronic signatures. The TOE protects the SCD and ensures that only an authorized Signatory can use it.

This functionality is subject of the current certification and thus forms the composite product from formal point of view. However, next to SSCD, the ChipDoc v3 application offers variety of applications like electronic identification (eID), electronic driver's license (eDL) or electronic passport (ePP).

1.3.2 TOE as Secure Signature Creation Device

An SSCD provides the following functions:

- to generate or import signature-creation data (SCD) and the correspondent signature-verification data (SVD),
- to export the SVD for certification through a trusted channel to the CGA if the SVD has been created by the device
- to prove the identity as SSCD to external entities,
- to, optionally, receive and store certificate info,
- to initialize user authentication data (RAD),
- to switch the SSCD from a non-operational state to an operational state, and
- if in an operational state, to create digital signatures for data with the following steps:
  - select an SCD if multiple are present in the SSCD,
  - receive data to be signed or a unique representation thereof (DTBS/R) through a trusted channel with SCA,
  - authenticate the signatory and determine its intent to sign,
  - apply an appropriate cryptographic signature-creation function using the selected SCD to the DTBS/R.

An SSCD shall only be switched to an operational state if it is properly prepared for the signatory's use and sole control by

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

Upon receiving an SSCD the signatory shall verify that any SCD it contains is in a non-operational state.

The SSCD provides management functions for key generation or import initiated by the user as specified in 2.1.1.2.

1.3.2.1 Additional Functionality including PACE Secure Messaging

1.3.2.1.1 User Authentication

The SSCD provides functions to enable the user to

1. Unblock the RAD,
2. Change the value of the RAD,

3. Add or modify user information to be included in signatory identification data in a SVD certificate.

1.3.2.1.2 User Management of Signing Key

The SSCD provides functions to enable the user to

1. Install an SCD, generated outside the device in a trusted environment and communicated over a secure communication link 2.1.1.3(2)
2. Generate an SCD,
3. Disabling an SCD it holds, e.g. by erasing it from memory,
4. Create, extend or modify certificate info stored in the device, and
5. Create SVD for an SCD stored and export it for certification by a certificate generating application protected by trusted communication (2.1.1.3 (1)).

1.3.2.1.3 Secure Communication based on PACE Authentication

The SSCD provides PACE authentication based on MRZ, CAN or PIN in order to enscure a trusted, cryptographically protected communication with

1. A certificate-generation application,
2. An SVD-generating application, and
3. A signature-creation application.

The supported functions include functions for management of the cryptographic keys, parameters and configuration used to establish the trusted communication.

1.3.3 TOE Life Cycle

The life cycle of a generic SSCD product introduces the role of the SSCD Provisioning service. The SSCD Life-cycle distinguishes stages for development, production, preparation and operational use. Development and production of the SSCD together constitute the development phase of the TOE. The development phase is subject of CC evaluation according to the assurance life cycle (ALC) class. The development phase ends with the delivery of the TOE to an SSCD-provisioning service provider. The functional integrity of the TOE shall be protected in delivering it to an SSCD-provisioning service provider.

The IC Developer, IC Manufacturer as well as the MRTD Embedded Software Developer of this TOE is NXP Semiconductors. In particular the software development for this composite TOE took place at “NXP Gratkorn, Mikron-Weg 1, A-8101 Gratkorn, Austria”. All other sites contributing to the Lifecycle of this TOE can be read from the certification report of the underlying IC[1]

1.3.3.1 Development Phase

1.3.3.1.1 Design Phase

The TOE is developed in this phase. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components

1 BSI-DSZ-CC-1136-V2-2022

1.3.3.1.2 Fabrication Phase

The core parts of the Operating System are sent in a secure way for masking into ROM. In addition to the TOE, the mask contains confidential data, knowledge of which is required in order to initialize and personalize the chip.

1.3.3.1.3 Integration Phase

This phase corresponds to the integration of the hardware and firmware components into the final product body. In the case of this TOE it will be a smart card, but it could also be a USB token. Modulare parts of the Operating System as well as the final application are loaded into the Flash memory of the TOE during this phase. The TOE is protected during transfer between various parties with a diversified (per card) Transport Key.

1.3.3.1.4 Initialization Phase

The initialization phase consists in OS configuration, applet instantiation and/or applet and OS patching activities.

To create the application, it is necessary to instantiate the applet and create an SSCD file system. In addition to the certified SSCD file system, one or more additional file systems may be present on the TOE. This allows the TOE user to switch between more than one (potentially certified) file systems or configurations of the application. Since the ChipDoc v3 application offers electronic identity, driving license or MRTD functionalities in addition to SSCD, the associated file systems may coexist on the TOE.

At this point, additional applets could be loaded in the TOE. Afterwards, Card Content Loading and Installing mechanism is terminated in this phase, i.e. the platform is closed

The product becomes operational and is delivered to the SSCD Provisioning Service after this initialization phase. The card is protected by a Transport Key during the transfer between NXP Manufacturing and the SSCD Provisioning Service site.

1.3.3.2 Operational Phase

1.3.3.2.1 Personalization Phase

After unlocking the product with the transport key, NXP or 3rd Party Personalization facility which includes the loading of Personal Application Data and optional generation of the SCD/SVD pair if loading does not include importing an SCD/SVD pair. The product is considered in use phase

If not performed by NXP, personalization is usually applied by an **SSCD-provisioning Service Provider**, preparing the TOE for use and delivering it to the legitimate user. The preparation phase ends when the legitimate user of the TOE, having received it from an SSCD provisioning service enables an SCD it holds for use in signing.

During preparation of the TOE, an SSCD-provisioning service provider performs the following tasks:

- 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;

- 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;
- Generate a certificate for at least one SCD either by:
  - The TOE generating an SCD/SVD pair and obtaining a certificate for the SVD exported from the TOE, or
  - Initializing security functions in the TOE for protected export of the SVD and obtaining a certificate for the SVD after receiving it from the TOE;
- Optionally, present certificate info to the SSCD;
- Deliver the TOE and the accompanying VAD info to the legitimate user.

The SVD certification task (third list item above) of an SSCD-provisioning service provider as specified in this PP may support a centralised, 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.

Data required for inclusion in the SVD certificate at least includes (The Directive [15] ,Annex II):

- The SVD;
- The name of the signatory either:
  - A legal name, or
  - A pseudonym together with an indication of this fact.

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

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

- the sender as genuine SSCD
- the integrity of the SVD to be certified as sent by the originating SSCD,
- that the originating SSCD has been personalized for the legitimate user,
- correspondence between SCD and SVD, and
- that the signing algorithm and key size for the SVD are approved and appropriate for the type of certificate.

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 i . Security requirements to protect the SVD export function and the certification data if the SVD is generated by the signatory and then exported from the SSCD to the CGA are specified in part 4 of this series of European standards

Prior to generating the certificate the certification service provider shall assert the identity of the signatory as the legitimate user of the TOE

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 to the legitimate user shall protect the confidentiality of the corresponding RAD.

1.3.3.2.2 Usage Phase

In the operational-use stage the signatory can use the TOE to create advanced electronic signatures. The signatory can render an SCD in the TOE permanently unusable. Rendering the last SCD in the TOE permanently unusable may end the life of the TOE as SSCD.

Note that an SSCD that supports key generation in the operational-use stage does not end its life when it no longer has a usable SCD

The TOE may support functions to generate signing keys in the operational stage (6.2.2.3(2)). 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 to be incorporated in the certificate, for instance to use a pseudonym instead of the legal name. If the conditions to obtain a qualified certificate are met the new key can also 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 SSCD- Provisioning service provider in an environment that is secure or using trusted communication.

1.3.3.3 Scope of SSCD PP Application

This ST refers to qualified certificates as electronic attestation of the SVD corresponding to the signatory's SCD that is implemented by the TOE.

While the main application scenario of a SSCD will assume a qualified certificate to be used in combination with a SSCD, there still is a large benefit in the security when such SSCD is applied in other areas and such application is encouraged. The SSCD may as well be applied to environments where the certificates expressed as 'qualified certificates' in the SSCD do not fulfil the requirements laid down in Annex I and Annex II of the Directive [15].

When an instance of a SSCD is used with a qualified certificate, such use is from the technical point of view eligible for an electronic signature as referred to in Directive [15], article 5, paragraph 1. This Directive does not prevent TOE itself from being regarded as a SSCD, even when used together with a non-qualified certificate.

1.3.4 TOE Identification

1.3.4.1 TOE Delivery

The delivery comporises the following items:

Table 4. Delivery Items

Type	Name	Version	Form of delivery
JCOP 4 P71 Platform	NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library ROM Code (Platform ID) FLASH content (FLASH ID) Patch Code (Patch ID)	R1.00.4 R1.01.4 R1.02.4	Micro Controller including on-chip software: Firmware, Crypto Library and JCOP 4 Operating System
ChipDoc v3 application	FLASH content	3.0.0.52	Application Software loaded onto the IC

Table 4. Delivery Items*...continued*

Type	Name	Version	Form of delivery
Document	ChipDoc 3.0 User Guide Manual [10]	2.5	Electronic document
Document	ChipDoc 3.0 SSCD Personalization Guide [11]	1.6	Electronic document
Document	ChipDoc V3 Application note [14]	1.6	Electronic document

1.3.4.2 Identification of the TOE

The TOE can be identified by

- identifying the JCOP 4 P71 platform: The IDENTIFY command shall be sent to the TOE to verify the correct values of Platform ID, the FLASH ID and the Patch ID as stated in section "2.2 Platform identification" of the Personalization Guidance for this TOE [11]
- identifying the SSCD application: The ChipDoc v3 application and the specific TOE configuration (SSCD) can be verified according the respective instructions in section "2. Identification" of the Personalization Guidance for this TOE [11]

1.3.5 Evaluated Package Types

A number of package types are supported for this TOE. All package types, which are covered by the certification of the used platform (see [13]), are also allowed to be used in combination with each product of this TOE.

The package types do not influence the security functionality of the TOE. They only define which pads are con- nected in the package and for what purpose and in which environment the chip can be used. Note that the security of the TOE is not dependent on which pad is connected or not - the connections just define how the product can be used. If the TOE is delivered as wafer the customer can choose the connection on his own.

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target claims to be conformant to the Common Criteria version 3.1:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, CCMB-2017-04-001, April 2017 [1].
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, CCMB-2017-04-002, April 2017 [2].
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, CCMB-2017-04-003, April 2017 [3].

For the evaluation the following methodology will be used:

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

This Security Target claims to be CC Part 2 extended and CC Part 3 conformant. The extended Security Functional Requirements are defined in Section 5.

2.2 PP Claim

This Security Target claims strict conformance to the following Protection Profiles:

- [PP_Part2] Protection profiles for secure signature creation device — Part 2: Device with key generation [5].
- [PP_Part3] Protection profiles for secure signature creation device — Part 3: Device with key import [6].
- [PP_Part4] Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application [7].
- [PP_Part5] Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application [8].
- [PP_Part6] Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted communication with signature creation application [9].

2.3 Package Claim

This Security Target claims conformance to the assurance package EAL5 augmented with AVA_VAN.5 and ALC_DVS.2.

2.4 Conformance Claim Rationale

The conformance claim rationale is given in section Section 8.3

3 Security Problem Definition

This section lists the assets, threats, organisational security policies and assumptions from the Protection Profiles as cited here:

3.1 Assets

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. The subesquently listed are relevant for this TOE:

1. SCD: 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.
2. SVD: public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when it is exported must be maintained.
3. DTBS and DTBS/R: 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 electronic signature must be maintained.

