HID Global
viale Remo De Feo, 1
80022 Arzano (NA), ITALY

www.hidglobal.com

HIDApp-eDoc suite

Security Target eIDAS eSign Application

Common Criteria version 3.1 revision 5
Assurance Level EAL5+

Version	1.1
Date	2023-05-29
Reference	TCLE210006
Classification	PUBLIC

Table of Contents

List of Tables

List of Figures

Abbreviations and notations

Numerical values

Numbers are printed in decimal, hexadecimal or binary notation.
Hexadecimal values are indicated with a 'h' suffix as in XXh, where X is a hexadecimal digit from 0 to F.
Decimal values have no suffix.

Example: the decimal value 179 may be noted as the hexadecimal value B3h.

Acronyms

The term HID is an acronym for Human Interface Device, as described in section 12.1, used in the protection profiles for secure signature creation device [R10] [R11] [R12] and should not be confused with the name of the company HID Global.

Keywords

The words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" are to be interpreted as described in RFC 2119 [R30].

Definitions

The IC Developer is defined as the Platform Developer of the composite product evaluation; the IC Manufacturer is defined as the Platform Manufacturer of the composite product evaluation (see section 3.4).

Foreword

This security target refers to the European Parliament Directive 1999/93/EC [R15] in accordance with the protection profiles EN 419211-2:2013 [R10], EN 419211-4:2013 [R11], EN 419211-5:2013 [R12] it declares conformance with (cf. Section 3.3). However, it also incorporates the requirements of the eIDAS Regulation (EU) No 910/2014 [R13] and the according Commission Implementing Decision (EU) 2016/650 [R14], repealing the Directive 1999/93/EC.

1. Introduction

1.1 Security Target overview

This document is the sanitized version of the document Security Target for HIDApp-eDoc suite – eIDAS eSign Application [R20].

This security target defines the security requirements, as well as the scope of the Common Criteria evaluation, for the signature creation functionality of HIDApp-eDoc suite.

The Target Of Evaluation (TOE) is the platform NXP JCOP 4 P71 [R37] with application Java Card Applet HID HIDApp-eDoc suite, namely an International Civil Aviation Organization (ICAO) applet compliant with ICAO Doc 9303 8th ed. 2021 – LDS1 [R27] [R28] [R29] and an eIDAS eSign Applet providing qualified signature features (QSCD). The qualified signature features are compliant with the eIDAS Regulation (EU) No 910/2014 [R13] and the according Commission Implementing Decision (EU) 2016/650 [R14], repealing the European Parliament Directive 1999/93/EC [R15]. The eIDAS eSign application is also compliant to the BSI TR-03110-2 [R4] and TR Signature creation and administration for eIDAS token [R1].

This security target specifies the security requirements for the eIDAS eSign application of the TOE.
Furthermore, the ICAO application of the TOE supports:

- Basic Access Control (BAC) compliant with ICAO Doc 9303 [R28].

which is addressed by another security target [R18] and:

- Password Authenticated Connection Establishment (PACE) compliant with ICAO Doc 9303 [R28];
- Active Authentication (AA) compliant with ICAO Doc 9303 [R28];
- Extended Access Control (EAC) v1 compliant with BSI TR-03110 [R3] [R4] [R5];

which are addressed by still another security target [R19].

1.2 Security Target reference

Table 1-1 Security Target reference

Title	Security Target for HIDApp-eDoc suite - eIDAS eSign Application - Public version
Version	1.1
Authors	Giovanni LICCARDO, Roberta SODANO

Date	2023-05-29
Reference	TCLE210006

1.3 TOE reference

Table 1-2 TOE reference

TOE name	HIDApp-eDoc suite eIDAS eSign Application
TOE version	3_00
TOE developer	HID Global
TOE identifier	HIDApp-eDoc_3_00
TOE identification data	48h 49h 44h 41h 70h 70h 2Dh 65h 44h 6Fh 63h 5Fh 33h 5Fh 30h 30h
Platform security target	JCOP 4 P71, Security Target Lite for JCOP 4 P71 / SE050 Rev. 4.11 – 3 January 2023 [R37]
Platform certification report	NSCIB-CC-180212-5MA1 [R44]

The TOE is delivered as a chip ready for initialization. It is identified by the following string, which constitutes the TOE identifier:

HIDApp-eDoc_3_00

(ASCII encoding: 48h 49h 44h 41h 70h 70h 2Dh 65h 44h 6Fh 63h 5Fh 33h 5Fh 30h 30h)

where:

- “HIDApp-eDoc” is the TOE name,
- the underscore character is a separator and
- “3” is the TOE major version number and
- “00” is the TOE minor version number

The ASCII encoding of the TOE identifier constitutes the TOE identification data, located in the persistent memory of the chip. Instructions for reading these data are provided by the guidance documentation [R21] [R22] [R23] [R24] [R25].

1.4 TOE overview

1.4.1 TOE type, usage and major security features

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

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

The TOE provides the following functions:

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

The TOE is prepared for the Signatory's use by:

1. generating at least one SCD/SVD pair and
2. personalizing for the Signatory by storing in the TOE:
    a. the Signatory's Reference Authentication Data (RAD),
    b. optionally, certificate info for at least one SCD in the TOE.

The eIDAS eSign application supports the General Authentication Protocol (GAP) [R4].

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

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. The means of providing this information is expected to protect the confidentiality and the integrity of the corresponding Reference Authentication Data (RAD).

If the use of an SCD is no longer required, then it shall be destroyed.

1.4.2 Required non-TOE hardware/software/firmware

In order to be powered up and to communicate with the external world, the TOE needs a terminal that supports contactless or contact-based communication according to [R31], [R33] and [R32].
The TOE shall be able to distinguish the following kinds of terminals:

- Signature Management Terminal (SMT), this is a terminal that allows signature creation as well as the management of the signature application.
- Signature Terminal (ST), this is a terminal that allows for the creation of electronic signature.

The TOE operates in the following operational environments:

- The preparation environment, where it interacts with a Certification Service Provider (CSP) through a Certificate Generation Application (CGA) to obtain a certificate for the Signature Verification Data (SVD) corresponding to the Signature Creation Data (SCD) generated by the TOE. The TOE exports the SVD through a trusted channel allowing the CGA to check its authenticity. The preparation environment interacts further with the TOE to personalize it with the initial value of the Reference Authentication Data (RAD);
- The signing environment, where it interacts with the signer through a Signature Creation Application (SCA) to sign data after authenticating the signer as its Signatory. The SCA provides the data to be signed or a unique representation thereof (DTBS/R) as input to the TOE signature creation function and obtains the resulting digital signature. The TOE and the SCA communicate through a trusted channel to ensure the integrity of the DTBS/R;
- The management environment, where it interacts with the user to perform management operations, e.g. to reset a blocked RAD, after authenticating the user as its Signatory. A single device, e.g. a smart card terminal, may provide the required environment for management and signing.

Therefore, the use of the TOE requires any hardware, software and firmware component of such operational environments, particularly a Certificate Generation Application (CGA) and Signature Creation Application (SCA) supporting trusted channels with the TOE.

2. TOE description

2.1 TOE physical scope

The HIDApp-eDoc suite is comprised of the following parts:

- The platform NXP JCOP 4 P71 (see Appendix A), which is composed by the Micro Controller and a software stack which is stored on the Micro Controller and which can be executed by the Micro Controller. The software stack can be further split into the following components:
    - Firmware for booting and low level functionality of the Micro Controller (MC FW) like writing to flash memory. This includes software for implementing cryptographic operations, called Crypto Library.
    - Software for implementing a Java Card Virtual Machine [R42], a Java Card Runtime Environment [R41] and a Java Card Application Programming Interface [R40] called JCVM, JCRE and JCAPI.
    - Software for implementing content management according to GlobalPlatform [R16] called GlobalPlatform Framework.
    - Software for executing native libraries, called Secure Box.
- the applet, composed by:
    - an ICAO application LDS1 compliant with ICAO Doc 9303 [R27] [R28] [R29][1],
    - eIDAS eSign application compliant with the eIDAS Regulation (EU) No 910/2014 [R13] and the according Commission Implementing Decision (EU) 2016/650 [R14], repealing the European Parliament Directive 1999/93/EC [R15]. The eIDAS eSign application is also compliant to the BSI TR-03110-2 [R4].
- guidance documentation about the initialization of the TOE, the preparation and use of the ICAO application and eIDAS eSign application, composed by:
    - the Initialization Guidance [R21],
    - the Personalization Guidance [R22] – ICAO application,
    - the Operational User Guidance [R24] – ICAO application,
    - the Personalization Guidance [R23] – eIDAS eSign application,
    - the Operational User Guidance [R25] – eIDAS eSign application.

[1] The ICAO Application is out of the scope of this Security Target.

Table 2-5 identifies, for each guidance document, the actors involved in TOE life cycle who are the intended recipients of that document.

Table 2-1 described the format and delivery method of each TOE components:

Table 2-1 TOE component delivery

Type	TOE component	Format	Delivery method
Platform	NXP JCOP 4 P71	Smart Card	Secure courier
Applet	HIDApp-eDoc suite	CAP file	Secure IC Manufacturer's Web application
Document	Preparative and operational guidance	pdf/docx	Encrypted email message

The delivery procedure for the TOE is described in detail [R26].

2.2 TOE logical scope

The eIDAS eSign application of the TOE supports the same life cycle phases, as well as the same roles, i.e. *Administrator* and *Signatory*, as those defined in the PPs [R10] [R11] [R12]:

- "Administrator: User who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator."
- "Signatory: User who hold the TOE and use it on their own behalf or on behalf of the natural or legal person or entity they represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as signatory."

The BSI TR-03110-2 [R4] defines the following terminal types:

- Signature Management Terminal (SMT) is an extension of a Authentication Terminal to support management of the Signature Application. This terminal allows signature creation as well as the management of the Signature Application (e.g. signature key generation).
- Signature Terminal (ST) is a terminal that allows for the creation of electronic signatures. The eIDAS token SHALL require a Signature Terminal to authenticate itself before access according to the effective authorization is granted. To authenticate a terminal as Signature Terminal, the General Authentication Procedure MUST be used. The authorization level of a Signature Terminal SHALL be determined by the effective authorization calculated from the certificate chain.

In this Security Target we assume that:

- The administrator is a user who is in charge to perform the TOE administrative functions. He uses a terminal that is entitled to manage the eSign application.
  The administrator shall also use a terminal that is authorized to manage the eSign application.
  The signatory can be the administrator in the case he can perform the operations using an authorized terminal (cf. section 2.2 of [R25]).
- The signatory is a user who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity they represent. He uses a terminal that is entitled to create electronic signature with the eSign application.
  To prove his entitlement to sign, the user shall know the signature PIN, that could be the Global PIN or Local PIN (cf. section 2.2 of [R25]).

The TOE distinguishes between S.Admin or S.Sigy based on the effective authorization obtained from GAP [R1].

For each of the Signatory's authentication secrets provided for by the PPs [R10] [R11] [R12], i.e. the RAD, the VAD and the PUK[2], the Signatory's credentials are

- RAD: Global PIN with sign privileges or Local PIN
- VAD: Global PIN with sign privileges or Local PIN
- PUC: PUK

Each of the main operations of the TOE is described here below.

2.2.1 Mutual authentication

As a precondition for gaining access to further operations, both the Administrator and the Signatory must perform a mutual authentication with respect to the eIDAS eSign application. This is executed by means of the General Authentication Procedure (GAP) as in TR-03110 part 2 [R4] and it is comprised of the following steps:

1. Authentication by means of a PACE authentication;
2. Extended Access Control (EACv2) authentication, composed by Terminal Authentication v2 (TA2) and Chip Authentication v2 (CA2).

[2] The PPs implicitly provide for the existence of a PUK by allowing the support of RAD unblock.

The PACE authentication supports the following algorithms:

- Key agreement: ECDH
- Mapping: Generic Mapping, Integrated Mapping
- Symmetric ciphering and MAC computation (key bit length): 3DES (112), AES (128, 192 and 256)
- Standardized Domain Parameters: see Table 2-2 (identifiers other than the standard ones must be used for proprietary Domain Parameters)

Table 2-2 Standardized domain parameters

Id	Name
0	Not supported
1	2048-bit MODP Group with 224-bit Prime Order Subgroup
2	2048-bit MODP Group with 256-bit Prime Order Subgroup
3-7	RFU
8	Not supported
9	Not supported
10	NIST P-224 (secp224r1)
11	BrainpoolP224r1
12	NIST P-256 (secp256r1)
13	BrainpoolP256r1
14	BrainpoolP320r1
15	NIST P-384 (secp384r1)
16	BrainpoolP384r1
17	BrainpoolP512r1
18	NIST P-521 (secp521r1)
19-31	RFU

For PACE-PIN, the key lengths that can be used are limited to 256, 384 and 512 bits. For PACE-CAN, all key sizes can be used (cf. section 6.4 of [R39]).

The export of the SVD to the CGA upon key pair generation, as well as the import of the DTBS/R from the SCA upon signature creation, shall be executed over the trusted channel compliant with TR-03110 part 2 [R4] opened by means of General Authentication Procedure.

Table 2-3 identifies the credentials associated to either of the QSCD roles, through which they can perform their respective mutual authentication procedures.

Table 2-3 Mapping between QSCD roles and their credentials

QSCD roles	Credentials
Administrator	• CAN • Administrator's terminal key pair

	• Global PIN without sign privileges
Signatory (for ordinary operations)	• CAN • Signatory's terminal key pair • Global PIN with sign privileges • Local PIN
Signatory (for RAD unblock)	• CAN • Signatory's terminal key pair • PUK

In accordance with Table 2-3, either of the QSCD roles shall perform mutual authentication as follows:

- The Administrator shall perform:
  1. GAP authentication using CAN and Administrator's terminal key pair.

     Or

  1. GAP authentication using Global PIN without sign privileges and Administrator's terminal key pair.
- The Signatory shall perform:
  1. GAP authentication using CAN and Signatory's terminal key pair;
  2. Verification of the Global PIN with sign privileges, for signature operations.

     Or

  1. GAP authentication using CAN and Signatory's terminal key pair;
  2. Verification of the Local PIN, for signature operations.

     Or

  1. GAP authentication using CAN and Signatory's terminal key pair;
  2. Verification of the PUK, for RAD unblock.

     Or

  1. GAP authentication using Global PIN with sign privileges and Signatory's terminal key pair, for signature operations.

2.2.2 Generation of SCD/SVD pairs

The eIDAS eSign application supports the generation of multiple SCD/SVD pairs. The import of certificate info from the CGA is supported as well.

SCD/SVD pair generation is only allowed after the authentication and must be executed over the trusted channel opened via GAP. This ensures the protection of SVD integrity upon export of the SVD to the CGA. The import of certificate info from the CGA must be executed over the same trusted channel.

The eIDAS eSign application supports the generation of:

- RSA key pairs compliant with [R43] of 2048, 3072 or 4096 bits;
- ECDSA key pairs compliant with [R6] of 256, 320, 384, 512 and 521 bits.

2.2.3 Signature creation with SCD

The signature creation function of the eIDAS eSign application is compliant to [R1].

The eIDAS eSign application supports digital signature creation with signature creation algorithm RSASSA-PKCS1-v1_5 compliant with PKCS #1 [R43]. The signature creation algorithm RSASSA-PSS [R43] is supported as well. In both cases the hash algorithm is SHA-256 and SHA-512 compliant with FIPS PUB 180-4 [R35] and keys of 2048, 3072 or 4096 bits are supported.
The eIDAS eSign application support digital signature creation with signature creation algorithm ECDSA and keys of 256, 320, 384, 512 or 521 bits are supported[3]. The hash algorithms are SHA-256, SHA-384 or SHA-512 compliant with FIPS PUB 180-4 [R35].

The export of public keys and certificate info to the SCA is supported as well.

Signature creation is only allowed after the authentication of the user in the Signatory role (cf. section 2.2.1) and must be executed over the trusted channel opened via the GAP. This guarantees the protection of DTBS/R integrity upon import of the DTBS/R from the SCA. The export of digital signatures to the SCA must be executed over the same trusted channel.

2.3 TOE life cycle

The TOE life cycle is comprised of four life cycle phases, i.e. *development*, *manufacturing*, *personalization* and *operational use*. With regard to the life cycle of the eIDAS eSign application, these phases can be split into eight steps. The last step, which takes place when the TOE stands in the operational use phase, matches the QSCD life cycle phases defined in the PPs [R10] [R11] [R12].
Figure 2-1 represents the life cycle of the TOE eIDAS eSign application. Particularly, it illustrates the correspondence between the life cycle phases of the TOE and the life cycle

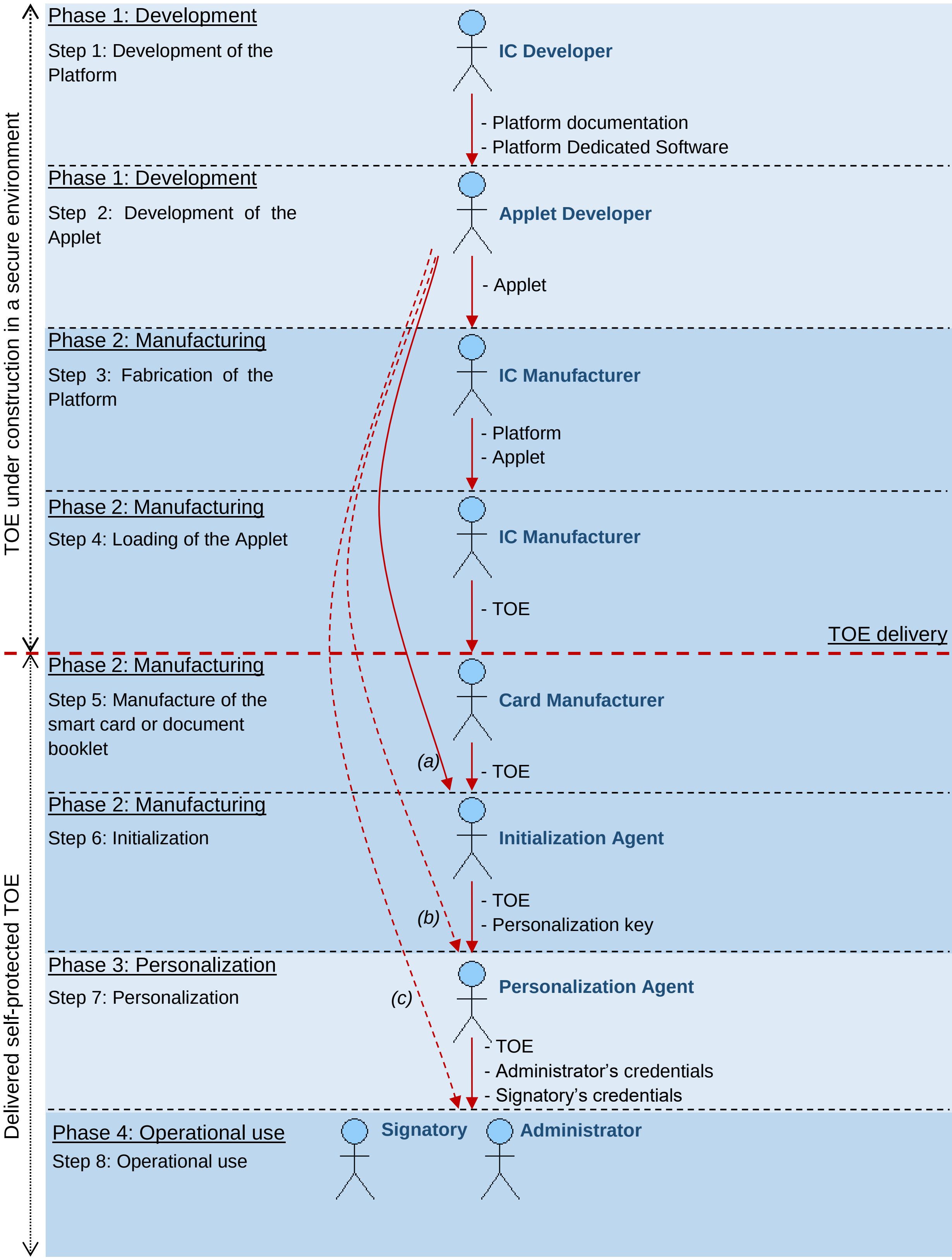
[3] The cryptographic requirement REQ_ECC_POINT_MULT defined in section 6.4 of [R39] do not apply to the TOE because the ECC point multiplication is never used in protocol other than Diffie Hellman Key Exchange and ECDSA.

phases of the eIDAS eSign application as defined in the PPs and identifies the actors involved in each life cycle step. Direct deliveries of items between actors are represented with continuous lines, while deliveries in which intermediate actors may be in charge of receiving the exchanged items and forwarding them to the subsequent actors are represented with dotted lines.
Deliveries of items occurring between non-consecutive actors are just marked with letters in order to preserve the clarity of the diagram. A legend for these deliveries, which identifies the exchanged items for each of them, is provided in Table 2-4.

Table 2-4 Legend for deliveries occurring between non-consecutive actors

Delivery	Delivered items
(a)	• Initialization key • Initialization guidance
(b)	• Personalization guidance
(c)	• Operational user guidance

Figure 2-1 Life cycle of the TOE eIDAS eSign application



Detailed information about the operations available in each life cycle phase of the TOE is provided in the guidance documentation of the TOE eIDAS eSign application [R21] [R23] [R25]. Table 2-5 identifies, for each guidance document, the actors who are the intended recipients of that document.

Table 2-5 Identification of recipient actors for the guidance documentation of the TOE eIDAS eSign application

Guidance document	Recipient actors
Initialization guidance	Initialization Agent
Personalization guidance	Personalization Agent
Operational user guidance	Administrator, Signatory

The phases and steps of the TOE life cycle are described in what follows. The names of the involved actors are emphasized using boldface.

2.3.1 Phase 1: Development

Step 1: Development of the Platform

The **IC Developer** develops the JCOP 4 P71 Platform, the platform dedicated software and the guidance documentation associated with these TOE components.

Finally, the following items are securely delivered to the **Applet Developer**:

- the Platform documentation,
- the Platform dedicated software,

Step 2: Development of the Applet

The **Applet Developer** uses the guidance documentation for the Platform and for relevant parts of the Platform Dedicated Software and develops the applets, consisting of the ICAO application and the eIDAS eSign application, as well as the guidance documentation associated with these TOE components.

Furthermore, the **Applet Developer** generates the initialization key.

Finally:

- the Applet is securely delivered to the **IC Manufacturer**;
- the initialization key are securely delivered to the **Initialization Agent**;

As regards TOE guidance documentation, all documents are securely delivered to the **Initialization Agent**, or each document is securely delivered to the recipient actors as identified in Table 2-5.