3.2 Subjects

This Security Target considers the following users and subjects representing users:

Table 5. Users and Subjects for this TOE

Users	Subjects	Definition
User	S.User	End user of the TOE which can be identified with S.Admin or S.Signatory. The subject S.User may act as S.Admin in the rol *Administrator* or as S.Signatory in the role *Signatory*
Administrator	S.Admin	User who is in charge to perform the TOE initialization, TOE personalization or other TOE adminstrative functions. The subject S.Admin is acting in the role *Administrator* for this user after successful authentication as *Administrator*
Signatory	S.Signatory	User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents. The subject S.Signatory is acting in the role *Signatory* for this use after successful authentication as *Signatory*.

The following threat agent is relevant for this Security Target:

1. Attacker: 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.

3.3 Threats

T.SCD_Divulg *Storing, copying and releasing of the signature creation data*

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*

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*

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*

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*

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*

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*

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.

3.4 Organisational Security Policies

P.CSP_QCert *Qualified certifcate*

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. **the directive**, article 2, clause 9, and Annex I) for the SVD generated by the SSCD. The certificates contain at least the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE as SSCD is evident with signatures through the certificate or other publicly available information.

P.QSign *Qualified electronic signatures*

The signatory uses a signature creation system to sign data with an advanced electronic signature (cf. **the directive**, article 1, clause 2), which is a qualified electronic signature if it is based on a valid qualified certificate (according to **the directive** Annex I)[1] . The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature created with a SCD implemented in the SSCD that the signatory maintain under their sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

P.Sigy_SSCD *TOE as secure signature creation device*

The TOE meets the requirements for an SSCD laid down in Annex III of the **directive**. 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-repudation of signatures*

The lifecycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate.

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

3.5 Assumptions

A.CGA *Trustworthy certificate generation application*

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*

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.

A.CSP *Secure SCD/SVD management by CSP*

The CSP uses only a trustworthy SCD/SVD generation device and ensures that this device can be used by authorised user only. The CSP ensures that the SCD generated practically occurs only once, that generated SCD and SVD actually correspond to each other and that SCD cannot be derived from the SVD. The CSP ensures the confidentiality of the SCD during generation and export to the TOE, does not use the SCD for creation of any signature and irreversibly deletes the SCD in the operational environment after export to the TOE.

4 Security Objectives

4.1 Security Objectives for the TOE

OT.Lifecycle_Security *Lifecycle security*

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

Application note: 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 SSCD e.g. after the (qualified) certificate for the corresponding SVD has been expired.

OT.SCD/SVD_Auth_Gen *Authorized SCD/SVD generation*

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

OT.SCD_Auth_Imp *Authorized SCD Import*

The TOE shall provide security features to ensure that authorised users only may invoke the import of the SCD.

OT.SCD_Unique *Uniqueness of the signature creation data*

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*

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.Secrecy *Secrecy of the signature creation data*

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

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

OT.Sig_Secure *Cryptographic security of the electronic signatures*

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*

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*

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 emanations security*

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*

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*

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

OT.TOE_SSCD_Auth *Authentication proof as SSCD*

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

OT.TOE_TC_SVD_Exp *TOE trusted channel for SVD export*

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.

OT.TOE_TC_VAD_Imp *Trusted channel of TOE for VAD import*

The TOE shall provide a trusted channel for the protection of the confidentiality and integrity of the VAD received from the HID as needed by the authentication method employed.

Application note: This security objective for the TOE is partly covering OE.HID_VAD from the core PP. While OE.HID_VAD in the core PP requires only the operational environment to protect VAD, this PP requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp. Therefore this PP re-assigns partly the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

OT.TOE_TC_DTBS_Imp *Trusted channel of TOE for DTBS import*

The TOE shall provide a trusted channel to the SCA to detect alteration of the DTBS/R received from the SCA. The TOE must not generate electronic signatures with the SCD for altered DTBS.

Application note: This security objective for the TOE is partly covering OE.DTBS_Protect from the core PP. While OE.DTBS_Protect in the core PP requires only the operational environment to protect DTBS, this PP requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp. Therefore this PP re-assigns partly the DTBS protection from the operational environment as described by OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp and leaves only the necessary functionality by the SCA.

4.2 Security Objectives for the operational environment

OE.SCD/SVD_Auth_Gen *Authorized SCD/SVD Generation*

The CSP shall provide security features to ensure that authorised users only may invoke the generation of the SCD and the SVD.

OE.SCD_Secrecy *SCD Secrecy*

The CSP shall protect the confidentiality of the SCD during generation and export to the TOE. The CSP shall not use the SCD for creation of any signature and shall irreversibly delete the SCD in the operational environment after export to the TOE.

OE.SCD_Uniqe *Uniqueness of the signature creation data*

The CSP shall ensure the cryptographic quality of the SCD/SVD pair, which is generated in the environment, for the qualified or advanced electronic signature. The SCD used for signature creation shall practically occur only once, i.e. the probability of equal SCDs shall be negligible, and the SCD shall not be reconstructable from the SVD

OE.SCD_SVD_Corresp *Correspondence between SVD and SCD*

The CSP shall ensure the correspondence between the SVD and the SCD generated by the CSP. This includes the correspondence between the SVD send to the CGA and the SCD exported to the TOE of the signatory identified in the SVD certificate.

OE_SVD_Auth *Authenticity of the SVD*

The operational environment shall ensure the integrity of the SVD sent to the CGA of the CSP. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

OE.CGA_QCert *Generation of qualified certificates*

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

1. the name of the signatory controlling the TOE,
2. the SVD matching the SCD stored in the TOE and being under sole control of the signatory,
3. 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 SSCD.

OE.SSCD_Prov_Service *Authentic SSCD provided by SSCD-provisioning service*

The SSCD-provisioning service shall initialise and personalise for the signatory an authentic copy of the TOE and deliver this copy as SSCD to the signatory.

OE.HID_VAD *Protection of VAD*

If an external device provides the human interface for user authentication, this device shall ensure confidentiality and integrity of the VAD as needed by the authentication method employed from import through its human interface until import through the TOE interface. In particular, if the TOE requires a trusted channel for import of the VAD, the HID shall support usage of this trusted channel.

OE.DTBS_Intend *SCA sends data intended to be signed*

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.

Application note: 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 SSCD for use by SCA and identification of the corresponding SCD if more than one SCD is stored on the SSCD.

OE.DTBS_Protect *SCA protects the data intended to be signed*

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*

The signatory shall check that the SCD stored in the SSCD received from SSCD-provisioning service is in non-operational state. The signatory shall keep their VAD confidential.

OE.Dev_Prov_Service *Authentic SSCD provided by SSCD Provisioning Service*

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

OE.CGA_SSCD_Auth *Pre-initialisation of the TOE for SSCD authentication*

The CSP shall check by means of the CGA whether the device presented for application of a (qualified) certificate holds unique identification as SSCD, successfully proved this identity as SSCD 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*

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

OE.HID_TC_VAD_Exp *Trusted channel of HID for VAD export*

The HID provides the human interface for user authentication. The HID will ensure confidentiality and integrity of the VAD as needed by the authentication method employed including export to the TOE by means of a trusted channel.

Application note: This security objective for the TOE is partly covering OE.HID_VAD from the core PP. While OE.HID_VAD in the core PP requires only the operational environment to protect VAD, this PP requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp. Therefore this PP re-assigns partly the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

OE.SCA_TC_DTBS_Exp *Trusted channel of SCA for DTBS export*

The SCA provides a trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS/R cannot be altered undetected in transit between the SCA and the TOE.

Application note: This security objective for the TOE is partly covering OE.DTBS_Protect from the core PP. While OE.DTBS_Protect in the core PP requires only the operational environment to protect DTBS, this PP requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp. Therefore this PP re-assigns partly the DTBS protection from the operational environment as described by OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp and leaves only the necessary functionality by the SCA.

4.3 Security Objectives Rationale

All the security objectives described in the ST are traced back to items described in the TOE security environment and any items in the TOE security environment are covered by those security objectives appropriately.

4.3.1 Security Objectives Coverage

The following table indicates that all security objectives of the TOE are traced back to threats and/or organizational security policies and that all security objectives of the environment are traced back to threats, organizational security policies and/or assumptions.

Table 6. Mapping of security problem definition to security objectives

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Auth_Imp	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_SSCD_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_TC_VAD_Imp	OT_TOE_TC_DTBS_Imp	OE.SCD/SVD_Auth_Gen	OE.SCD_Secrecy	OE.SCD_Unique	OE.SCD_SVD_Corresp	OE.CGA_Qcert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory	OE.Dev_Prov_Service	OE_CGA_SSCD_Auth	OE.CGA_TC_SVD_Imp	OE.HID_TC_VAD_Exp	OE.SCA_TC_DTBS_Exp
T.SCD_Divulg			X			X											X	X														
T.SCD_Derive		X					X												X													
T.Hack_Phys						X				X	X	X																				
T.SVD_Forgery					X									X						X		X								X		
T.SigF_Misuse	X							X	X						X	X								X	X	X	X			X	X
T.DTBS_ Forgery									X							X									X	X						X
T.Sig_Forgery				X			X												X		X											
P.CSP_QCert	X		X		X								X				X			X	X								X			X
P.QSign							X	X													X				X							
P.Sigy_SSCD	X	X	X	X		X	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	X		X	X	X	X	X	X	X	X	X
A.CGA																					X	X										
A.SCA																									X							
A.CSP																	X	X	X	X												

4.3.2 Security objectives sufficiency

Countering of threats by security objectives:

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 and OE.SCD_Secrecy, which assures the secrecy of the SCD in the CSP environment.

Furthermore, generation and/or import of SCD known by an attacker is countered by OE.SCD/SVD_Auth_Gen, which ensures that only authorized SCD generation in the environment is possible, and OT.SCD_Auth_Imp, which ensures that only authorised SCD import is possible.

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 as well as OE.SCD_Unique are countering this threat by implementing cryptographically secure generation of the SCD/SVD pair. OT.Sig_Secure ensures cryptographically secure electronic signatures.

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.

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 SSCD 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.

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. The combination of OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS) counters the undetected manipulation of the DTBS during the transmission form the SCA to 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_TC_VAD_Exp (Trusted channel of HID for VAD) requires the HID to protect the confidentiality and the integrity of the VAD as needed by the authentication method employed. The HID and the TOE will protect the VAD by a trusted channel between HID and TOE according to OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) and OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD). OE.Signatory (Security obligation of the signatory) ensures that the signatory checks that an SCD stored in the SSCD when received from an SSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the signatory becomes control over the SSCD.

OE.Signatory (Security obligation of the signatory) ensures also that the signatory keeps their VAD confidential.

T.DTBS_Forgery (Forgery of the DTBS/R) addresses the threat arising from modifications of the DTBS/R sent to the TOE for signing which than does not correspond to the DTBS/R corresponding to the DTBS the signatory intends to sign. The threat T.DTBS_Forgery is addressed by the security objectives OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS), which ensure that the DTBS/R is sent through a trusted channel and cannot be altered undetected in transit between the SCA and the TOE. The TOE counters internally this threat by the means of OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) ensuring the integrity of the DTBS/R inside the TOE. The TOE IT environment also 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.

T.Sig_Forgery (Forgery of the electronic signature) deals with non-detectable forgery of the electronic signature. OT.Sig_Secure, OT.SCD_Unique, OE.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 and OE.SCD_Unique ensure 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:

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 directive, article 5, paragraph 1. Directive, recital (15) refers to SSCDs 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_SSCD_Auth the copies of the TOE will hold unique identity and authentication data as SSCD and provide security mechanisms enabling the CGA to identify and to authenticate the TOE as SSCD to prove this identity as SSCD to the CGA. The OE.CGA_SSCD_Auth ensures that the SP checks the proof of the device presented of the applicant that it is a SSCD. 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.

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.

P.Sigy_SSCD (TOE as secure signature creation device) requires the TOE to meet Annex III of the directive. 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_Gen and OT.Sigy_SigF.

OE.Dev_Prov_Service ensures that the legitimate user obtains a TOE sample as an authentic, initialised and personalised TOE from an SSCD Provisioning Service through the TOE delivery procedure. If the TOE implements SCD generated under control of the SSCD Provisioning Service the legitimate user receives the TOE as SSCD. 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_SSCD_Auth and OT.TOE_TC_SVD_Exp) to check whether the device presented is a SSCD linked to the applicant as required by OE.CGA_SSCD_Auth and the received SVD is sent by this SSCD as required by OE.CGA_TC_SVD_Imp. Thus the obligation of the SSCD 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.

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, which ensures the aspects of signatory’s sole control over and responsibility for the electronic signatures generated with the TOE.

OE.Dev_Prov_Service and OE.SSCD_Prov_Service ensure 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. 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.

OE.Signatory ensures that the signatory checks that the SCD, stored in the SSCD received from an SSCD provisioning service is in non-operational state (i.e. the SCD cannot be used before the signatory becomes into sole control over the SSCD). The TOE security feature addressed by the security objectives OT.TOE_SSCD_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 SSCD as required by OE.CGA_SSCD_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. The confidentiality of VAD is protected during the transmission between the HI device and TOE according to OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) and OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD).

OE.DTBS_Intend, OE.DTBS_Protect, OT.DTBS_Integrity_TOE, OT.TOE_TC_DTBS_Imp and OE.SCA_TC_DTBS_Exp 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.

OE.SSCD_Prov_Service ensures that the signatory obtains an authentic copy of the TOE, initialised and personalised as SSCD from the SSCD-provisioning service. OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy and OE.SCD_Unique ensure the security of the SCD in the CSP environment. OE.SCD_Secrecy ensures the confidentiality of the SCD during generation, during and after export to the TOE. The CSP does not use the SCD for creation of any signature and deletes the SCD irreversibly after export to the TOE. OE.SCD_Unique provides that the signatory’s SCD can practically occur just once. OE.SCD_SVD_Corresp ensures that the SVD in the certificate of the signatory corresponds to the SCD that is implemented in the copy of the TOE of the signatory.

OE.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. 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.

OE.Signatory ensures that the signatory checks that the SCD, stored in the SSCD received from an SSCD- provisioning service is in non-operational state (i.e. the SCD cannot be used before the signatory becomes into sole control over the SSCD). 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 creates electronic signatures only for those DTBS/R, which the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig_Secure ensure that only this SCD may create 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

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.

A.CGA *(Trustworthy certificate 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 verification of the authenticity and 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 SSCD of the signatory.

A.CSP *(Secure SCD/SVD management by CSP)* establishes several security aspects concerning handling of SCD and SVD by the CSP. That the SCD/SVD generation device can only be used by authorized users is addressed by OE.SCD/SVD_Auth_Gen (Authorized SCD/SVD Generation), that the generated SCD is unique and cannot be derived by the SVD is addressed by OE.SCD_Unique (Uniqueness of the signature creation data), that SCD and SVD correspond to each other is addressed by OE.SCD_SVD_Corresp (Correspondence between SVD and SCD), and that the SCD are kept confidential, are not used for signature generation in the environment and are deleted in the environment once exported to the TOE is addressed by OE.SCD_Secrecy (SCD Secrecy).

5 Extended Components Definition

This Security Target contains the following extended component define as extension to CC part in the claimed Protection Profiles:

- SFR FPT_EMS.1 "TOE Emanation" (denoted as FPT_EMSEC in Protection Profile)
- SFR FIA_API.1 "Authentication Proof of Identity"

5.1 TOE Emanation (FPT_EMS.1)

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.

FPT_EMS TOE Emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations

Component Leveling:

FPT_EMS.1 TOE Emandation has two constituents:

- FPT_EMS.1.1 Limit of Emissions requires to net emit intelligible emissions enabling access to TSF data or user data.
- FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1

There are no management activities foressen.

Audit: FPT_EMS.1

There are no actions identified that shall be auditable if FAU_GEN (Security audit data generation) is included in a PP or ST using FPT_EMS.1

FPT_EMS.1	**TOE Emanation**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit [assignment: *types of emission*] in excess of [assignment: *specified limits* enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*]
FPT_EMS.1.2	The TOE shall ensure [assignment: *types of users*] are unable to use the following interface [assignment: *type of connection*]

to gain access [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*]}

5.2 Authentication Proof of Identity (FIA_API.1)

To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. 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

FIA_API Authentication Proof of Identity

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 Leveling:

FIA_API.1 Authentication Proof of Identitiy

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.

Audit: FIA_API.1

There are no actions defined to be auditable.

FIA_API.1	**Authentication Proof of Identity**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TOE shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user of role*.

6 Security Requirements

This chapter gives the security functional requirements and the security assurance requirements for the TOE.

Security functional requirements components given in Section 6.1, expect FPT_EMSEC.1 which is explicitly stated, are drawn from Common Criteria Part 2 [2]

Some security functional requirements represent extensions to Common Criteria Part 2 [2]. Operations for assignment, selection and refinement have been made and are designated by an underline, in addition, where operations that were uncompleted in the PPs and performed in this Security Target, are also identified by *italic underlined* type

6.1 Security Functional Requirements

6.1.1 Cryptographic Support (FCS)

6.1.1.1 Cryptographic key management (FCS_CKM)

6.1.1.1.1 FCS_CKM.1

The TOE shall meet the requirement "Cryptographic key generation" as specified below.

FCS_CKM.1	**Cryptographic key generation**
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm *RSA and ECC*[2] and specified cryptographic key sizes *between 1024 bit, 2048, 3072 and 4096 bit in case of RSA, and 224, 256, 384 and 521 bit in case of ECC* [3]that meet the following: *PKCS#1 v2.2 [17] in case of RSA and [18] and [19] in case of ECC*[4]

6.1.1.1.2 FCS_CKM.4

The TOE shall meet the requirement "Cryptographic key destruction" as specified below.

FCS_CKM.4	**Cryptographic key destruction**
Hierarchical to:	No other components.

2 [assignment: *cryptographic key generation algorithm*]
3 [assignment: *cryptographic key sizes*]
4 [assignment: *list of standards*].

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.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting old key with new key*[5] that meets the following: *none*[6].

6.1.1.2 Cryptographic operation (FCS_COP)

6.1.1.2.1 FCS_COP.1

The TOE shall meet the requirement "Cryptographic operation" as specified below.

FCS_COP.1	**Cryptographic operation**
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
FCS_COP.1.1	The TSF shall perform digital signature-generation[7] in accordance with the specified cryptographic algorithm *RSA and ECC* [8] and cryptographic key sizes *1024, 2048, 3072 and 4096 bits (RSA) or 224, 256, 384 and 521 bit (ECC)*[9] that meet the following:*RSA CRT with hashing SHA-1 or SHA-2 and with padding PKCS#1 v1.5 as per Algorithms and parameters for algorithms[13]*[10] [2]

6.1.1.2.2 FCS_COP.1/ENC

The TOE shall meet the requirement "Cryptographic Operation (Encryption)" as specified below.

FCS_COP.1/ENC	**Cryptographic Operation (Encryption)**
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

5 [assignment: *cryptographic key destruction method*]
6 [assignment: *list of standards*]
7 [assignment: *list of cryptographic operations*]
8 [assignment: *cryptographic algorithm*]
9 [assignment: *cryptographic key sizes*]
10 [assignment: *list of standards*]

	FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ENC	The TSF shall perform *data encryption/decryption for Administrator and Signatory Authentication and Secure Messaging*[11] in accordance with a specified cryptographic algorithm *TDES CBC and AES*[12] and cryptographic key sizes *16, 24 and 32 bytes* [13]that meet the following: *FIPS PUB 46-3 Data Encryption Standard (DES)[20]*[14] [2]

6.1.1.2.3 FCS_COP.1/MAC

The TOE shall meet the requirement "Cryptographic Operation (MAC)" as specified below.

FCS_COP.1/MAC	**Cryptographic Operation (MAC)**
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
FCS_COP.1.1/MAC	The TSF shall perform *Message Authentication Code for Secure Messaging*[15] in accordance with a specified cryptographic algorithm *TDES MAC and AES* [16] and cryptographic key sizes *16, 24 and 32 bytes*[17] that meet the following: *FIPS PUB 46-3 Data Encryption Standard (DES)[20]*[18] [2]

6.1.2 User Data Protection (FDP)

The security attributes for the user, TOE components and related status are defined in Table 7

Table 7. Security Attributes for Access Control

Subject / Object	Security Attribute	Status
General Attribute		
S.User	Role	Administrator, Signatory
Initialisation Attribute		

11 [assignment: *list of cryptographic operations*]
12 [assignment: *cryptographic algorithm*]
13 [assignment: *cryptographic key sizes*]
14 [assignment: *list of standards*]
15 [assignment: *list of cryptographic operations*]
16 [assignment: *cryptographic algorithm*]
17 [assignment: *cryptographic key sizes*]
18 [assignment: *list of standards*]

Table 7. Security Attributes for Access Control*...continued*

Subject / Object	Security Attribute	Status
S.User	SCD / SVD Management	Authorized, Not Authorized
SCD	Secure SCD Import Allowed	No, Yes
SCD	SCD Idenftifier	Arbitrary Value (2 bytes)
Signature-Creation Attribute Group		
SCD	SCD operational	No, Yes
DTBS, DTBS/R	sent by an authorized SCA	No, Yes

The verification of the Security Attributes for Access Control is covered by SF.Access

6.1.2.1 Access control policy (FDP_ACC)

6.1.2.1.1 FDP_ACC.1/SVD_Transfer

The TOE shall meet the requirement "Subset access control (SVD Transfer)" as specified below.

FDP_ACC.1/ SVD_Transfer	**Subset access control (SVD Transfer)**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/ SVD_Transfer	The TSF shall enforce the SVD Transfer SFP[19] on 1. subjects: S.User, 2. objects: SVD, 3. operations: export[20]

Application Note: FDP_ACC.1/SVD_Transfer_SVD is only required to protect the exportation of the SVD as the SVD is never imported from an SSCD type 1 into the TOE.

6.1.2.1.2 FDP_ACC.1/SCD_Import

The TOE shall meet the requirement "Subset access control (SCD Import)" as specified below.

FDP_ACC.1/ SCD_Import	**Subset access control (SCD Import)**
Hierarchical to:	No other components.

19 [assignment: *access control SFP*]
20 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/ SCD_Import	The TSF shall enforce the SCD Import SFP[21] on 1. subjects: S.User, 2. objects: DTBS/R, SCD, 3. operations: import of SCD[22]

6.1.2.1.3 FDP_ACC.1/SCD/SVD_Generation

The TOE shall meet the requirement "Subset access control (SCD/SVD Generation)" as specified below.