2.3.2 Phase 2: Manufacturing

<u>Step 3: Fabrication of the platform</u>

The **IC Manufacturer** produces the JCOP 4 P71 Platform.

<u>Step 4: Loading of the Applet</u>

The **IC Manufacturer** loads the Applet received from the Applet Developer and creates in the IC persistent memory the high-level objects relevant for the eIDAS eSign application. Particularly, the initialization key is stored into the IC persistent memory.

Finally, the TOE is securely delivered to the **Card Manufacturer**.

Application Note 1 *The point of delivery of the TOE coincides with the completion of step 4, i.e. with the delivery of the TOE, in the form of an IC not yet embedded, from the IC Manufacturer to the Card Manufacturer. That is to say, this is the event upon which the construction of the TOE in a secure environment ends and the TOE begins to be self-protected.*

<u>Step 5: Manufacture of the smart card or document booklet</u>

The **Card Manufacturer** equips the IC with contact-based and/or contactless interfaces and embeds the IC into a smart card or a document booklet.

Finally, the TOE is securely delivered to the **Initialization Agent**.

<u>Step 6: Initialization</u>

The **Initialization Agent** use the initialization key to mutual authentication with the TOE to instantiate the eIDAS QSCD applet and writes the Personalization Key.

Finally, the TOE is securely delivered to the **Personalization Agent**, along with the personalization key if it was delivered to the **Initialization Agent** rather than directly to the **Personalization Agent**.

As regards TOE guidance documentation, if the **Initialization Agent** also received the documents intended for the subsequent actors, then either all of these documents are securely delivered to the **Personalization Agent**, or each document is securely delivered to the recipient actors as identified in Table 2-5.

2.3.3 Phase 3: Personalization

Step 7: Personalization

The **Personalization Agent** establishes the identity of the Signatory to whom the TOE is to be assigned and generate the following credentials:

- CAN;
- Global PIN without sign privileges

And, optionally:

- Global PIN with sign privileges;
- Local PIN;
- PUK.

Then, the **Personalization Agent** creates/modifies in the IC persistent memory the high-level objects relevant for the eIDAS eSign application.
Particularly:

- The Initialization key is overwritten with the Personalization key;
- The number of the empty private/public key objects and certificate info files being created, each associated with an unambiguous identifier, is equal to the maximum possible number of key pairs required for signature creation in the operational use phase. Although the key pairs are not generated yet, their lengths are fixed when the key objects are created and cannot be changed afterwards.

Finally, the TOE is securely delivered to the **Administrator**, along with the following item:

- Administrator’s credentials;

As regards TOE guidance documentation, if the **Personalization Agent** also received the operational user guidance, then this document is securely delivered to the **Administrator**.

2.3.4 Phase 4: Operational use

Step 8: Operational use

Then, the **Administrator** and **Signatory** are required/allowed to modify in the IC persistent memory the high-level objects relevant for the eIDAS eSign application.
Particularly:

- The **Administrator** can generate one or more key pairs for signature creation.
  In this case, as many private/public key objects created in the personalization phase are filled with the key pairs being generated.
- The **Administrator** shall fill one or more certificate info files for each generated key pair (if any).
- The **Signatory** can generate one or more key pairs for signature creation.
  In this case, as many private/public key objects created in the personalization phase are filled with the key pairs being generated.
- The **Signatory** shall fill one or more certificate info files for each generated key pair (if any).

Furthermore, the **Signatory** performs the following operations:

- activate signature creation for the private keys generated by the **Administrator** (If any);
- create digital signatures using the available signature creation private keys;
- destroy signature creation private keys;
- change or unblock Global PIN with sign privileges;
- change or unblock Local PIN.

3. Conformance claims

3.1 Common Criteria conformance claim

This security target claims conformance to:

- Common Criteria version 3.1 revision 5 [R7] [R8] [R9], as follows:
    - Part 2 (security functional requirements) extended,
    - Part 3 (security assurance requirements) conformant.

The applet runs on the platform NXP JCOP 4 P71. This platform is certified against Common Criteria at the assurance level EAL6+ (cf. Appendix A).

3.2 Package conformance claim

This security target claims conformance to Evaluation Assurance Level EAL5, augmented with the following security assurance requirements defined in CC Part 3 [R9]:

- ALC_DVS.2 "Sufficiency of security measures";
- AVA_VAN.5 "Advanced methodical vulnerability analysis".

3.3 Protection Profile conformance claim

This security target claims strict conformance to the following Protection Profiles (PPs):

- Protection profiles for secure signature creation device – Part 2: Device with key generation, v2.0.1, EN 419211-2:2013 (certificate BSI-CC-PP-0059-2009-MA-02) [R10];
- Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, EN 419211-4:2013 (certificate BSI-CC-PP-0071-2012-MA-01) [R11];
- Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, v1.0.1, EN 419211-5:2013 (certificate BSI-CC-PP-0072-2012-MA-01) [R12].

3.4 Protection Profile conformance rationale

3.4.1 Terminology

In this Security Target the term QSCD replaces all occurrences of the term SSCD referred to in the PPs;

3.4.2 Security problem definition

The source of threats, organizational security policies and assumptions is specified in Table 3-1.

Table 3-1 Source of assumptions, threats, and OSPs

	Source		
	PP Part 2 [R10]	**PP Part 4 [R11]**	**PP Part 5 [R12]**
Threats	• T.SCD_Divulg • T.SCD_Derive • T.Hack_Phys • T.SVD_Forgery • T.SigF_Misuse • T.DTBS_Forgery • T.Sig_Forgery	All threats of the PP Part 2 [R10] This PP does not define any additional threats.	All threats of the PP Part 2 [R10] This PP does not define any additional threats.
Organizational Security Policies	• P.CSP_QCert • P.QSign • P.Sigy_QSCD • P.Sig_Non-Repud	All OSP of the PP Part 2 [R10] This PP does not define any additional OSP.	All OSP of the PP Part 2 [R10] This PP does not define any additional OSP.
Assumptions	• A.CGA • A.SCA	All Assumptions of the PP Part 2 [R10] This PP does not define any additional assumptions.	All Assumptions of the PP Part 2 [R10] This PP does not define any additional assumptions.

Changes, additions, and deletions to asset, threat agents, threats, OSPs and assumptions with respect to the PPs (cf. section 3.3) are listed in Table 3-2 and Table 3-3

Table 3-2 Changes, additions, and deletions to the threats with respect to the PPs

Threat	Difference	Rationale
-	-	-

Table 3-3 Changes, additions, and deletions to the OSPs with respect to the PPs

OSP	Difference	Rationale
P.Manufact	Addition	Added to specify the security policy to be enforced by the TOE in the manufacturing phase of its life cycle (cf. section 2.3.2).
P.Personalization	Addition	Added to specify the security policy to be enforced by the TOE in the personalization phase of its life cycle (cf. section 2.3.3).

3.4.3 Security objectives for the TOE

The source of the security objectives for the TOE is specified in Table 3-4.

Table 3-4 Source of security objectives for the TOE

	Source		
	PP Part 2 [R10]	PP Part 4 [R11]	PP Part 5 [R12]
Security objectives for the TOE	• OT.Lifecycle_Security • OT.SCD/SVD_Auth_Gen • OT.SCD_Unique • OT.SCD_SVD_Corresp • OT.SCD_Secrecy • OT.Sig_Secure • OT.Sigy_SigF • OT.DTBS_Integrity_TOE • OT.EMSEC_Design • OT.Tamper_ID • OT.Tamper_Resistance	• OT.TOE_QSCD_Auth • OT.TOE_TC_SVD_Exp	• OT.TOE_TC_VAD_Imp • OT.TOE_TC_DTBS_Imp

Changes, additions, and deletions to the security objectives for the TOE with respect to the PPs (cf. section 3.3) are listed in Table 3-5.

Table 3-5 Changes, additions, and deletions to the security objectives for the TOE with respect to the PPs

Security objective	Difference	Rationale
OT.AC_Init	Addition	Added to specify the access control to be enforced by the TOE as regards the storage of TOE initialization data (cf. section 2.3.2).

Security objective	Difference	Rationale
OT.AC_Pers	Addition	Added to specify the access control to be enforced by the TOE as regards the storage of personalization data (cf. section 2.3.3).

3.4.4 Security objectives for the operational environment

The source of the security objectives for the operational environment is specified in Table 3-6.

PP Part 4 [R11] replaces (~~strikethrough~~ text) OE.QSCD_Prov_Service from PP Part 2 [R10] with OE.Dev_Prov_Service, and adds the security objectives for the operational environment OE.CGA_QSCD_Auth, OE.CGA_TC_SVD_Imp in order to address the additional method of use of SCD/SVD pair generation after delivery to the Signatory and outside a secure preparation environment.
PP Part 5 [R12] replaces (~~strikethrough~~ text) OE.HID_VAD from PP Part 2 [R10] with OE.HID_TC_VAD_Exp, and OE.DTBS_Protect from PP Part 2 with OE.SCA_TC_DTBS_Exp.

Table 3-6 Source of security objectives for the operational environement

	Source		
	PP Part 2 [R10]	**PP Part 4 [R11]**	**PP Part 5 [R12]**
Security objectives for the operational environment	• OE.SVD_Auth • OE.CGA_QCert ~~• OE.QSCD_Prov_Service~~ ~~• OE.HID_VAD~~ • OE.DTBS_Intend ~~• OE.DTBS_Protect~~ • OE.Signatory	• OE.Dev_Prov_Service • OE.CGA_QSCD_Auth • OE.CGA_TC_SVD_Imp	• OE.HID_TC_VAD_Exp • OE.SCA_TC_DTBS_Exp

3.4.5 Security functional requirements

The source of the security functional requirements is specified in Table 3-7.

Table 3-7 Source of security functional requirements

	Source		
	PP Part 2 [R10]	PP Part 4 [R11]	PP Part 5 [R12]
Security objectives for the TOE	• FCS_CKM.1 • FCS_CKM.4 • FCS_COP.1 • 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/Signature_Creation • FDP_ACF.1/Signature creation • FDP_RIP.1 • FDP_SDI.2/Persistent • FDP_SDI.2/DTBS • FIA_UID.1 • FIA_UAU.1 • FIA_AFL.1 • FMT_SMR.1 • FMT_SMF.1 • 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 • FPT_EMS.1 • FPT_FLS.1 • FPT_PHP.1	• FIA_UAU.1 (extends [R10]) • FIA_API.1 • FDP_DAU.2/SVD • FTP_ITC.1/SVD	• FIA_UAU.1 (extends [R10]) • FDP_UIT.1/DTBS • FTP_ITC.1/VAD • FTP_ITC.1/DTBS

	• FPT_PHP.3 • FPT_TST.1		

Changes, additions, and deletions to the security functional requirements with respect to the PPs (cf. section 3.3) are listed in Table 3-8.