FDP_ACC.1/SCD/ SVD_Generation	**Subset access control (SCD/SVD Generation)**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/SCD/ SVD_Generation	The TSF shall enforce the SCD/SVD_Generation_SFP[23] on 1. subjects: S.User, 2. objects: SCD, SVD, 3. operations: generation of SCD/SVD pair[24]

6.1.2.1.4 FDP_ACC.1/Signature_Creation

The TOE shall meet the requirement "Subset access control (Signature Creation)" as specified below.

FDP_ACC.1/ Signature_Creation	**Subset access control (Signature Creation)**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/ Signature_Creation	The TSF shall enforce the Signature creation SFP[25] on 1. subjects: S.User, 2. objects: DTBS/R, SCD 3. operations: signature creation[26]

21 [assignment: *access control SFP*]
22 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
23 [assignment: *access control SFP*]
24 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
25 [assignment: *access control SFP*]
26 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

6.1.2.2 Access control functions (FDP_ACF)

6.1.2.2.1 FDP_ACF.1/SCD/SVD_Generation

The TOE shall meet the requirement "Security attribute based access control (SCD/SVD Generation)" as specified below.

FDP_ACF.1/SCD/ SVD_Generation	**Security attribute based access control (SCD/SVD Generation)**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/SCD/ SVD_Generation	The TSF shall enforce the SCD/SVD Generation SFP [27] to objects based on the following: S.User is associated with the security attribute "SCD / SVD Management" [28].
FDP_ACF.1.2/SCD/ SVD_Generation	The TSF shall enforce the following rules to detmerin if any operation among controlled subjects and controlled objects is allowed: S.User with the security attribute "SCD / SVD Management" set to "authorised" is allowed to generate SCD/ SVD pair.[29]
FDP_ACF.1.3/SCD/ SVD_Generation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.[30]
FDP_ACF.1.4/SCD/ SVD_Generation	The TSF shall explicitly deny access of subjects to objects based on the rule: S.User is associated with the security attribute "SCD / SVD Management" set to "not authorised" is not allowed to generate SCD/SVD pair[31].

6.1.2.2.2 FDP_ACF.1/SVD_Transfer

The TOE shall meet the requirement "Security attribute based access control (SVD Transfer)" as specified below.

FDP_ACF.1/ SVD_Transfer	**Security attribute based access control (SVD Transfer)**
Hierarchical to:	No other components.

27 [assignment: *access control SFP*]
28 [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*].
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 authorise access of subjects to objects*].
31 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/ SVD_Transfer	The TSF shall enforce the SVD Transfer SFP [32] to objects based on the following: 1. the S.User is associated with the security attribute Role, 2. the SVD[33]
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: The user with the security attribute "role" set to "Administrator" or to "Signatory" is allowed to export SVD[34]
FDP_ACF.1.3/ SVD_Transfer	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[35].
FDP_ACF.1.4/ SVD_Transfer	The TSF shall explicitly deny access of subjects to objects based on the rule: none[36].

6.1.2.2.3 FDP_ACF.1/SCD_Import

The TOE shall meet the requirement "Security attribute based access control (SCD Import)" as specified below.

FDP_ACF.1/ SCD_Import	**Security attribute based access control (SCD Import)**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/ SCD_Import	The TSF shall enforce the SCD Import SFP [37] to objects based on the following: the S.User is associated with the security attribute "SCD/SVD Management" [38]
FDP_ACF.1.2/ SCD_Import	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled 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*].
35 [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].
36 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].
37 [assignment: *access control SFP*]
38 [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*].

	is allowed: S.User with the security attribute "SCD/SVD Management" set to "authorised" is allowed to import SCD. [39]
FDP_ACF.1.3/ SCD_Import	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[40].
FDP_ACF.1.4/ SCD_Import	The TSF shall explicitly deny access of subjects to objects based on the rule: S.User with the security attribute "SCD/SVD Management" set to "not authorised" is not allowed to import SCD.[41].

6.1.2.2.4 FDP_ACF.1/Signature_Creation

The TOE shall meet the requirement "Security attribute based access control (Signature Creation)" as specified below.

FDP_ACF.1/ Signature_Creation	**Security attribute based access control (Signature Creation)**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/ Signature_Creation	The TSF shall enforce the Signature_Creation SFP [42] to objects based on the following: 1. the S.User is associated with the security attribute "Role" and 2. the SCD with the security attribute "SCD Operational"[43]
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: User with the security attribute "role" set to "Signatory" is allowed to create digital signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "yes"[44]
FDP_ACF.1.3/ Signature_Creation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[45].

39 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].
40 [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].
41 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].
42 [assignment: *access control SFP*]
43 [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*].
44 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].
45 [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4/ Signature_Creation	The TSF shall explicitly deny access of subjects to objects based on the rules: S.User is not allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no"[46].

6.1.2.3 Data authentication (FDP_DAU)

6.1.2.3.1 FDP_DAU.2/SVD

The TOE shall meet the requirement "Data Authentication with Identity of Guarantor (SVD)" as specified below.

FDP_DAU.2/SVD	**Data Authentication with Identity of Guarantor (SVD)**
Hierarchical to:	FDP_DAU.1 Basic Data Authentication
Dependencies:	FIA_UID.1 Timing of Identification
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[47].
FDP_DAU.2.2/SVD	The TSF shall provide CGA[48] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

6.1.2.4 Import from outside of the TOE (FDP_ITC)

6.1.2.4.1 FDP_ITC.1/SCD

The TOE shall meet the requirement "Import of user data without security attributes (SCD)" as specified below.

FDP_ITC.1/SCD	**Import of user data without security attributes (SCD)**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation
FDP_ITC.1.1/SCD	The TSF shall enforce the SCD Import SFP[49] when importing user data, controlled under the SFP, from outside of the TOE.

46 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].
47 [assignment: *list of objects or information types*]
48 [assignment: *list of subjects*]
49 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

FDP_ITC.1.2/SCD	The TSF shall ignore any security attributes associated with the **SCD** when imported from outside the TOE
FDP_ITC.1.3/SCD	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *SCD shall be sent by an authorized SCD/SVD generation application from outside of the TOE.*[50]

6.1.2.5 Inter-TSF user data confidentiality transfer protection (FDP_UCT)

6.1.2.5.1 FDP_UCT.1/SCD

The TOE shall meet the requirement "Basic data exchange confidentiality (SCD)" as specified below.

FDP_UCT.1/SCD	**Basic data exchange confidentiality (SCD)**
Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_UCT.1.1/SCD	The TSF shall enforce the SCD Import SFP[51] to be able to receive[52] **SCD** in a manner protected from unauthorised disclosure.

6.1.2.6 Inter-TSF user data integrity transfer protection (FDP_UIT)

6.1.2.6.1 FDP_UIT.1/DTBS

The TOE shall meet the requirement "Data exchange integrity (DTBS)" as specified below.

FDP_UIT.1/DTBS	**Data exchange integrity (DTBS)**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

50 [assignment: *additional importation control rules*].
51 [assignment: access control SFP(s) and/or information flow control SFP(s)]
52 [selection: *transmit, receive*]

FDP_UIT.1.1/DTBS	The TSF shall enforce the Signature Creation SFP[53] to receive[54] user data in a protected manner from modification and insertion[55] errors.
FDP_UIT.1.2/DTBS	The TSF shall be able to determine on receipt of user data, whether modification and insertion[56] has occurred.

6.1.2.7 Residual information protection (FDP_RIP)

6.1.2.7.1 FDP_RIP.1

The TOE shall meet the requirement "Subset residual information protection" as specified below.

FDP_RIP.1	**Subset residual information protection**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of the resource from[57] the following objects: SCD, *VAD, RAD*[58]

6.1.2.8 Stored data integrity (FDP_SDI)

6.1.2.8.1 FDP_SDI.2/Persistent

Note: The following data persistently stored by TOE have the user data attribute "integrity checked persistent stored data" (integrity redundancy code):

1. SCD
2. SVD(if persistently stored by TOE)
3. *RAD*

The TOE shall meet the requirement "Stored data integrity monitoring and action (Persistent)" as specified below.

FDP_SDI.2/ Persistent	**Stored data integrity monitoring and action (Persistent)**
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring

53 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
54 [selection: *transmit, receive*]
55 [selection: *modification, deletion, insertion, replay*]
56 [selection: *modification, deletion, insertion, replay*]
57 [selection: *allocation of the resource to, deallocation of the resource from*]
58 [assignment: *list of objects*]

Dependencies:	No dependencies.
FDP_SDI.2.1/ Persistent	The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[59] on all objects, based on the following attributes: *integrity checked persistent data*[60].
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 Signatory about integrity error[61]

6.1.2.8.2 FDP_SDI.2/DTBS

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

The TOE shall meet the requirement "Stored data integrity monitoring and action (DTBS)" as specified below.

FDP_SDI.2/DTBS	**Stored data integrity monitoring and action (DTBS)**
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.
FDP_SDI.2.1/DTBS	The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[62] on all objects, based on the following attributes: integrity checked stored data[63].
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 Signatory about integrity error[64]

6.1.3 Identification and Authentication (FIA)

6.1.3.1 Authentication failures (FIA_AFL)

6.1.3.1.1 FIA_AFL.1

The TOE shall meet the requirement "Authentication failure handling" as specified below.

59 [assignment: *integrity errors*]
60 [assignment: *user data attributes*]
61 [assignment: *action to be taken*]
62 [assignment: *integrity errors*]
63 [assignment: *user data attributes*]
64 [assignment: *action to be taken*]

FIA_AFL.1	**Authentication failure handling**
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when *5 consecutive*[65] unsuccessful authentication attempts occure related to: consecutive failed authentication attempts[66]
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met[67], the TSF shall block RAD[68]

6.1.3.2 User authentication (FIA_UAU)

6.1.3.2.1 FIA_UAU.1

The TOE shall meet the requirement "Timing of Authentication" as specified below.

FIA_UAU.1	**Timing of Authentication**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
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, 4. Establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD, 5. Establishing a trusted path between the TOE and a SSCD of Type 1 my means of TSF required by FTP_ITC.1/SCD[69] on behalf of the user to be performed before the user is authenticated.
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.

65 [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
66 [assignment: *list of authentication events*]
67 [selection: *met, surpassed*
68 [assignment: *list of actions*]
69 [assignment: *list of TSF mediated actions*]

Application Note: The user mentioned in component FIA_UAU.1.1 is the local user using the trusted path provided between the SGA in the TOE environment and the TOE.

6.1.3.3 Authentication proof of identity (FIA_API)

6.1.3.3.1 FIA_API.1

The TOE shall meet the requirement "Authentication proof of identity" as specified below.

FIA_API.1	**Authentication proof of identity**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide a 1. *PACE authentication according to [20]* 2. *Chip Authentication according to EAC v1 [20]* 3. *Chip Authentication according to EAC v2 [21] [22]*[70] to prove the identity of the SSCD[71]

Application Note: The ST writer shall perform the missing operation in the element FIA_API.1.1. Via the authentication mechanism to be assigned here the TOE has to be able to authenticate itself as SSCD to the CGA, using authentication data implemented in the TOE during pre-initialisation phase.

6.1.3.4 User identification (FIA_UID)

6.1.3.4.1 FIA_UID.1

The TOE shall meet the requirement "Timing of Identification" as specified below.

FIA_UID.1	**Timing of Identification**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow 1. Self test according to FPT_TST.1 2. *Establishing a trusted channel between the TOE and a SSCD of Type 1 by means of TSF required by FTP_ITC.1/SCD*[72]

70 [assignment: *authentication mechanism*]
71 [assignment: *authorized user or rule*]
72 [assignment: *list of TSF-mediated actions*]

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

6.1.4 Security Management (FMT)

6.1.4.1 Management of functions in TSF (FMT_MOF)

6.1.4.1.1 FMT_MOF.1/Sign

The TOE shall meet the requirement "Management of security functions behaviour (Sign)" as specified below.

FMT_MOF.1/Sign	**Management of security functions behaviour (Sign)**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security Roles FMT_SMF.1 Specification of Management Functions
FMT_MOF.1.1/Sign	The TSF restrict the ability to enable[73] the functions signature-creation function[74] to Signatory[75]

6.1.4.2 Management of security attributes (FMT_MSA)

6.1.4.2.1 FMT_MSA.1/Admin

The TOE shall meet the requirement "Management of security attributes (Admin)" as specified below.

FMT_MSA.1/Admin	**Management of security attributes (Admin)**
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
FMT_MSA.1.1/ Admin	The TSF shall enforce the SCD Import SFP and SCD/SVD generation SFP[76] to restrict the ability to modify[77] the security

73 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
74 [assignment: *list of functions*]
75 [assignment: *the authorised identified roles*]
76 [assignment: *access control SFP(s), information flow control SFP(s)*]
77 [selection: *change_default, query, modify, delete, [assignment: other operations]*]

attributes SCD/SVD management and Secure SCD import allowed[78] to Administrator[79].

6.1.4.2.2 FMT_MSA.1/Signatory

The TOE shall meet the requirement "Management of security attributes (Signatory)" as specified below.

FMT_MSA.1/ Signatory	**Management of security attributes (Signatory)**
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
FMT_MSA.1.1/ Signatory	The TSF shall enforce the Signature-creation SFP[80] to restrict the ability to modify[81] the security attributes SCD operational [82] to Signatory[83].

6.1.4.2.3 FMT_MSA.2

The TOE shall meet the requirement "Secure security attributes" as specified below.

FMT_MSA.2	**Secure security attributes**
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
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for *all security attributes*[84]

6.1.4.2.4 FMT_MSA.3

The TOE shall meet the requirement "Static attribute initialization" as specified below.

FMT_MSA.3	**Static attribute initialization**

78 [assignment: *list of security attributes*]
79 [assignment: *the authorised identified roles*]
80 [assignment: *access control SFP(s), information flow control SFP(s)*]
81 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
82 [assignment: *list of security attributes*]
83 [assignment: *the authorised identified roles*]
84 [assignment: *list of security attributes*]

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the SCD Import SFP, SCD/SVD Generation SFP, SVD Transfer SFP and Signature-creation SFPs[85] to provide restrictive[86] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the Administrator[87] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.2.5 FMT_MSA.4

The TOE shall meet the requirement "Static attribute value inheritance" as specified below.

FMT_MSA.4	**Static attribute value inheritance**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control, FDP_IFC.1 Subset information flow control
FMT_MSA.4.1	The TSF shall use the following rules to set the value of security attributes: 1. If Administrator successfully generates an SCD/SVD pair without Signatory being authenticated the security attribute "SCD operational" of the SCD shall be set to "no" as a single operation. 2. If Signatory successfully generates an SCD/SVD pair the security attribute "SCD operational" of the SCD shall be set to "yes" as a single operation. 3. If Administrator imports SCD while Signatory is not currently authenticated, the security attribute "SCD operational" of the SCD shall be set to "no" after import of the SCD as a single operation 4. If Administrator imports SCD while Signatory is currently authenticated, the security attribute "SCD operational" of the SCD shall be set to "yes" after import of the SCD as a single operation. [88]

85 [assignment: *access control SFP, information flow control SFP*]
86 [selection, choose one of: *restrictive, permissive, [assignment: other property]*]
87 [assignment: *the authorised identified roles*]
88 [assignment: *rules for setting the values of security attributes*]

6.1.4.3 Management of TSF data (FMT_MTD)

6.1.4.3.1 FMT_MTD.1/Admin

The TOE shall meet the requirement "Management of TSF data (Admin)" as specified below.

FMT_MTD.1/Admin	**Management of TSF data (Admin)**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/ Admin	The TSF shall restrict the ability to create[89] the RAD [90] to Administrator[91].

Application Note: The RAD can be unblocked by the Signatory after presentation of the PUK by the Signatory.

6.1.4.3.2 FMT_MTD.1/Signatory

The TOE shall meet the requirement "Management of TSF data (Signatory)" as specified below.

FMT_MTD.1/ Signatory	**Management of TSF data (Signatory)**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/ Admin	The TSF shall restrict the ability to modify *or unblock*[92] the RAD [93] to Signatory[94].

6.1.4.4 Specification of management functions (FMT_SMF)

6.1.4.4.1 FMT_SMF.1

The TOE shall meet the requirement "Specification of Management Functions" as specified below.

89 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
90 [assignment: *list of TSF data*]
91 [assignment: *the authorised identified roles*]
92 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
93 [assignment: *list of TSF data*]
94 [assignment: *the authorised identified roles*]

FMT_SMF.1	**Specification of Management Functions**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
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, 4. SCD operational 5. Change the default value of the security attribute SCD Identifier, Access Condition Management [95]

6.1.4.5 Security management roles (FMT_SMR)

6.1.4.5.1 FMT_SMR.1

The TOE shall meet the requirement "Security roles" as specified below.

FMT_SMR.1	**Security roles**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles Administrator and Signatory[96].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.1.5 Protection of the TSF (FPT)

6.1.5.1 TOE emanation (FMT_EMS)

6.1.5.1.1 FPT_EMS.1

The TOE shall meet the requirement "TOE Emanation" as specified below.

FPT_EMS.1	**TOE Emanation**
Hierarchical to:	No other components.

95 [assignment: *list of management functions to be provided by the TSF*]
96 [assignment: the authorised identified roles]

Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit *information of IC Power consumption*[97] in excess of *State of the Art values*[98] enabling access to RAD and SCD
FPT_EMS.1.2	The TOE shall ensure *any user*[99] is unable to use the following interface *physical chip contacts and contactless I/O*[100] to gain access to RAD[101] and SCD[102]

Application Note: 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. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission. Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

6.1.5.2 Fail secure (FPT_FLS)

6.1.5.2.1 FPT_FLS.1

The TOE shall meet the requirement as specified below.

FPT_FLS.1	**Failure with preservation of secure state**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1. self-test according to FPT_TST fails 2. *IC environmental sensors detection (Temperature out of range, Supply Voltage of chip)*

97 [assignment: *types of emissions*
98 [assignment: *specified limits*]
99 [assignment: *type of users*]
100 [assignment: *type of connection*]
101 [assignment: *list of types of TSF data*]
102 [assignment: *list of types of user data*]

3. *IC internal error detection sensors failure (Parity, RNG operation)* [103]

Refinement: The failed self-test above also covers related “circumstances”. The TOE prevents failures for the “circumstances” defined above.

6.1.5.3 TSF physical protection (FPT_PHP)

6.1.5.3.1 FPT_PHP.1

The TOE shall meet the requirement "Passive detection of physical attack" as specified below.

FPT_PHP.1	**Passive detection of physical attack**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.1.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF
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.

6.1.5.3.2 FPT_PHP.3

The TOE shall meet the requirement "Resistance to physical attack" as specified below.

FPT_PHP.3	**Resistance to physical attack**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF shall resist *Environment attacks (clock frequency and voltage tampering) and Intrusive attacks (penetration of the module protective layers)*[104] to the *IC Hardware*[105] by responding automatically such that the SFRs are always enforced.

6.1.5.4 TSF self test (FPT_TST)

103 [assignment: *list of types of failures in the TSF*]
104 [assignment: *physical tampering scenarios*]
105 [assignment: *list of TSF devices/elements*

6.1.5.4.1 FPT_TST.1

The TOE shall meet the requirement "TSF testing" as specified below.

FPT_TST.1	**TSF testing**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suit of self-tests *during initial start-up or before running a secure operation*[106] to demonstrate the correct operation of the TSF[107]
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data[108]
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of *TSF (stored executable code)*[109]

Application Note: Crypto Self-tests are performed by the Operating System during start-up.

6.1.6 Trusted path/channels (FPT)

6.1.6.1 Inter-TSF trusted channel (FTP_ITC)

6.1.6.1.1 FTP_ITC.1/SCD

The TOE shall meet the requirement "Inter-TSF trusted channel (SCD)" as specified below.

FTP_ITC.1/SCD	**Inter-TSF trusted channel (SCD)**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/SCD	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its

106 [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions[assignment: condictions under which self test should occur]*]
107 [selection: *assignment: parts of the TSF], the TSF*]
108 [selection: *assignment: parts of TSF data], TSF data*]
109 [selection: *assignment: parts of TSF], TSF*]

end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/SCD The TSF shall permit another trusted IT product[110] to initiate communication via the trusted channel.

FTP_ITC.1.3/SCD The TSF shall initiate communication via the trusted channel for

1. Data exchange integrity according to FDP_UCT.1/SCD
2. *SCD Import*[111]

Refinement: *The mentioned remote trusted IT products are: an authorized SCD/SVD generation application for SCD import, the CGA for the SVD export, and the SCA for DTBS Import.*

Application Note: The component FPT_ITC.1 requires the TSF to support a trusted channel established to another trusted IT product generating the SCD/SVD pair for import the SCD as described by FDP_UCT.1/ SCD. The ST writer shall perform the missing operations in the element FTP_ITC.1.3/SCD. If the TSF does not enforce the use of trusted channel for other functions the operation in the element FTP_ITC.1.3/ SCD is "none"

6.1.6.1.2 FTP_ITC.1/SVD

The TOE shall meet the requirement "Inter-TSF trusted channel (SVD)" as specified below.

FTP_ITC.1/SVD **Inter-TSF trusted channel (SVD)**

Hierarchical to: No other components.

Dependencies: No dependencies.

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.

FTP_ITC.1.2/SVD The TSF shall permit another trusted IT product[112] to initiate communication via the trusted channel.

FTP_ITC.1.3/SVD The TSF **or the CGA** shall initiate communication via the trusted channel for

110 [selection: *the TSF, another trusted IT product*]
111 [assignment: *list of functions for which a trusted channel is required*]
112 [selection: *the TSF, another trusted IT product*]

1. data Authentication with Identity of Guarantor according to FIA_API.1 and FDP_DAU.2/SVD,

Application Note: The component FPT_ITC.1/SVD requires the TSF to enforce a trusted channel established by the CGA to export the SVD to the CGA. The ST writer shall perform the missing operations in the element FTP_ITC.1.3. If the TSF does not enforce the use of trusted channel for other functions the operation in the element FTP_ITC.1.3 is “none”.

Application Note: If the ST writer requires the TSF to support (not to enforce) a trusted channel established by the CGA to export the SVD to the CGA than he or she shall use the core PP SSCD KG and include a similar component FPT_ITC.1/SVD with assignment “none” in the element FPT_ITC.1.3/SVD.

6.1.6.1.3 FTP_ITC.1/VAD

The TOE shall meet the requirement "Inter-TSF trusted channel - TC Human Interface Device" as specified below.