Table 3-8 Changes, additions, and deletions to the security functional requirements with respect to the PPs

SFR	Difference	Rationale
FCS_CKM.1/RSA	Change	An iteration labelled RSA has been added to take into account ECDSA as an additional algorithm.
FCS_CKM.1/ECDSA	Addition	Added to cover key generation algorithm ECDSA
FCS_COP.1/RSA	Change	An iteration labelled RSA has been added to take into account ECDSA as an additional algorithm.
FCS_COP.1/ECDSA	Addition	Added to cover key generation algorithm ECDSA
FIA_UAU.1	Change	Refined to remove user identification from the list of the actions allowed by the TOE before the user is authenticated.
FMT_SMR.1/QSCD	Change	Iteration performed on PP SFR FMT_SMR.1 due to the introduction of further iterations, related to the roles supported by the TOE in addition to those specified in the PPs (cf. below).
FMT_SMR.1/Init	Addition	Added to cover the Initialization Agent role, supported by the TOE in addition to the roles specified in the PPs (cf. section 2.3.2).
FMT_SMR.1/Pers	Addition	Added to cover the Personalization Agent role, supported by the TOE in addition to the roles specified in the PPs (cf. section 2.3.3).
FMT_MTD.1/Admin	Change	Refined to remove the capability of creation of RAD in Operational use by R.Admin.
FMT_MTD.1/Init	Addition	Added to specify the requirements to be enforced by the TOE as regards the management of TOE initialization data (cf. section 2.3.2).
FMT_MTD.1/Pers	Addition	Added to specify the requirements to be enforced by the TOE as regards the management of Personalization data, including the RAD (cf. section 2.3.3).

FTP_ITC.1/Init	Addition	Added to account for the additional trusted channel supported by the TOE for the import of TOE initialization data (cf. section 2.3.2).
FTP_ITC.1/Pers	Addition	Added to account for the additional trusted channel supported by the TOE for the import of personalization data (cf. section 2.3.3).

3.4.6 Security assurance requirements

The minimum package of security assurance requirements allowed for conformance to the PPs (cf. section 3.3) is Evaluation Assurance Level EAL4 augmented with AVA_VAN.5.
As this security target claims conformance to Evaluation Assurance Level EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 (cf. section 3.2), the aforesaid requirement is met.

4. Security problem definition

4.1 Assets, users, and threat agents

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.

Assets and objects:

The PPs [R10] [R11] [R12] share the same assets, reported here below.

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 must be maintained when it is exported.
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.

Users and subjects acting for users:

The PPs [R10] [R11] [R12] share the same users, reported here below.

1. User: end user of the TOE who can be identified as Administrator or Signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.
2. Administrator: user who is in charge of performing administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as Administrator.
3. Signatory: user who holds the TOE and uses it on their own behalf or on behalf of the natural or legal person or entity they represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as Signatory.
4. Initialization Agent: user in charge of performing step 6, initialization, of TOE life cycle (cf. section 2.3.2), particularly of writing TOE initialization data. The subject S.Init is acting in the role R.Init for this user after successful authentication as Initialization Agent.
5. Personalization Agent: user in charge of performing step 7, personalization, of TOE life cycle (cf. section 2.3.3), particularly of writing personalization data. The subject S.Pers is acting in the role R.Pers for this user after successful authentication as Personalization Agent.

Threat agents:

The PPs [R10] [R11] [R12] share the same threat agents, reported here below.

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

4.2 Threats

The PPs [R10] [R11] [R12] share the same threats, reported here below.

4.2.1 T.SCD_Divulg

Storing, copying, and releasing of 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.

4.2.2 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.

4.2.3 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.

4.2.4 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.

4.2.5 T.SigF_Misuse

Misuse of the signature creation function of the TOE

An attacker misuses the signature creation function of the TOE to create an 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.

4.2.6 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 that the Signatory intended to sign.

4.2.7 T.Sig_Forgery

Forgery of the electronic signature

An attacker forges an SDO, maybe using an electronic signature which has been created by the TOE, and the violation of the integrity of the SDO 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.

4.3 Organizational Security Policies

The PPs [R10] [R11] [R12] share the same OSPs, reported here below.

4.3.1 P.CSP_QCert

CSP generates qualified certificates

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate ([R15], article 2, clause 9, and Annex I) for the SVD generated by the QSCD. The certificates contain at least the name of the Signatory and the SVD matching the SCD implemented in the TOE under sole control of the Signatory. The CSP ensures that the use of the TOE as QSCD is evident with signatures through the certificate or other publicly available information.

4.3.2 P.QSign

Qualified electronic signatures

The Signatory uses a Signature Creation System to sign data with an advanced electronic signature ([R15], article 1, clause 2), which is a qualified electronic signature if it is based on a valid qualified certificate (according to [R15], Annex I). The DTBS are presented to the

Signatory and sent by the SCA as DTBS/R to the QSCD. The QSCD creates the electronic signature with an SCD implemented in the QSCD that the Signatory maintains under their sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

4.3.3 P.Sigy_QSCD

TOE as secure signature creation device

The TOE meets the requirements for a QSCD laid down in [R15], Annex III. This implies the SCD is used for digital signature creation under sole control of the Signatory and the SCD can practically occur only once.

4.3.4 P.Sig_Non-Repud

Non-repudiation of signatures

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

Here below are further OSPs, added in this security target to those defined in the PPs.

4.3.5 P.Manufact

Manufacturing of the e-Document

The IC Manufacturer writes IC initialization data in step 3, IC manufacturing, of TOE life cycle, including the key for the authentication of the Initialization Agent (cf. section 2.3.2).

The Initialization Agent writes TOE initialization data in step 6, initialization, of TOE life cycle, including the key for the authentication of the Personalization Agent (cf. section 2.3.2).

The Initialization Agent acts on behalf of the QSCD provisioning service.

4.3.6 P.Personalization

Personalization of the e-Document

The Personalization Agent writes personalization data in step 7, personalization, of TOE life cycle (cf. section 2.3.3), including the credentials for the authentication of the Administrator and of the Signatory.

The Personalization Agent acts on behalf of the QSCD provisioning service.

4.4 Assumptions

The PPs [R10] [R11] [R12] share the same assumptions, reported here below.

4.4.1 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.

4.4.2 A.SCA

Trustworthy Signature Creation Application

The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS/R of the data that the signatory wishes to sign in a form appropriate for signing by the TOE.

5. Security objectives

5.1 Security objectives for the TOE

Here below are the security objectives for the TOE defined in PP Part 2 [R10].

5.1.1 OT.Lifecycle_Security

Lifecycle security

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

Application Note 2 *The TOE may contain more than one set of SCD. There is no need to destroy the SCD in case of repeated SCD generation. The Signatory shall be able to destroy the SCD stored in the QSCD, e.g. after the (qualified) certificate for the corresponding SVD has expired.*

5.1.2 OT.SCD/SVD_Auth_Gen

Authorized SCD/SVD generation

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

5.1.3 OT.SCD_Unique

Uniqueness of Signature Creation Data

The TOE shall ensure the cryptographic quality of an SCD/SVD pair that 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.

5.1.4 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 with the SCD.

5.1.5 OT.SCD_Secrecy

Secrecy of 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 3 *The TOE shall keep the confidentiality of the SCD at all times, in particular during SCD/SVD generation, signature creation operation, storage and secure destruction.*

5.1.6 OT.Sig_Secure

Cryptographic security of the electronic signature

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.

5.1.7 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.

5.1.8 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.

5.1.9 OT.EMSEC_Design

Provision of 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.

5.1.10 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.

5.1.11 OT.Tamper_Resistance

Tamper resistance

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

Here below are the security objectives for the TOE defined in PP Part 4 [R11].

5.1.12 OT.TOE_QSCD_Auth

Authentication proof as QSCD

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

5.1.13 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.

Here below are the security objectives for the TOE defined in PP Part 5 [R12].

5.1.14 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 4 *This security objective for the TOE is partly covering OE.HID_VAD from PP Part 2 [R10]. While OE.HID_VAD in PP Part 2 requires only the operational* *environment to protect VAD, PP Part 5 [R12] 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, PP Part 5 partly re-assigns 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.*

5.1.15 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 5 *This security objective for the TOE is partly covering OE.DTBS_Protect from PP Part 2 [R10]. While OE.DTBS_Protect in PP Part 2 requires only the operational environment to protect DTBS, PP Part 5 [R12] 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, PP Part 5 partly re-assigns 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.*

Here below are further security objectives for the TOE, added in this security target to those defined in the PPs.

5.1.16 OT.AC_Init

Access control for the initialization of the e-Document

The TOE must ensure that TOE initialization data, including the personalization key, can be written in step 6, initialization, of TOE life cycle (cf. section 2.3.2) by the authorized Initialization Agent only.

5.1.17 OT.AC_Pers

Access control for the personalization of the e-Document

The TOE must ensure that personalization data can be written in step 7, personalization, of TOE life cycle (cf. section 2.3.3) by the authorized Personalization Agent only.

5.2 Security objectives for the operational environment

Here below are the security objectives for the operational environment defined in PP Part 2 [R10].

5.2.1 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 QSCD of the Signatory and the SVD in the qualified certificate.

5.2.2 OE.CGA_QCert

Generation of qualified certificates

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

- the name of the Signatory controlling the TOE,
- the SVD matching the SCD stored in the TOE and being under sole control of the Signatory,
- 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 the QSCD.

5.2.3 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.

5.2.4 OE.Signatory

Security obligation of the Signatory

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

Here below are the security objectives for the operational environment defined in PP Part 4 [R11].

5.2.5 OE.Dev_Prov_Service

Authentic QSCD provided by the QSCD provisioning service

The QSCD provisioning service handles authentic devices that implement the TOE, prepares the TOE for proof as QSCD to external entities, personalizes the TOE for the legitimate user as Signatory, links the identity of the TOE as QSCD with the identity of the legitimate user, and delivers the TOE to the Signatory.

Application Note 6 *This objective replaces OE.QSCD_Prov_Service from PP Part 2 [R10], which is possible as it does not imply any additional requirement for the operational environment when compared with OE.QSCD_Prov_Service (OE.Dev_Prov_Service is a subset of OE.QSCD_Prov_Service).*

5.2.6 OE.CGA_QSCD_Auth

Preparation of the TOE for QSCD authentication

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

5.2.7 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 QSCD.

Application Note 7 *The developer prepares the TOE for the delivery to the customer (i.e. the QSCD provisioning service) in the development phase, not addressed by security* *objectives for the operational environment. The QSCD provisioning service performs initialization and personalization as TOE for the legitimate user (i.e. the device holder). If the TOE is delivered to the device holder with SCD, the TOE is a QSCD. This situation is addressed by OE.QSCD_Prov_Service except for the additional initialization of the TOE for proof as QSCD and trusted channel to the CGA. If the TOE is delivered to the device holder without SCD, the TOE will be a QSCD only after generation of the first SCD/SVD pair. Because this SCD/SVD pair generation is performed by the Signatory in the operational use stage, the TOE provides additional security functionality addressed by OT.TOE_QSCD_Auth and OT.TOE_TC_SVD_Exp. But this security functionality must be initialized by the QSCD provisioning service as described in OE.Dev_Prov_Service. Therefore, PP Part 4 [R11] substitutes OE.QSCD_Prov_Service by OE.Dev_Prov_Service, allowing generation of the first SCD/SVD pair after delivery of the TOE to the device holder and requiring initialization of security functionality of the TOE. Nevertheless, the additional security functionality must be used by the operational environment as described in OE.CGA_QSCD_Auth and OE.CGA_TC_SVD_Imp. This approach does not weaken the security objectives and requirements for the TOE, but enforces more security functionalities of the TOE for additional methods of use. Therefore, it does not conflict with the CC conformance claim to PP Part 2 [R10].*

Here below are the security objectives for the operational environment defined in PP Part 5 [R12].