FTP_ITC.1/VAD	**Inter-TSF trusted channel - TC Human Interface Device**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/VAD	The TSF shall provide a communication channel between itself and another trusted IT product **HID** 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.
FTP_ITC.1.2/VAD	The TSF shall permit the remote trusted IT product[113] to initiate communication via the trusted channel.
FTP_ITC.1.3/VAD	The TSF **or the HID** shall initiate communication via the trusted channel for 1. User authentication according to FIA_UAU.1,

Application Note: The component FTP_ITC.1/VAD requires the TSF to support a trusted channel established by the HID to send the VAD. The ST writer shall perform the missing operations in the element FTP_ITC.1.3. If the TSF does not enforce the use of trusted channel for other functions the operation in the element FTP_ITC.1.3 is “none”. Note the VAD needs protection depending on the authentication methods employed: VAD for authentication by knowledge needs protection in confidentiality; VAD for biometric authentication may need protection in integrity only.

113 [selection: *the TSF, another trusted IT product*]

6.1.6.1.4 FTP_ITC.1/DTBS

The TOE shall meet the requirement "Inter-TSF trusted channel - Signature creation application" as specified below.

FTP_ITC.1/DTBS	**Inter-TSF trusted channel - Signature creation application**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/DTBS	The TSF shall provide a communication channel between itself and another trusted IT product **SCA** 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.
FTP_ITC.1.2/DTBS	The TSF shall permit the remote trusted IT product[114] to initiate communication via the trusted channel.
FTP_ITC.1.3/DTBS	The TSF **or the SCA** shall initiate communication via the trusted channel for 1. signature creation,

Application Note: The component FTP_ITC.1/DTBS requires the TSF to support a trusted channel established by the SCA to send the DTBS. The ST writer shall perform the missing operations in the element FTP_ITC.1.3. If the TSF does not enforce the use of trusted channel for other functions the operation in the element FTP_ITC.1.3 is “none”.

6.2 Security Assurance Requirements

The following table lists all security assurance components that are valid for this Security Target.

Table 8. Security Assurance Requirements according to EAL5 augmented

Name		Title
ADV: Devlopment	ADV_ARC.1	Security architecture description
	ADV_FSP.5	Complete semi-formal functional specification with additional error information
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	Well-structured internals
	ADV_TDS.4	Semiformal modular design
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures

114 [selection: *the TSF, another trusted IT product*]

Table 8. Security Assurance Requirements according to EAL5 augmented*...continued*

Name		Title
ALC: Lifecycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.5	Development tools CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.2	Compliance with implementation standards
ASE: Security Target evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_ECD.1	Extendend components definition
	ASE_REQ.2	Derived security requirements
	ASE_TSS.1	TOE summary specification
ATE: Test	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	Testing: modular design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability Assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

6.3 Security Assurance Requirements Rationale

The EAL5 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, although rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL5 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL5 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

Augmentation results from the selection of:

ALC_DVS.2 *Life-cycle support- Sufficiency of security measures*

The selection of the component ALC_DVS.2 provides a higher assurance with regards to the security measures providing the necessary level of protection to maintain the confidentiality and integrity of the TOE.

The component ALC_DVS.2 has no dependencies.

AVA_VAN.5 *Vulnerability Assessment - Advanced methodical vulnerability analysis*

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.

The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_FSP.4 Complete functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ATE_DPT.1 Testing: basic design

All of these are met or exceeded in the EAL5 assurance package.

6.4 Security Requirements Rationale

6.4.1 Security Requirement Coverage

The following table indicates the association of the security requirements and the security objectives of the TOE. Some requirements correspond to the security objectives of the TOE in combination with other objectives.

Table 9. Mapping of security problem definition to security objectives

TOE SFRs / TOE Security Objectives	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.SCD_Auth_Imp	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp
FCS_CKM.1	x		x	x	x											
FCS_CKM.4	x				x											
FCS_COP.1	x					x										
FCS_COP.1/ENC						x										
FCS_COP.1/MAC						x										
FDP_ACC.1/SCD/SVD_ Generation	x	x														
FDP_ACC.1/SVD_Transfer	x													x		
FDP_ACC.1/SCD_Import	x											x				
FDP_ACC.1/Signature_ Creation	x						x									

Table 9. Mapping of security problem definition to security objectives*...continued*

TOE SFRs / TOE Security Objectives	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.SCD_Auth_Imp	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp
FDP_ACF.1/SCD/SVD_ Generation	x	x														
FDP_ACF.1/SVD_Transfer	x													x		
FDP_ACF.1/SCD_Import	x	x														
FDP_ACF.1/Signature_ Creation	x						x									
FDP_ITC.1/SCD	x															
FDP_UCT.1/SCD	x															
FDP_RIP.1					x		x									
FDP_SDI.2/Persistent				x	x	x										
FDP_SDI.2/DTBS							x	x								
FDP_UIT.1/DTBS																x
FDP_DAU.2/SVD														x		
FIA_AFL.1							x									
FIA_UAU.1		x					x					x	x			
FIA_API.1													x			
FIA_UID.1		x					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									
FMT_MTD.1/Admin	x						x									
FMT_MTD.1/Signatory	x						x									
FMT_SMR.1	x						x									
FMT_SMF.1	x			x			x									
FPT_EMSEC.1					x				x							
FPT_FLS.1					x											
FPT_PHP.1										x						
FPT_PHP.3					x						x					

Table 9. Mapping of security problem definition to security objectives*...continued*

TOE SFRs / TOE Security Objectives	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.SCD_Auth_Imp	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp
FPT_TST.1	x				x	x										
FPT_ITC.1/SCD	x				x											
FPT_ITC.1/SVD														x		
FTP_ITC.1/VAD															x	
FTP_ITC.1/DTBS																x

6.4.2 Security Requirements Sufficiency

OT.Lifecycle_Security (*Lifecycle security*) is provided by the SFR as follows:

The SCD import is controlled by TSF according to FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import and FDP_ITC.1/SCD. The confidentiality of the SCD is protected during import according to FDP_UCT.1/SCD in the trusted channel FTP_ITC.1/SCD.

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 secure SCD usage is ensured cryptographically according to FCS_COP.1. The SCD usage is controlled 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. The FMT_SMF.1 and FMT_SMR.1 defines security management rules and functions. The test functions FPT_TST.1 provides failure detection throughout the lifecycle. The SFR FCS_CKM.4 ensures a secure SCD destruction.

OT.SCD_Auth_Imp (*Authorized SCD import*) is provided by the security functions specified by the following SFR. FIA_UID.1 and FIA_UAU.1 ensure that the user is identified and authenticated before SCD can be imported. FDP_ACC.1/SCD_Import and FDP_ACF.1/SCD_Import ensure that only authorised users can import SCD.

OT.SCD/SVD_Gen (*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 authorised 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 initialisation. The SFR FMT_MSA.4 defines rules for inheritance of the security attribute “SCD operational” of the SCD.

OT.SCD_Unique (*Uniqueness of the signature-creation data*) implements the requirement of practically unique SCD as laid down in the directve [15]Annex III, paragraph 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1.

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.

OT.SCD_Secrecy (*Secrecy of signature creation data*) is provided by the security functions specified by the following SFR. FDP_UCT.1/SCD and FTP_ITC.1/SCD ensures the confidentiality for SCD import. 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 used for signature creation and that destruction of SCD leaves no residual information.

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_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).

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

OT.Sig_Secure (*Cryptographic security of the electronic signature*) is provided by the cryptographic algorithms specified by FCS_COP.1, which ensure the cryptographic robustness of the signature algorithms. FCS_COP.1/ENC and FCS_COP.1/MAC strengthen Secure Messaging protocol with regards to integrity and confidentiality of data exported from the TOE. Thus OT.Sig_Secure is supported with regards to withstand attacks trying to forge signature data. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE and FPT_TST.1 ensures self-tests ensuring correct signature creation.

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

The FIA_UAU.1 and FIA_UID.1 that ensure that no signature creation 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. The 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.

FDP_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature-creation process).

FMT_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory.

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.1/Signatory, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4. FMT_MOF.1 ensures that only the signatory can enable/disable the signature creation function. 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.

Furthermore, the security functionality specified by FDP_RIP.1 will ensure that no attacker can get hold of the SCD (to create signatures outside the TOE) once SCD have been deleted by the legitimate signatory.

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

OT.EMSEC_Design (*Provide physical emanations security*) covers that no intelligible information is emanated. This is provided by FPT_EMSEC.1.1.

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

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

OT.TOE_SSCD_Auth (*Authentication proof as SSCD*) requires the TOE to provide security mechanisms to identify and to authenticate themselves as SSCD, which is directly provided by FIA_API.1 (Authentication Proof of Identity). The SFR FIA_UAU.1 allows (additionally to the core PP SSCD KG) establishment of the trusted channel before (human) user is authenticated.

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 CG

OT.TOE_TC_VAD_Imp (*Trusted channel of TOE for VAD import*) is provided by FTP_ITC.1/VAD to provide a trusted channel to protect the VAD provided by the HID to the TOE.

OT.TOE_TC_DTBS_Imp (*Trusted channel of TOE for DTBS*) is provided by FTP_ITC.1/DTBS to provide a trusted channel to protect the DTBS provided by the SCA to the TOE and by FDP_UIT.1/DTBS, which requires the TSF to verify the integrity of the received DTBS.

7 TOE Summary Specification

7.1 SF.Access Control

This function checks that for each operation initiated by a user, the security attributes for user authorization (FMT_SMR.1) and data communication required are satisfied.

The function includes:

Control over the authorization of Administrator to:

- Create an initial SCD/SVD Key Pair
  - Import SCD with fixed SVD (FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import) from an authorised SCD/SVD generation application
  - Generate the SCD/SVD key pair
  - Export SVD (FDP_ACC.1/SVD_Transfer, FDP_ACF.1/SVD_Transfer)
- Manage the SCD/SVD security attributes after the key pair is created (imported or generated)
- – “SCD/SVD management” is set to "not authorized" (FMT_MSA.1/Admin, FMT_SMF.1)
  - “SCD Operational” is set to “No” (FMT_MSA.3)
  - Security attributes management according to FTM_MSA.4
- Create the RAD during personalisation (FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation)

Control over the authorization of Signatory to:

- Activate the SCD and set its operational state to “Yes” (FMT_MSA.1/Signatory, FMT_SMF.1)
- Import a new SCD (FDP_ITC.1/SCD)
- Generate a new SCD/SVD key pair
- Export SVD (FDP_ACC.1/SVD Transfer SFP, FDP_ACF.1/SVD_Transfer)
- Sign DTBS data sent by an authorized SCA (FDP_ACC.1/Signature-creation, FDP_ACF.1/Signature-creation, FMT_MOF.1). Any security attributes associated with the DTBS are ignored
- Unblock and modify the RAD (FMT_MTD.1/Administrator, FMT_SMF.1)

Control over the enforcement of secure messaging over:

- Export of the SVD
- Importation of the SCD (FTP_ITC.1/SCD)

7.2 SF.Administration

In Initialization Phase (informative, covered by ALC family), this TSF provides Card initialization and pre-personalization services as per GlobalPlatform. This includes but is not restricted to card initialization, patch loading, applet installation and instantiation.

When the TOE is ready to be personalized, the Administrator will create the authentication data for the Personalization Phase within the Applet and terminate this manufacturing stage by disabling the card content loading and installation functions.

In Personalization Phase, the Administrator is identified through the relevant access rights during the initialization and personalization of the TOE (FMT_SMF.1).