5.2.8 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 8 *This security objective for the TOE is partly covering OE.HID_VAD from PP Part 2 [R10]. While OE.HID_VAD in PP Part 2 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, PP Part 5 [R12] partly re-assigns 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.*

5.2.9 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 9 *This security objective for the TOE is partly covering OE.DTBS_Protect from PP Part 2 [R10]. While OE.DTBS_Protect in PP Part 2 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, PP Part 5 [R12] partly re-assigns 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.*

6. Security objectives rationale

6.1 Coverage of security objectives

Table 6-1 and Table 6-2 map the elements of the security problem definition to the security objectives for the TOE and for the operational environment, respectively. The rows are split according to the kind of element (threats, OSPs, assumptions), while the columns are split according to the source of the security objectives (PP Part 2 [R10], PP Part 4 [R11], PP Part 5 [R12], or this security target).

Table 6-1 Mapping of the security problem definition to the security objectives for the TOE

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_QSCD_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	OT.AC_Init	OT.AC_Pers
T.SCD_Divulg					X												
T.SCD_Derive		X				X											
T.Hack_Phys					X				X	X	X						
T.SVD_Forgery				X									X				
T.SigF_Misuse	X						X	X						X	X		
T.DTBS_Forgery								X							X		
T.Sig_Forgery			X			X											
P.CSP_QCert	X			X								X					
P.QSign						X	X										
P.Sigy_QSCD	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		
P.Manufact																X	
P.Personalization		X															X
A.CGA																	
A.SCA																	

Table 6-2 Mapping of the security problem definition to the security objectives for the operational environment

	OE.CGA_QCert	OE.SVD_Auth	OE.DTBS_Intend	OE.Signatory	OE.Dev_Prov_Service	OE.CGA_QSCD_Auth	OE.CGA_TC_SVD_Imp	OE.HID_TC_VAD_Exp	OE.SCA_TC_DTBS_Exp
T.SCD_Divulg									
T.SCD_Derive									
T.Hack_Phys									
T.SVD_Forgery		X					X		
T.SigF_Misuse			X	X				X	X
T.DTBS_Forgery			X						X
T.Sig_Forgery	X								
P.CSP_QCert	X					X			
P.QSign	X		X						
P.Sigy_QSCD					X	X	X		
P.Sig_Non-Repud	X	X	X	X	X	X	X	X	X
P.Manufact					X				
P.Personalization					X				
A.CGA	X	X							
A.SCA			X						

6.2 Sufficiency of security objectives

In PP Part 4 [R11], the rationale for T.SCD_Divulg, T.SCD_Derive, T.Hack_Phys, T.SigF_Misuse, T.DTBS_Forgery, T.Sig_Forgery, P.QSign, A.CGA, and A.SCA remains unchanged as given in PP Part 2 [R10], section 7.3.2. The rationale how security objectives address threats T.SCD_Divulg, T.SVD_Forgery and policies P.CSP_QCert, P.Sigy_QSCD, and P.Sig_Non-Repud changes as reported below.
In PP Part 5 [R12], the rationale for T.Hack_Phys, T.SCD_Divulg, T.SCD_Derive, T.Sig_Forgery, T.SVD_Forgery, P.CSP_QCert, P.QSign, A.CGA, and A.SCA remains unchanged as given in PP Part 2 [R10], section 7.3.2. The rationale how security objectives address threats T.DTBS_Forgery, T.SigF_Misuse and policy P.Sig_Non-Repud changes as reported below.

Here below is the rationale borrowed from PP Part 2 [R10].

T.SCD_Divulg *(Storing, copying and releasing of the signature creation data)* addresses the threat against the legal validity of electronic signature, as expressed in recital (18) of [R15], and confidentiality of encrypted data due to storage and copying of SCD outside the TOE. This threat is countered by ***OT.SCD_Secrecy***, which assures the secrecy of the SCD used for signature creation.

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

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 by detecting and by resisting tampering attacks.

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

P.QSign *(Qualified electronic signatures)* states 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.

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***, 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***, which ensures the generation of qualified certificates, and by ***OE.SVD_Auth***, which ensures the protection of the integrity of the received SVD and the verification of the correspondence between the SVD and the SCD that is implemented by the QSCD of the Signatory.

Here below is the rationale borrowed from PP Part 4 [R11].

T.SVD_Forgery *(Forgery of Signature Verification Data)* deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate. The threat 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, signature creation with the SCD, and by ***OE.SVD_Auth***, which ensures the integrity of the SVD exported by the TOE to the CGA and verification of the correspondence between the SCD in the QSCD of the Signatory and the SVD in the input provided to the certificate generation function of the CSP. Additionally, the threat 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.

P.CSP_QCert *(CSP generates qualified certificates)* states that the TOE and the SCA may be employed to sign data with (qualified) electronic signatures, as defined by [R15], article 5, paragraph 1. [R15], recital (15) refers to QSCDs to ensure the functionality of advanced signatures. ***OE.CGA_QCert*** addresses the requirement of qualified (or advanced) electronic signatures as being based on qualified (or non-qualified) certificates. According to ***OT.TOE_QSCD_Auth***, the copies of the TOE will hold unique identity and authentication data as QSCD and provide security mechanisms enabling the CGA to identify and to authenticate the TOE as QSCD. ***OE.CGA_QSCD_Auth*** ensures that the CSP checks the proof that the device is a QSCD presented by the applicant. ***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. ***OT.Lifecycle_Security*** ensures that the TOE detects flaws during initialization, personalization, and operational usage.

P.Sigy_QSCD *(TOE as Secure Signature Creation Device)* requires the TOE to meet [R15], Annex III. Paragraph 1(a) of Annex III is ensured by ***OT.SCD_Unique***, requiring that the SCD used for signature creation can practically occur only once. ***OT.SCD_Secrecy***, ***OT.Sig_Secure***, ***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 requirement 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 requirement 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 requirement in paragraph 2 of Annex III as the TOE must not alter the DTBS/R. The usage of SCD under sole control of the Signatory is ensured by ***OT.Lifecycle_Security***, ***OT.SCD/SVD_Auth_Gen***, and ***OT.Sigy_SigF***.

OE.Dev_Prov_Service ensures that the legitimate user obtains a TOE sample as an authentic, initialized, and personalized TOE from a QSCD provisioning service through the TOE delivery procedure. If the TOE implements SCD generated under control of the QSCD provisioning service, the legitimate user receives the TOE as QSCD. If the TOE is delivered to the legitimate user without SCD, in the operational phase the user 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 security objectives ***OT.TOE_QSCD_Auth*** and ***OT.TOE_TC_SVD_Exp***) to check whether the device presented is a QSCD linked to the applicant, as required by ***OE.CGA_QSCD_Auth***, and whether the received SVD is sent by this QSCD, as required by ***OE.CGA_TC_SVD_Imp***. Thus, the obligation of the QSCD provisioning service for the first SCD/SVD pair is complemented in an appropriate way by the CSP for the SCD/SVD pair generated outside a secure preparation environment.

Here below is the rationale borrowed from PP Part 5 [R12].

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 an SDO by others than the Signatory, or 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 [R15], Annex III. ***OT.Lifecycle_Security*** requires the TOE to detect flaws during initialization, personalization, and operational usage, including secure destruction of the SCD, which may be initiated by the Signatory. ***OT.Sigy_SigF*** ensures that the TOE provides the signature creation function for the legitimate Signatory only. ***OE.DTBS_Intend*** ensures that the SCA sends the DTBS/R only for data that the Signatory intends to sign. The combination of ***OT.TOE_TC_DTBS_Imp*** and ***OE.SCA_TC_DTBS_Exp*** counters the undetected manipulation of the DTBS during the transmission from the SCA to the TOE. ***OT.DTBS_Integrity_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*** 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 them according to ***OE.HID_TC_VAD_Exp*** and ***OT.TOE_TC_VAD_Imp***. ***OE.Signatory*** ensures that the Signatory checks that an SCD stored in the QSCD, when received from a QSCD provisioning service provider, is in non-operational state, i.e. the SCD cannot be used before the Signatory obtains control over the QSCD. ***OE.Signatory*** also ensures 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 then does not match the DTBS/R corresponding to the DTBS that the Signatory intends to sign. The threat is addressed by security objectives ***OT.TOE_TC_DTBS_Imp*** and ***OE.SCA_TC_DTBS_Exp***, 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 means of ***OT.DTBS_Integrity_TOE***, ensuring the integrity of the DTBS/R inside the TOE. The TOE IT environment also addresses the threat by 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.

Here below is the rationale for policy P.Sig_Non-Repud, resulting from the combination of the rationales provided in PP Part 4 [R11] and PP Part 5 [R12].

P.Sig_Non-Repud *(Non-repudiation of signatures)* deals with the repudiation of signed data by the Signatory, although the electronic signature is successfully verified with the SVD contained in their certificate valid at the time of signature creation. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, that ensure the aspects of Signatory's sole control over and responsibility for the electronic signatures generated with the TOE. ***OE.Dev_Prov_Service*** ensures that the Signatory uses an authentic TOE, initialized and personalized 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*** ensures that the Signatory's SCD can practically occur just once.
OE.Signatory ensures that the Signatory checks that the SCD stored in the QSCD received from a QSCD provisioning service is in non-operational state (i.e. the SCD cannot be used before the Signatory obtains sole control over the QSCD). The TOE security feature addressed by security objectives ***OT.TOE_QSCD_Auth*** and ***OT.TOE_TC_SVD_Exp***, supported by ***OE.Dev_Prov_Service***, enables the verification whether the device presented by the applicant is a QSCD, as required by ***OE.CGA_QSCD_Auth***, and whether the received SVD is sent by the device holding the corresponding SCD, as required by ***OE.CGA_TC_SVD_Imp***. ***OT.Sigy_SigF*** ensures 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 HID and the TOE according to ***OE.HID_TC_VAD_Exp*** and ***OT.TOE_TC_VAD_Imp***. ***OE.DTBS_Intend***, ***OT.DTBS_Integrity_TOE***, ***OE.SCA_TC_DTBS_Exp***, and ***OT.TOE_TC_DTBS_Imp*** 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. Security objectives for the TOE ***OT.Lifecycle_Security***, ***OT.SCD_Secrecy***, ***OT.EMSEC_Design***, ***OT.Tamper_ID***, and ***OT.Tamper_Resistance*** protect the SCD against any compromise.

Here below is the rationale for the elements of the security problem definition added in this security target to those defined in the PPs.

P.Manufact *(Manufacturing of the e-Document)* requires the storage of TOE initialization data to be restricted to the Initialization Agent, which is ensured by ***OT.AC_Init***. Furthermore, since access control requires user authentication, the secure storage of the initialization key and the personalization key prescribed by the policy is implied by ***OT.AC_Init***. Finally, the fact that the Initialization Agent acts on behalf of the QSCD provisioning service, as stated by the policy, is implied by ***OE.Dev_Prov_Service***, which puts the whole preparation of the TOE for its use as QSCD on the part of the Signatory under the responsibility of the QSCD provisioning service.

P.Personalization *(Personalization of the e-Document)* requires the storage of personalization data to be restricted to the Personalization Agent, which is ensured by ***OT.AC_Pers***. Furthermore, since access control requires user authentication, the secure storage of Administrator's and Signatory's credentials prescribed by the policy is implied by ***OT.SCD/SVD_Auth_Gen***. Finally, the fact that the Personalization Agent acts on behalf of the QSCD provisioning service, as stated by the policy, is implied by ***OE.Dev_Prov_Service***, which puts the whole preparation of the TOE for its use as QSCD on the part of the Signatory under the responsibility of the QSCD provisioning service.