In Usage phase, the Administrator could also use this authentication method to set TERMINATE the TOE. (FMT_SMF.1)

7.3 SF.Signatory Authentication

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

Signatory Authentication: RAD

TSF mediated actions are not allowed by the TOE before the user is identified (FIA_UID.1), authenticated and associated to the role of Signatory (FDP_ACF.1/ Signature-Creation).

The authentication of the Signatory is made through validation of the RAD by the TOE (FIA_UAU.1). This is only possible if the RAD allows remaining attempts (FIA_AFL.1): each failed attempt to authenticate is counted and when maximum amount of consecutive attempts failure is reached RAD is blocked. A successful authentication resets the counter and an unblocking mechanism is provided (FMT_MTD.1/Signatory).

The RAD can be a PIN or a Key, and RAD validation consists of:

- in case of a RAD-PIN, presentation of the VAD and comparison with the stored RAD,
- in case of a RAD-Key, achievement of a challenge-response authentication (FCS_COP.1/ENC)

Signatory data characteristics:

Table 10. Signatory Data Characteristics

Data	Type	Length	Max Retry	Purpose of Verification
RAD	Pin	>= 6 bytes	5	Authenticate the Signatory
	TDES Key	16 bytes	5	
PUK	PIN	>= 6 bytes	5	Unblock RAD-PIN (i.e. Reset Retry Counter)

IC power variation emanation is below state of the art values, and physical access to the RAD is protected during this SF activity (FPT_EMS.1).

7.4 SF.Signature Creation

This TSF is responsible for signing DTBS data using the SCD by the Signatory, following successful authentication of the Signatory.

The SF generates digital signatures using RSA and ECC with key sizes 1024, 2048, 3072 and 4096 bit in case of RSA and 224, 256, 384 and 521 bit in case of ECC (FMT_MSA.2, FCS_COP.1), as well as SHA-1 and SHA-2 hashing calculated by the host. The signature is calculated based on PKCS#1 version 1.5 [16].

A hash value calculated over the DTBS is sent to the TOE by the IT Environment.

The integrity of the DTBS representation is maintained through the use of SF.Secure Messaging (FDP_SDI.2/DTBS).

IC power variation emanation is limited to below state of the art values, and physical access to the SCD is protected during this SF activity (FPT_EMS.1).

7.5 SF.Secure Messaging

Commands and responses are exchanged between the TOE and the external device. This TSF provides a secure communication between legitimate end points both of the TOE and the external device.

Various data and processes such as DTBSs, signatures, public keys, identification and authentication data, SVD Transfer or other user data are embedded in command and response frames. The SF.Secure Messaging function is capable of providing a secure communication channel between legitimate end points both of the TOE and the external device. The secure communication channels are supported with cryptographic functions and provide for 4 distinct channels (TOE and authorized SCD/SVD generation application, TOE and CGA, TOE and SCA, TOE and User) logically distinct from each other and other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

This function is responsible for confidentiality and data authentication. Confidentiality is ensured through the encryption of communication data by symmetric cryptography by the use 3DES operations (FCS_COP.1/ENC). Data authentication and integrity is achieved by calculating of a cryptographic checksum (MAC) (FCS_COP.1/MAC).

The SCD/SVD Generation application, CGA, SCA and local user are allowed to initiate the communication with the TOE through via a trusted channel

TOE and SCD/SVD Generation application

During SCD Import (FTP_ITC/SCD), a trusted channel between the TOE and the SCD/SVD Generation application is established with secure messaging. Secure Messaging shall be setup to prevent disclosure of the imported SCD (FDP_UCT.1/SCD).

TOE and CGA

During SVD export from the TOE to the CGA, a trusted channel between the TOE and the CGA is established with secure messaging. Secure messaging maintains the integrity of the exported SVD. The SVD is exported without associated security attributes.

TOE and SCA

During import of the DTBS from the SCA to the TOE, a trusted channel, through secure messaging, is established between the SCA and the TOE. Secure Messaging maintains the integrity of the DTBS during import.

TOE and User

During the change of RAD secure messaging is enforced (FMT_SMF.1)

7.6 SF.Crypto

This Security Function is responsible for providing cryptographic support to all the other Security Functions including secure key generation and operations on data such as encrypt and sign:.

- Secure generation of asymmetric Key Pair (FCS_CKM.1, FMT_MSA.2), key generation is protected against SPA, Timing attacks, and electromagnetic emanation (FPT_EMS.1) and includes Key Pair Correspondence verification (FCS_COP.1): RSA

key pair with length from 1024 to 4096 bits and ECC key pair with length from 224 to 521 bits. This mechanism involves underlying cryptography:
  - The random number generator of the IC is used by the TOE whenever the generation of a nonce is required.
  - Adequate number of Rabin Miller test rounds is performed in addition to GCD test in order to ensure correct generation of primes in case of RSA.
- Data hashing using SHA-1, or SHA-2 (FCS_COP.1)
- Digital Signature generation with RSA CRT Key Pair of lengths 1024 to 4096 bit with PKCS#1 v1.5, and ECC Key Pair of lengths 224 to 521 bit (FCS_COP.1)
- TDES (2 Key) and AES with 128, 192 and 256 bit key length (FCS_COP.1/ENC, FCS_COP.1/MAC)
- Secure destruction of cryptographic key secret or private material (FCS_CKM.4).

This TSF enforces protection of Key material during cryptographic functions processing and Key Generation, against state-of-the-art attacks, including IC power consumption analysis (FPT_EMS.1)

7.7 SF.Protection

This Security Function is responsible for protection of the TSF data, user data, and TSF functionality. The SF.Protection function is composed of software implementations of test and security functions including:

- Performing self tests of the TOE at each power-up (FPT_TST.1)
- Deleting authentication resources (Biometrics, PINs, secret and private keys) when relevant memory is de-allocated (FCS_CKM.4, FDP_RIP.1)
- Validating the integrity of all stored cryptographic keys and PINs before use (FDP_SDI.2/Persistent) and informing the Terminal when such validation fails (FPT_TST.1).
- Performing a set of test to verify that the underlying cryptographic algorithms are operating correctly (FPT_TST.1).
- Initializing memory after reset
- Initializing memory of de-allocated data
- Preserving secure state after sensitive processing failure (RNG, EEPROM handling) or potential physical tampering or intrusion detection (FPT_FLS.1, FPT_PHP.1, FPT_PHP.3)

This TSF prevents re-activation of de-activated or disabled or terminated mechanisms: the code area and data area are protected.

7.8 TOE Summary Specifications Rationale

The following table covers the mapping between TSFR and TSF:

Table 11. Mapping Security Functional Requirements to Security Functions

TOE SFRs / TOE Security Functions	SF.Access_Control	SF.Administration	SF.Signatory_Authentication	SF.Signature_Creation	SF.Secure_Messaging	SF.Crypto	SF.Protection
FCS_CKM.1						x	
FCS_CKM.4						x	x
FCS_COP.1				x		x	
FCS_COP.1/ENC		x	x		x	x	
FCS_COP.1/MAC					x	x	
FDP_ACC.1/SCD/SVD_Generation	x						
FDP_ACC.1/SVD_Transfer	x						
FDP_ACC.1/SCD_Import	x						
FDP_ACC.1/Signature_Creation	x						
FDP_ACF.1/SCD/SVD_Generation	x						
FDP_ACF.1/SVD_Transfer	x						
FDP_ACF.1/SCD_Import	x						
FDP_ACF.1/Signature_Creation	x						
FDP_ITC.1/SCD	x						
FDP_UCT.1/SCD					x		
FDP_RIP.1							x
FDP_SDI.2/Persistent							x
FDP_SDI.2/DTBS					x		
FIA_AFL.1			x				
FIA_UAU.1		x	x				
FIA_UID.1			x				
FMT_MOF.1	x						
FMT_MSA.1/Admin	x						
FMT_MSA.1/Signatory	x						
FMT_MSA.2				x		x	
FMT_MSA.3	x						
FMT_MSA.4	x						
FMT_MTD.1/Admin	x		x				
FMT_MTD.1/Signatory	x		x				
FMT_SMR.1		x	x				

Table 11. Mapping Security Functional Requirements to Security Functions*...continued*

TOE SFRs / TOE Security Functions	SF.Access_Control	SF.Administration	SF.Signatory_Authentication	SF.Signature_Creation	SF.Secure_Messaging	SF.Crypto	SF.Protection
FMT_SMF.1	x	x			x		x
FPT_EMSEC.1		x	x	x		x	
FPT_FLS.1							x
FPT_PHP.1							x
FPT_PHP.3							x
FPT_TST.1							x
FPT_ITC.1/SCD	x				x		

8 Additional Rationale

8.1 Dependencies Rationale

8.1.1 SAR Dependencies

The functional and assurance requirements dependencies for the TOE are completely fulfilled.

Table 12. Dependencies of Security Assurance Requirements (Security Target)

Assurance Requirement	Dependencies
ADV_ARC.1	ADV_FSP.5, ADV_TDS.4
ADV_FSP.5	ADV_TDS.4, ADV_IMP.1
ADV_IMP.1	ADV_TDS.4, ALC_TAT.2
ADV_INT.2	ADV_IMP.1, ADV_TDS.4, ALC_TAT.2
ADV_TDS.4	ADV_FSP.5
AGD_OPE.1	ADV_FSP.5
AGD_PRE.1	No dependencies
ALC_CMC.4	ALC_CMS.5, ALC_DVS.1, ALC_LCD.1
ALC_CMS.5	No dependencies
ALC_DEL.1	No dependencies
ALC_DVS.2	No dependencies
ALC_LCD.1	No dependencies
ALC_TAT.1	ADV_IMP.1
ASE_CCL.1	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No dependencies
ASE_INT.1	No dependencies
ASE_OBJ.2	ASE_SPD.1
ASE_REQ.2	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No dependencies
ASE_TSS.1	ADV_FSP.5, ASE_INT.1, ASE_REQ.2
ATE_COV.2	ADV_FSP.5, ATE_FUN.1
ATE_DPT.3	ADV_ARC.1, ADV_TDS.4, ATE_FUN.1
ATE_FUN.1	ATE_COV.2
ATE_IND.2	ADV_FSP.5, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
ATA_VAN.5	ADV_ARC.1, ADV_FSP.5, ADV_TDS.4, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1

8.1.2 Justification of Unsupported Dependencies

All dependencies are supported.

8.1.3 SFR Dependencies

The functional and assurance requirements dependencies for the TOE are completely fulfilled.