7. Extended components definition

7.1 Definition of family FPT_EMS

The additional family FPT_EMS (TOE emanation) of class FPT (Protection of the TSF) is defined in PP Part 2 [R10] 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 electromagnetic radiation, Simple Power Analysis (SPA), Differential Power Analysis (DPA), timing attacks, radio emanation, etc.
Family FPT_EMS describes the functional requirements for the limitation of intelligible emanations. This family belongs to class FPT because it is the class for TSF protection. Other families within class FPT do not cover TOE emanations.

FPT_EMS TOE emanation

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

Component levelling:

FPT_EMS.1 (TOE emanation) has two constituents:

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be auditable.

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 emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

FPT_EMS.1.2:

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

7.2 Definition of family FIA_API

The additional family FIA_API (Authentication proof of identity) of class FIA (Identification and authentication) is defined in PP Part 4 [R11] to describe the IT security functional requirements of the TOE.
This family describes the functional requirements for the proof of the claimed identity of the TOE by an external entity, whereas the other families of 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 its identity and to be verified by an external entity in the TOE IT environment.

Component levelling:

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

8. Security functional requirements

Common Criteria allow several operations to be performed on functional requirements: *refinement*, *selection*, *assignment*, and *iteration* (cf. [R7], section 8.1). Each of these operations is used in this security target.

A (non-editorial) **refinement** operation is used to add details to a requirement, and thus further restricts a requirement (as regards the distinction between editorial and non-editorial refinements, cf. [R7], section 8.1.4). Non-editorial refinements of security requirements are written in **bold** text for additions or changes, in ~~strikethrough~~ text for deletions, and those made by the authors of this security target on the requirements borrowed from the PPs are signalled by an application note.

A **selection** operation is used to select one or more options provided by the CC in stating a requirement. A selection that has been made in the PPs is indicated as underlined text, and the original text of the component is given by a footnote. Selections filled in by the authors of this security target are written in **underlined bold** text, and the original text of the component is given by a footnote.

An **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment that that has been made in the PPs is indicated as underlined text, and the original text of the component is given by a footnote. Assignments filled in by the authors of this security target are written in **underlined bold** text, and the original text of the component is given by a footnote.

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

Table 8-1 maps each SFR stated in this security target to the PPs in which it is defined, if any. Particularly, SFR FIA_UAU.1 is mapped to both PP Part 4 [R11] and PP Part 5 [R12] since both PPs extend the formulation of the SFR given in PP Part 2 [R10]. Therefore, the formulation of the SFR given in this security target results from the combination of those given in PP Part 4 and PP Part 5.

Table 8-1 Mapping of the security functional requirements to the PPs

Security functional requirement	PP Part 2	PP Part 4	PP Part 5
FCS_CKM.1/RSA	X		
FCS_CKM.1/ECDSA	X		

Security functional requirement	PP Part 2	PP Part 4	PP Part 5
FCS_CKM.4	X		
FCS_COP.1/RSA	X		
FCS_COP.1/ECDSA	X		
FDP_ACC.1/SCD/SVD_Generation	X		
FDP_ACF.1/SCD/SVD_Generation	X		
FDP_ACC.1/SVD_Transfer	X		
FDP_ACF.1/SVD_Transfer	X		
FDP_ACC.1/Signature_Creation	X		
FDP_ACF.1/Signature_Creation	X		
FDP_RIP.1	X		
FDP_SDI.2/Persistent	X		
FDP_SDI.2/DTBS	X		
FDP_DAU.2/SVD		X	
FDP_UIT.1/DTBS			X
FIA_UID.1	X		
FIA_UAU.1		X	X
FIA_AFL.1	X		
FIA_API.1		X	
FMT_SMR.1/QSCD	X		
FMT_SMR.1/Init			
FMT_SMR.1/Pers			
FMT_SMF.1	X		
FMT_MOF.1	X		
FMT_MSA.1/Admin	X		
FMT_MSA.1/Signatory	X		
FMT_MSA.2	X		
FMT_MSA.3	X		
FMT_MSA.4	X		
FMT_MTD.1/Admin	X		
FMT_MTD.1/Signatory	X		
FMT_MTD.1/Init			
FMT_MTD.1/Pers			

Security functional requirement	PP Part 2	PP Part 4	PP Part 5
FPT_EMS.1	X		
FPT_FLS.1	X		
FPT_PHP.1	X		
FPT_PHP.3	X		
FPT_TST.1	X		
FTP_ITC.1/SVD		X	
FTP_ITC.1/VAD			X
FTP_ITC.1/DTBS			X
FTP_ITC.1/Init			
FTP_ITC.1/Pers			

8.1 Class FCS: Cryptographic support

8.1.1 FCS_CKM.1/RSA

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 **SCD/SVD pairs** in accordance with a specified cryptographic key generation algorithm **two-prime RSA**[4] and specified cryptographic key sizes **2048, 3072, 4096 bits**[5] that meet the following: **PKCS #1 [R43]**[6].

Application Note 10 *The refinement in the element FCS_CKM.1.1 substitutes "cryptographic keys" with "SCD/SVD pairs" because it clearly addresses the SCD/SVD key generation.*

[4] [assignment: *cryptographic key generation algorithm*]
[5] [assignment: *cryptographic key sizes*]
[6] [assignment: *list of standards*]

8.1.2 FCS_CKM.1/ECDSA

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 **SCD/SVD pairs** in accordance with a specified cryptographic key generation algorithm **ECDSA with SHA-256, SHA-384 and SHA-512**[7] and specified cryptographic key sizes **256, 320, 384, 512 and 521 bits**[8] that meet the following: **FIPS 186-4 [R36]**[9].

Application Note 11 *The refinement in the element FCS_CKM.1.1 substitutes "cryptographic keys" with "SCD/SVD pairs" because it clearly addresses the SCD/SVD key generation.*

8.1.3 FCS_CKM.4

Cryptographic key destruction

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.4.1:

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **physical**

---

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

deletion by overwriting the memory data with zeros[10] that meets the following: **none**[11].

8.1.4 FCS_COP.1/RSA

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/RSA:

The TSF shall perform digital signature creation[12] in accordance with a specified cryptographic algorithm **RSASSA-PKCS1-v1_5 with SHA-256, SHA-512 and RSASSA-PSS with SHA-256, SHA-512**[13] and cryptographic key sizes **2048, 3072, 4096 bits**[14] that meet the following: **PKCS #1 [R43], FIPS PUB 180-4 [R35]**[15].

8.1.5 FCS_COP.1/ECDSA

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/ECDSA:

---

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

The TSF shall perform digital signature creation[16] in accordance with a specified cryptographic algorithm **ECDSA with SHA-256, SHA-384, SHA-512**[17] and cryptographic key sizes **256, 320, 384, 512 and 521 bits**[18] that meet the following: **Elliptic Curve Cryptography [R6], FIPS PUB 180-4 [R35]**[19].

Application Note 12 *For EC cryptography, the TOE makes use of the NXP cryptographic library. The cryptographic requirement REQ_ECC_POINT_MULT defined in section 6.4 of [R39] do not apply to the TOE because the ECC point multiplication is never used in protocol other than Diffie Hellman Key Exchange and ECDSA.*

8.2 Class FDP: User data protection

The security attributes of subjects and objects relevant for access control and the related values are reported in Table 8-2.

Table 8-2 Security attributes of subjects and objects for access control

Subject or object	Security attribute	Security attribute values
S.User	Role	R.Admin, R.Sigy
S.User	SCD/SVD management	authorized, not authorized
SCD	SCD operational	no, yes
SCD	SCD identifier	arbitrary value
SVD	-	-

Application Note 13 *The roles of R.Admin and R.Sigy are directly related to the definitions of Administrator and Signatory (cf. section 2.2).*

8.2.1 FDP_ACC.1/SCD/SVD_Generation

Subset access control

Hierarchical to: No other components.

[16] [assignment: *list of cryptographic operations*]
[17] [assignment: *cryptographic algorithm*]
[18] [assignment: *cryptographic key sizes*]
[19] [assignment: *list of standards*]

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[20] on

- subjects: S.User;
- objects: SCD, SVD;
- operations: generation of SCD/SVD pairs[21].

8.2.2 FDP_ACF.1/SCD/SVD_Generation

Security attribute based access control

Hierarchical to: No other components.

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

FDP_ACF.1.1/SCD/SVD_Generation:

The TSF shall enforce the SCD/SVD Generation SFP[22] to objects based on the following: the user S.User is associated with the security attribute "SCD/SVD management"[23].

FDP_ACF.1.2/SCD/SVD_Generation:

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

S.User with the security attribute "SCD/SVD management" set to "authorized" is allowed to generate SCD/SVD pair[24].

FDP_ACF.1.3/SCD/SVD_Generation:

---

[20] [assignment: *access control SFP*]
[21] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[22] [assignment: *access control SFP*]
[23] [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*]
[24] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[25].

FDP_ACF.1.4/SCD/SVD_Generation:

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

S.User with the security attribute "SCD/SVD management" set to "not authorized" is not allowed to generate SCD/SVD pair[26].

Application Note 14 *Both the Administrator and the Signatory are allowed to generate SCD/SVD pairs (cf. section 2.2.2).*

8.2.3 FDP_ACC.1/SVD_Transfer

Subset access control

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[27] on

- subjects: S.User;
- objects: SVD;
- operations: export[28].

8.2.4 FDP_ACF.1/SVD_Transfer

Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

---

[25] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
[26] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[27] [assignment: *access control SFP*]
[28] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/SVD_Transfer:

The TSF shall enforce the SVD Transfer SFP[29] to objects based on the following:

- the S.User is associated with the security attribute "Role";
- the SVD[30].

FDP_ACF.1.2/SVD_Transfer:

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **R.Admin, R.Sigy**[31] are allowed to export SVD[32].

FDP_ACF.1.3/SVD_Transfer:

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[33].

FDP_ACF.1.4/SVD_Transfer:

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[34].

Application Note 15 *Both the Administrator and the Signatory are allowed to export SVD to the CGA in order to apply for certificates (cf. section 2.2.2).*

8.2.5 FDP_ACC.1/Signature_Creation

Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

[29] [assignment: *access control SFP*]
[30] [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*]
[31] [selection: *R.Admin, R.Sigy*]
[32] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[33] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
[34] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

FDP_ACC.1.1/Signature_Creation:

The TSF shall enforce the Signature Creation SFP[35] on

- subjects: S.User;
- objects: DTBS/R, SCD;
- operations: signature creation[36].

8.2.6 FDP_ACF.1/Signature_Creation

Security attribute based access control

Hierarchical to: No other components.

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

FDP_ACF.1.1/Signature_Creation:

The TSF shall enforce the Signature Creation SFP[37] to objects based on the following:

- the user S.User is associated with the security attribute "Role", and
- the SCD with the security attribute "SCD Operational"[38].

FDP_ACF.1.2/Signature_Creation:

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

R.Sigy is allowed to create electronic signatures for DTBS/R with SCD whose security attribute "SCD operational" is set to "yes"[39].

---

35 [assignment: *access control SFP*]
36 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
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*]
39 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

FDP_ACF.1.3/Signature_Creation:

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[40].

FDP_ACF.1.4/Signature_Creation:

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

S.User is not allowed to create electronic signatures for DTBS/R with SCD whose security attribute "SCD operational" is set to "no"[41].

8.2.7 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[42] the following objects: SCD[43].

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

- SCD;
- SVD.

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

8.2.8 FDP_SDI.2/Persistent

Stored data integrity monitoring and action

40 [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
41 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
42 [selection: *allocation of the resource to, deallocation of the resource from*]
43 [assignment: *list of objects*]

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies.

FDP_SDI.2.1/Persistent:

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

FDP_SDI.2.2/Persistent:

Upon detection of a data integrity error, the TSF shall

- prohibit the use of the altered data;
- inform the S.Sigy about the integrity error[46].

8.2.9 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 errors[47] on all objects, based on the following attributes: integrity checked stored DTBS[48].

FDP_SDI.2.2/DTBS:

Upon detection of a data integrity error, the TSF shall

- prohibit the use of the altered data;
- inform the S.Sigy about the integrity error[49].

---

44 [assignment: *integrity errors*]
45 [assignment: *user data attributes*]
46 [assignment: *action to be taken*]
47 [assignment: *integrity errors*]
48 [assignment: *user data attributes*]
49 [assignment: *action to be taken*]

Application Note 16 *The integrity of TSF data like RAD is also protected to ensure the effectiveness of the user authentication.*

8.2.10 FDP_DAU.2/SVD

Data authentication with Identity of Guarantor

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[50].

FDP_DAU.2.2/SVD:

The TSF shall provide the CGA[51] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

8.2.11 FDP_UIT.1/DTBS

Data exchange integrity

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]

FDP_UIT.1.1/DTBS:

The TSF shall enforce the Signature Creation SFP[52] to receive[53] user data in a manner protected from modification and insertion[54] errors.

[50] [assignment: *list of objects or information types*]
[51] [assignment: *list of subjects*]
[52] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[53] [selection: *transmit, receive*]
[54] [selection: *modification, deletion, insertion, replay*]

FDP_UIT.1.2/DTBS:

The TSF shall be able to determine on receipt of user data, whether modification or insertion[55] has occurred.

8.3 Class FIA: Identification and authentication

8.3.1 FIA_UID.1

Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1:

The TSF shall allow

- self-test according to FPT_TST.1,
- **establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD;**
- **establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD;**
- **establishing a trusted channel between the Initialization Agent's terminal and the TOE by means of TSF required by FTP_ITC.1/Init;**
- **establishing a trusted channel between the Personalization Agent's terminal and the TOE by means of TSF required by FTP_ITC.1/Pers[56] [57];**

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

FIA_UID.1.2:

[55] [selection: *modification, deletion, insertion, replay*]
[56] [assignment: *list of additional TSF-mediated actions*]
[57] [assignment: *list of TSF-mediated actions*]

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

8.3.2 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

- self-test according to FPT_TST.1;
- ~~identification of the user by means of TSF required by FIA_UID.1;~~
- establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD;
- establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD;
- **establishing a trusted channel between the Initialization Agent's terminal and the TOE by means of TSF required by FTP_ITC.1/Init;**
- **establishing a trusted channel between the Personalization Agent's terminal and the TOE by means of TSF required by FTP_ITC.1/Pers**[58] [59].

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.

[58] [assignment: *list of additional TSF-mediated actions*]
[59] [assignment: *list of TSF-mediated actions*]

Application Note 17 *The TOE does not maintain any user identification information prior to user authentication; namely, the user is regarded as an unidentified terminal until user authentication is accomplished. Hence, this security target refines the element FIA_UAU.1.1 by deleting the bullet (2).*

Application Note 18 *PP Part 4 [R11] performs the assignment of the bullet (3) in the element FIA_UAU.1.1 of PP Part 2 [R10] by adding the establishment of a trusted channel to the CGA.*

Application Note 19 *PP Part 5 [R12] performs the assignment of the bullet (3) in the element FIA_UAU.1.1 of PP Part 2 [R10] by adding the establishment of a trusted channel to the HID.*

8.3.3 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 **an administrator configurable positive integer within 1-15**[60] unsuccessful authentication attempts occur related to consecutive failed authentication attempts[61].

FIA_AFL.1.2:

When the defined number of unsuccessful authentication attempts has been met[62], the TSF shall block RAD[63].

8.3.4 FIA_API.1

Authentication proof of identity

Hierarchical to: No other components.

---

[60] [selection: *[assignment: positive integer number]*, *an administrator configurable positive integer within [assignment: range of acceptable values]*]
[61] [assignment: *list of authentication events*]
[62] [selection: *met, surpassed*]
[63] [assignment: *list of actions*]

Dependencies: No dependencies.

FIA_API.1.1:

The TSF shall provide **General Authentication Protocol compliant with *TR-03110-2***[64] to prove the identity of the QSCD[65].

Application Note 20 *Via General Authentication Protocol, the TOE is able to authenticate itself as QSCD to the CGA (cf. section 2.2.2).*

Application Note 21 *For PACE-PIN, the key lengths that can be used are limited to 256, 384 and 512 bits. For PACE-CAN, all key sizes can be used* (cf. section 6.4 of [R39]).

8.4 Class FMT: Security management

8.4.1 FMT_SMR.1/QSCD

Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1/QSCD:

The TSF shall maintain the roles R.Admin and R.Sigy[66].

FMT_SMR.1.2/QSCD:

The TSF shall be able to associate users with roles.

Application Note 22 *The roles of R.Admin and R.Sigy are directly related to the definitions of Administrator and Signatory (cf. section 2.2).*

[64] [assignment: *authentication mechanism*]
[65] [assignment: *authorized user or role*]
[66] [assignment: *the authorized identified roles*]

8.4.2 FMT_SMR.1/Init

Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1/Init:

The TSF shall maintain the roles **R.Init**[67].

FMT_SMR.1.2/Init:

The TSF shall be able to associate users with roles.

8.4.3 FMT_SMR.1/Pers

Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1/Pers:

The TSF shall maintain the roles **R.Pers**[68].

FMT_SMR.1.2/Pers:

The TSF shall be able to associate users with roles.

8.4.4 FMT_SMF.1

Specification management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1:

---

[67] [assignment: *the authorized identified roles*]
[68] [assignment: *the authorized identified roles*]

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

- creation and modification of RAD;
- enabling the signature creation function;
- modification of the security attribute "SCD/SVD management", "SCD operational";
- change the default value of the security attribute "SCD identifier";
- **unblock of RAD,**
- **writing TOE initialization data,**
- **writing personalization data**[69] [70].

8.4.5 FMT_MOF.1

Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MOF.1.1:

The TSF shall restrict the ability to enable[71] the functions signature creation function[72] to R.Sigy[73].

Application Note 23 *The TOE distinguishes between S.Admin or S.Sigy based on the effective authorization obtained from GAP [R1].*

8.4.6 FMT_MSA.1/Admin

Management of security attributes

Hierarchical to: No other components.

---

69 [assignment: *list of other security management functions to be provided by the TSF*]
70 [assignment: *list of security management functions to be provided by the TSF*]
71 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
72 [assignment: *list of functions*]
73 [assignment: *the authorized identified roles*]

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/SVD Generation SFP[74] to restrict the ability to modify[75] [76] the security attributes SCD/SVD management[77] to R.Admin[78].

Application Note 24 *The TOE distinguishes between S.Admin or S.Sigy based on the effective authorization obtained from GAP [R1].*

8.4.7 FMT_MSA.1/Signatory

Management of security attributes

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[79] to restrict the ability to modify[80] the security attributes SCD operational[81] to R.Sigy[82].

Application Note 25 *The TOE distinguishes between S.Admin or S.Sigy based on the effective authorization obtained from GAP [R1].*

---

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

8.4.8 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 SCD/SVD management and SCD operational[83].

Application Note 26 *Since the TOE supports generation of SCD/SVD pairs on the part of the Signatory and a trusted channel for export of the SVD to the CGA, the security attribute "SCD/SVD management" is set to "yes" for both of subjects S.Admin and S.Sigy (cf. sections 2.2.2, 2.3.4).*

8.4.9 FMT_MSA.3

Static attribute initialization

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/SVD Generation SFP, SVD Transfer SFP and Signature Creation SFP[84] to provide restrictive[85] default values for security attributes that are used to enforce the SFP.

---

[83] [assignment: *list of security attributes*]
[84] [assignment: *access control SFP, information flow control SFP*]
[85] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

FMT_MSA.3.2:

The TSF shall allow the R.Admin[86] to specify alternative initial values to override the default values when an object or information is created.

8.4.10 FMT_MSA.4

Security attribute value inheritance

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
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:

- If S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated, the security attribute "SCD operational of the SCD" shall be set to "no" as a single operation.
- If S.Sigy successfully generates an SCD/SVD pair, the security attribute "SCD operational of the SCD" shall be set to "yes" as a single operation[87].

Application Note 27 *The TOE distinguishes between S.Admin or S.Sigy based on the effective authorization obtained from GAP [R1].*

8.4.11 FMT_MTD.1/Admin

Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

[86] [assignment: *the authorized identified roles*]
[87] [assignment: *rules for setting the values of security attributes*]

FMT_MTD.1.1/Admin:

The TSF shall restrict the ability to create[88] the RAD[89] to ~~R.Admin~~ **none**[90].

Application Note 28 *According to the Administrator definition given in section 2.2, the R.Admin can not create the RAD in Operational use phase. The RAD is created by the Personalization Agent in Personalization phase (cf. FMT_MTD.1/Pers).*

8.4.12 FMT_MTD.1/Signatory

Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MTD.1.1/Signatory:

The TSF shall restrict the ability to modify, **unblock, resume**[91] [92] the RAD[93] to R.Sigy[94].

8.4.13 FMT_MTD.1/Init

Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MTD.1.1/Init:

---

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

The TSF shall restrict the ability to **write**[95] the **TOE initialization data**[96] to **R.Init**[97].

8.4.14 FMT_MTD.1/Pers

Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MTD.1.1/Pers:

The TSF shall restrict the ability to **write**[98] the **personalization data**[99] to **R.Pers**[100].

Application Note 29 *The personalization data are written in Personalization and include the RAD.*

8.5 Class FPT: Protection of the TSF

8.5.1 FPT_EMS.1

TOE emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1:

---

95 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
96 [assignment: *list of TSF data*]
97 [assignment: *the authorized identified roles*]
98 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
99 [assignment: *list of TSF data*]
100 [assignment: *the authorized identified roles*]

The TOE shall not emit **any measurable emissions**[101] in excess of **intelligible thresholds**[102] enabling access to RAD[103] and SCD[104].

FPT_EMS.1.2:

The TSF shall ensure **any users**[105] are unable to use the following interface **contact-based/contactless interface and circuit contacts**[106] to gain access to RAD[107] and SCD[108].

Application Note 30 *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.*

8.5.2 FPT_FLS.1

Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1:

101 [assignment: *types of emissions*]
102 [assignment: *specified limits*]
103 [assignment: *list of types of TSF data*]
104 [assignment: *list of types of user data*]
105 [assignment: *type of users*]
106 [assignment: *type of connection*]
107 [assignment: *list of types of TSF data*]
108 [assignment: *list of types of user data*]

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

- self-test according to FPT_TST fails;
- **a physical attack is detected**[109] [110].

Application Note 31 *The assignments address failures detected by a failed self-test or revealing the occurrence of a physical attack and requiring appropriate action to prevent security violations. When the TOE is in a secure state, the TSF shall not perform any cryptographic operations, and all data output interfaces shall be inhibited by the TSF.*

8.5.3 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.