Table 13. Dependencies of Security Functional Requirements

SFR	Dependencies
FCS_CKM.1	FCS_COP.1, FCS_CKM.4
FCS_CKM.4	FCS_CKM.1
FCS_COP.1	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/ENC	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/MAC	FCS_CKM.1, FCS_CKM.4
FDP_ACC.1/SCD/SVD_ Generation	FDP_ACF.1/SCD/SVD_Generation
FDP_ACC.1/SVD_Transfer	FDP_ACF.1/SVD_Transfer
FDP_ACC.1/SCD_Import	FDP_ACF.1/SCD_Import
FDP_ACC.1/Signature_ Creation	FDP_ACF.1/Signature_Creation
FDP_ACF.1/SCD/SVD_ Generation	FDP_ACC.1/SCD/SVD_Generation, FMT_MSA.3
FPD_ACF.1/SVD_Transfer	FDP_ACC.1/SVD_Transfer, FMT_MSA.3
FDP_ACF.1/SCD_Import	FDP_ACC.1/SCD_Import, FMT_MSA.3
FDP_ACF.1/Signature_ Creation	FDP_ACC.1/Signature_Creation, FMT_MSA.3
FDP_DAU.2/SVD	FIA_UID.1
FDP_ITC.1/SCD	FDP_ACC.1/SCD_Import, FMT_MSA.3
FDP_UCT.1/SCD	FDP_ITC.1/SCD, FDP_ACC.1/SCD_Import
FDP_RIP.1	No dependencies
FDP_SDI.2/Persistent	No dependencies
FDP_SDI.2/DTBS	No dependencies
FDP_UIT.1/DTBS	FDP_ACC.1/Signature_Creation, FTP_ITC.1/DTBS
FIA_AFL.1	FIA.UAU.1
FIA_UAU.1	FIA_UID.1
FIA_API.1	No dependencies
FIA_UID.1	No dependencies
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1
FMT.MSA.1/Admin	FDP_ACC.1/SCD_Import, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_SMF.1

Table 13. Dependencies of Security Functional Requirements*...continued*

SFR	Dependencies
FMT_MSA.2	FDP_ACC.1/Signature_Creation, FDP_ACC.1/SCD_Import, FMT_MSA.1/Admin, MFT_MSA.1/Signatory, FMT_SMR.1, FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/Signature_Creation, FMT_SMF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory
FMT_MSA.3	FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FDP_ACC.1/Signature_Creation
FMT_MSA.4	FDP_ACC.1/SCD_Import, FDP_ACC.1/Signature_Creation, FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation
FMT_MTD.1/Admin	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	No dependencies
FMT_SMR.1	FIA_UID.1
FPT_EMS.1	No dependencies
FPT_FLS.1	No dependencies
FPT_PHP.1	No dependencies
FPT_PHP.3	No dependencies
FPT_TST.1	No dependencies
FTP_ITC.1/SCD	No dependencies
FTP_ITC.1/SVD	No dependencies
FTP_ITC.1/VAD	No dependencies
FTP_ITC.1/DTBS	No dependencies

8.2 Rationale for Extensions

Extensions are based on the Protection Profiles and have all been adopted by the developer of the TOE:

- FPT_EMS.1 'TOE emanation'
- FIA_API.1 'Authentication Proof of Identity'

8.3 PP Claim Rationale

This ST includes all the security objectives and requirements claimed by the claimed Protection Profiles and, all of the operations applied to the SFRs are in accordance with the requirements of these PPs. The security requirements in the ST is a super-set of the requirements from the claimed PPs.

8.3.1 SPD Rationale

All assets, assumptions, threats and OSPs of each claimed PPs have been strictly applied to this TOE.

No assumptions have been added.

8.3.2 Objectives Rationale

No objectives have been added.

8.3.3 SFR Rationale

The selections and assignments performed in the TOE are compliant with the Protection Profiles.

8.3.4 PP compliancy

The TOE type is compliant with the claimed PPs: the TOE is a Secure Signature-Creation Device representing the SCD storage, SCD/SVD generation, and signature-creation component. The TOE provides a secure channel to CGA and SCA

The TOE type is compliant with the claimed PPs.

The TOE is compliant with the representation provided in all claimed PPs.

The conformance to the PPs is strict

9 Bibliography

9 . 1 Evaluation documents

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

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, CCMB-2017-04-002, April 2017.

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, CCMB-2017-04-003, April 2017.

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

[5] Protection profiles for secure signature creation device — Part 2: Device with key generation, certified under the reference BSI-CC-PP-0059-2009-MA-02, Version 2.0.1, 2012-01-23.

[6] Protection profiles for secure signature creation device — Part 3: Device with key import, certified under the reference BSI-CC-PP-0075-2012-MA-01, Version 1.0.2, 2012-07-24.

[7] Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application, certified under the reference BSI-CC-PP-0071-2012-MA-01, Version 1.0.1, 2012-11-14.

[8] Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application, certified under the reference BSI-CC-PP-0072-2012-MA-01, Version 1.0.1, 2012-11-14.

[9] Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted communication with signature creation application, certified under the reference BSI-CC-PP-0076-2012-MA-01, Version 1.0.4, 2013-04-03.

9 . 2 Developer documents

[10] ChipDoc 3.0 User Guide Manual, NXP Semiconductors, Revision 2.5, 7 October 2019.

[11] ChipDoc 3.0 SSCD Personalization Guide, NXP Semiconductors, Revision 1.6, 2 December 2024.

[12] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4), Security Target Lite, NXP Semiconductors, Rev. 2.9, 17 January 2024, BSI-DSZ-CC-1136-V4-2024.

[13] JCOP 4 P71 Security Target Lite for JCOP 4 P71 / SE050, NXP Semiconductors, Rev. 4.14, 17 January 2024, NSCIB-CC-2300172-01.

[14] ChipDoc V3 Application note, Revision 1.6, Date 2 December 2024.

9 . 3 Standards

[15] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures.

[16] PKCS#1: RSA Cryptography Standard, Version 1.5.

[17] PKCS #1: RSA Cryptography Standard, Version 2.2, October 27, 2012, RSA Laboratories

[18] ISO/IEC 14888-3:2015: Information technology – Security techniques – Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms, 2016.

[19] ANSI X9.62-2005: Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute (ANSI), 2005.

[20] Technical Guideline TR-03110-1, Advanced Security Mechanisms fo Machine Readable Travel Documents and eIDAS Token – Part 1 – eMRTDs with BAC/ PACEv2 and EACv1, Version 2.20, 26. February 2015.

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

[22] Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3: Common Specifications, Version 2.21, 21. December 2016

10 Legal information

10.1 Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

10.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Suitability for use in non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

10.3 Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

DESFire — is a trademark of NXP B.V.

MIFARE — is a trademark of NXP B.V.

Tables

Tab. 1. TOE Reference and ST Reference 3
Tab. 2. Reference to Certified Micro Controller with IC Dedicated Software and Crypto Library 5
Tab. 3. Reference to certified Platform 5
Tab. 4. Delivery Items 10
Tab. 5. Users and Subjects for this TOE 13
Tab. 6. Mapping of security problem definition to security objectives 20
Tab. 7. Security Attributes for Access Control 30
Tab. 8. Security Assurance Requirements according to EAL5 augmented 52
Tab. 9. Mapping of security problem definition to security objectives 54
Tab. 10. Signatory Data Characteristics 60
Tab. 11. Mapping Security Functional Requirements to Security Functions 63
Tab. 12. Dependencies of Security Assurance Requirements (Security Target) 65
Tab. 13. Dependencies of Security Functional Requirements 66

Figures

Fig. 1. Components of the TOE 3

Contents

1 Introduction 3
1.1 TOE Reference and ST Reference 3
1.2 TOE Overview 3
1.3 TOE Description 4
1.3.1 TOE Components and Composite Certification 4
1.3.1.1 Micro Controller 4
1.3.1.2 Security IC Dedicated Software 5
1.3.1.3 Security IC Embedded Software 5
1.3.2 TOE as Secure Signature Creation Device 6
1.3.2.1 Additional Functionality including PACE Secure Messaging 6
1.3.3 TOE Life Cycle 7
1.3.3.1 Development Phase 7
1.3.3.2 Operational Phase 8
1.3.3.3 Scope of SSCD PP Application 10
1.3.4 TOE Identification 10
1.3.4.1 TOE Delivery 10
1.3.4.2 Identification of the TOE 11
1.3.5 Evaluated Package Types 11
2 Conformance Claims 12
2.1 CC Conformance Claim 12
2.2 PP Claim 12
2.3 Package Claim 12
2.4 Conformance Claim Rationale 12
3 Security Problem Definition 13
3.1 Assets 13
3.2 Subjects 13
3.3 Threats 13
3.4 Organisational Security Policies 14
3.5 Assumptions 15
4 Security Objectives 16
4.1 Security Objectives for the TOE 16
4.2 Security Objectives for the operational environment 17
4.3 Security Objectives Rationale 20
4.3.1 Security Objectives Coverage 20
4.3.2 Security objectives sufficiency 20
5 Extended Components Definition 26
5.1 TOE Emanation (FPT_EMS.1) 26
5.2 Authentication Proof of Identity (FIA_API.1) 27
6 Security Requirements 28
6.1 Security Functional Requirements 28
6.1.1 Cryptographic Support (FCS) 28
6.1.1.1 Cryptographic key management (FCS_CKM) 28
6.1.1.2 Cryptographic operation (FCS_COP) 29
6.1.2 User Data Protection (FDP) 30
6.1.2.1 Access control policy (FDP_ACC) 31
6.1.2.2 Access control functions (FDP_ACF) 33
6.1.2.3 Data authentication (FDP_DAU) 36
6.1.2.4 Import from outside of the TOE (FDP_ITC) 36
6.1.2.5 Inter-TSF user data confidentiality transfer protection (FDP_UCT) 37
6.1.2.6 Inter-TSF user data integrity transfer protection (FDP_UIT) 37
6.1.2.7 Residual information protection (FDP_RIP) 38
6.1.2.8 Stored data integrity (FDP_SDI) 38
6.1.3 Identification and Authentication (FIA) 39
6.1.3.1 Authentication failures (FIA_AFL) 39
6.1.3.2 User authentication (FIA_UAU) 40
6.1.3.3 Authentication proof of identity (FIA_API) 41
6.1.3.4 User identification (FIA_UID) 41
6.1.4 Security Management (FMT) 42
6.1.4.1 Management of functions in TSF (FMT_MOF) 42
6.1.4.2 Management of security attributes (FMT_MSA) 42
6.1.4.3 Management of TSF data (FMT_MTD) 45
6.1.4.4 Specification of management functions (FMT_SMF) 45
6.1.4.5 Security management roles (FMT_SMR) 46
6.1.5 Protection of the TSF (FPT) 46
6.1.5.1 TOE emanation (FMT_EMS) 46
6.1.5.2 Fail secure (FPT_FLS) 47
6.1.5.3 TSF physical protection (FPT_PHP) 48
6.1.5.4 TSF self test (FPT_TST) 48
6.1.6 Trusted path/channels (FPT) 49
6.1.6.1 Inter-TSF trusted channel (FTP_ITC) 49
6.2 Security Assurance Requirements 52
6.3 Security Assurance Requirements Rationale 53
6.4 Security Requirements Rationale 54
6.4.1 Security Requirement Coverage 54
6.4.2 Security Requirements Sufficiency 56
7 TOE Summary Specification 59
7.1 SF.Access Control 59
7.2 SF.Administration 59
7.3 SF.Signatory Authentication 60
7.4 SF.Signature Creation 60
7.5 SF.Secure Messaging 61
7.6 SF.Crypto 61
7.7 SF.Protection 62
7.8 TOE Summary Specifications Rationale 62
8 Additional Rationale 65
8.1 Dependencies Rationale 65
8.1.1 SAR Dependencies 65
8.1.2 Justification of Unsupported Dependencies 66
8.1.3 SFR Dependencies 66
8.2 Rationale for Extensions 67
8.3 PP Claim Rationale 67
8.3.1 SPD Rationale 67
8.3.2 Objectives Rationale 68
8.3.3 SFR Rationale 68
8.3.4 PP compliancy 68
9 Bibliography 69
9.1 Evaluation documents 69
9.2 Developer documents 69
9.3 Standards 69
10 Legal information 71

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 2 December 2024