8.5.4 FPT_PHP.3

Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1:

---

[109] [assignment: *list of other types of failures in the TSF*]
[110] [assignment: *list of types of failures in the TSF*]

The TSF shall resist **physical manipulation and physical probing**[111] to the **TSF**[112] by responding automatically such that the SFRs are always enforced.

Application Note 32 *The TOE will implement appropriate measures to continuously counter physical tampering which may compromise the SCD. The "automatic response" in the element FPT_PHP.3.1 means (i) assuming that there might be an attack at any time, and (ii) countermeasures are provided at any time. Due to the nature of these attacks, the TOE can by no means detect attacks on all of its elements (e.g. the TOE is destroyed). But physical tampering must not reveal information of the SCD. E.g. the TOE may be physically tampered in the power-off state of the TOE, which does not allow the TSF for overwriting the SCD, but leads to physical destruction of the memory and all information therein about the SCD. In case of physical tampering, the TSF may not provide the intended functions for SCD/SVD pair generation, signature creation, but ensures the confidentiality of the SCD by blocking these functions. The SFR FPT_PHP.1 requires the TSF to react to physical tampering in such a way that the Signatory is able to determine whether the TOE was physically tampered or not. The guidance documentation identifies the failure of TOE start-up as an indication of physical tampering [R21] [R23] [R25].*

8.5.5 FPT_TST.1

TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1:

The TSF shall run a suite of self-tests **during initial start-up, and at the conditions: when the applet is selected**[113] to demonstrate the correct operation of the TSF[114].

FPT_TST.1.2:

---

[111] [assignment: *physical tampering scenarios*]

[112] [assignment: *list of TSF devices/elements*]

[113] [selection: *during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self-test should occur]*]

[114] [selection: *[assignment: parts of TSF], the TSF*]

The TSF shall provide authorized users with the capability to verify the integrity of TSF data[115].

FPT_TST.1.3:

The TSF shall provide authorized users with the capability to verify the integrity of TSF[116].

Application Note 33 *The Applet is automatically selected at the initial start-up. At the selection, the Applet checks that is running on the expected platform JCOP 4 P71, using a specific function provided by the platform. In case of failure, the Applet will raise a security exception to the platform.*

Application Note 34 *The Applet will check the attack logger on selection. In case the counter is zero, the Applet will raise a security exception to the platform.*

8.6 Class FTP: Trusted path/channels

8.6.1 FTP_ITC.1/SVD

Inter-TSF trusted channel

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[117] to initiate communication via the trusted channel.

[115] [selection: *[assignment: parts of TSF data], TSF data*]
[116] [selection: *[assignment: parts of TSF], TSF*]
[117] [selection: *the TSF, another trusted IT product*]

FTP_ITC.1.3/SVD:

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

- data authentication with identity of guarantor according to FIA_API.1 and FDP_DAU.2/SVD;
- **import of certificate info from the CGA**[118] [119].

Application Note 35 *The component FTP_ITC.1/SVD requires the TSF to enforce a trusted channel established by the CGA to export the SVD to the CGA. Moreover, the TSF requires the use of the same trusted channel for the import of certificate info from the CGA (cf. section 2.2.2).*

8.6.2 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[120] 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

- user authentication according to FIA_UAU.1;

[118] [assignment: *list of other functions for which a trusted channel is required*]
[119] [assignment: *list of functions for which a trusted channel is required*]
[120] [selection: *the TSF, another trusted IT product*]

- **<u>import of a new value of the RAD from the HID</u>**[121] [122].

Application Note 36 *The component FTP_ITC.1/VAD requires the TSF to enforce a trusted channel established by the HID to import the VAD from the HID. In more detail, the trusted channel is opened by means of GAP authentication.*

8.6.3 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 <u>the remote trusted IT product</u>[123] 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

- <u>signature creation;</u>
- **<u>export of digital signatures to the SCA</u>**[124] [125].

Application Note 37 *The component FTP_ITC.1/DTBS requires the TSF to enforce a trusted channel established by the SCA to import the DTBS from the SCA. Moreover, the*

121 [assignment: *list of other functions for which a trusted channel is required*]
122 [assignment: *list of functions for which a trusted channel is required*]
123 [selection: *the TSF, another trusted IT product*]
124 [assignment: *list of other functions for which a trusted channel is required*]
125 [assignment: *list of functions for which a trusted channel is required*]

TSF requires the use of the same trusted channel for the export of digital signatures to the SCA (cf. section 2.2.3).

8.6.4 FTP_ITC.1/Init

Inter-TSF trusted channel – TOE initialization data

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/Init:

The TSF shall provide a communication channel between itself and another trusted IT product**, the Initialization Agent's terminal,** 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/Init:

The TSF shall permit **another trusted IT product**[126] to initiate communication via the trusted channel.

FTP_ITC.1.3/Init:

The TSF **or the Initialization Agent's terminal** shall initiate communication via the trusted channel for **import of TOE initialization data from the terminal**[127].

Application Note 38 *The component* FTP_ITC.1/Init *requires the TSF to enforce a trusted channel established by the Initialization Agent's terminal to import TOE initialization data from the terminal. This trusted channel is established through a SCP03 authentication [R17]. For further information, cf. the initialization guidance [R21].*

8.6.5 FTP_ITC.1/Pers

Inter-TSF trusted channel – Personalization data

---

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/Pers:

The TSF shall provide a communication channel between itself and another trusted IT product**, the Personalization Agent's terminal,** 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/Pers:

The TSF shall permit **another trusted IT product**[128] to initiate communication via the trusted channel.

FTP_ITC.1.3/Pers:

The TSF **or the Personalization Agent's terminal** shall initiate communication via the trusted channel for **import of personalization data from the terminal**[129].

Application Note 39 *The component FTP_ITC.1/Pers requires the TSF to enforce a trusted channel established by the Personalization Agent's terminal to import personalization data from the terminal. This trusted channel is established through a SCP03 authentication. [R17]. For further information, cf. the personalization guidance [R23].*

---

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

9. Security assurance requirements

The Evaluation Assurance Level claimed by this security target is EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 [R9] (cf. section 3.2). Moreover, the refinements to security assurance requirements for composite product evaluations are also applied [R34].
Table 9-1 summarizes the security assurance requirements enforced by this Security Target.

Table 9-1 Security assurance requirements: EAL5 augmented with ALC_DVS.2 and AVA_VAN.5

Assurance class	Assurance components
ADV *Development*	ADV_ARC.1 *Security architecture description*
	ADV_FSP.5 *Complete semiformal 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*
ALC *Life cycle 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_CCL.1 *Conformance claims*
	ASE_ECD.1 *Extended components definition*
	ASE_INT.1

Assurance class	Assurance components
	ST introduction
	ASE_OBJ.2 *Security objectives*
	ASE_REQ.2 *Derived security requirements*
	ASE_SPD.1 *Security problem definition*
	ASE_TSS.1 *TOE summary specification*
ATE *Tests*	ATE_COV.2 *Analysis of coverage*
	ATE_DPT.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*

10. Security requirements rationale

10.1 Coverage of security functional requirements

Table 10-1 maps the security functional requirements to the security objectives for the TOE. The rows are split according to SFR classes, while the columns are split according to the source of the security objectives (PP Part 2 [R10], PP Part 4 [R11], PP Part 5 [R12], or this security target).

Table 10-1 Mapping of the security functional requirements to the security objectives for the TOE

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_QSCD_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	OT.AC_Init	OT.AC_Pers
FCS_CKM.1/ RSA	X		X	X	X												
FCS_CKM.1/ ECDSA	X		X	X	X												
FCS_CKM.4	X				X												
FCS_COP.1/ RSA	X					X											
FCS_COP.1/ ECDSA	X					X											
FDP_ACC.1/SCD/ SVD_Generation	X	X															
FDP_ACF.1/SCD/ SVD_Generation	X	X															
FDP_ACC.1/SVD _Transfer	X												X				
FDP_ACF.1/SVD_ Transfer	X												X				
FDP_ACC.1/Signa ture_Creation	X						X										
FDP_ACF.1/Signa ture_Creation	X						X										
FDP_RIP.1					X		X										

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_QSCD_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	OT.AC_Init	OT.AC_Pers
FDP_SDI.2/Persistent				X	X	X											
FDP_SDI.2/DTBS							X	X									
FDP_DAU.2/SVD													X				
FDP_UIT.1/DTBS															X		
FIA_UID.1		X					X									X	X
FIA_UAU.1		X					X					X				X	X
FIA_AFL.1							X										
FIA_API.1												X					
FMT_SMR.1/QSCD	X						X										
FMT_SMR.1/Init	X															X	
FMT_SMR.1/Pers	X																X
FMT_SMF.1	X			X			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			X										
FMT_MTD.1/Admin	X						X										

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_QSCD_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	OT.AC_Init	OT.AC_Pers
FMT_MTD.1/Signatory	X						X										
FMT_MTD.1/Init																X	
FMT_MTD.1/Pers																	X
FPT_EMS.1					X				X								
FPT_FLS.1					X												
FPT_PHP.1										X							
FPT_PHP.3					X						X						
FPT_TST.1	X				X	X											
FTP_ITC.1/SVD													X				
FTP_ITC.1/VAD														X			
FTP_ITC.1/DTBS															X		
FTP_ITC.1/Init																X	
FTP_ITC.1/Pers																	X

10.2 Sufficiency of security functional requirements

Here below is the rationale for the security objectives borrowed from PP Part 2 [R10].

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

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

OT.SCD_Unique *(Uniqueness of Signature Creation Data)* implements the requirement of practically unique SCD as laid down in [R15], 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 SFRs. ***FCS_CKM.1*** ensures the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of SCD/SVD pairs shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD. The security functions specified by ***FDP_RIP.1*** and ***FCS_CKM.4*** ensure that residual information on SCD is destroyed after the SCD has been used for signature creation and that destruction of SCD leaves no residual information.

The security functions specified by ***FDP_SDI.2/Persistent*** ensure that no critical data are modified which could alter the efficiency of the security functions or leak information on 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).

SFRs ***FPT_EMS.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 ensures the cryptographic robustness of the signature algorithms. ***FDP_SDI.2/Persistent*** corresponds to the integrity of the SCD implemented by the TOE and ***FPT_TST.1*** ensures self-tests ensuring correct signature creation.

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

FIA_UAU.1 and ***FIA_UID.1*** 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. SFR ***FIA_AFL.1*** provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by ***FDP_SDI.2/DTBS*** ensures the integrity of stored DTBS, and ***FDP_RIP.1*** prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature creation process).

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 SFRs ***FMT_MTD.1/Signatory***, ***FMT_MSA.2***, ***FMT_MSA.3*** and ***FMT_MSA.4***. The SFRs ***FMT_SMF.1*** and ***FMT_SMR.1/QSCD*** list these management functions and the roles. These ensure that the signature process is restricted to the Signatory. ***FMT_MOF.1*** restricts the ability to enable the signature creation function to the Signatory. ***FMT_MSA.1/Signatory*** restricts the ability to modify the security attribute SCD operational to the Signatory.

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

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

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

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

Here below is the rationale for the security objectives borrowed from PP Part 4 [R11].

OT.TOE_QSCD_Auth *(Authentication proof as QSCD)* requires the TOE to provide security mechanisms to identify and to authenticate itself as QSCD, which is directly provided by ***FIA_API.1***. The SFR ***FIA_UAU.1*** allows establishment of the trusted channel before the (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 the CGA with the ability to verify evidence of the validity of the SVD and the identity of the user that generated the evidence.
- ***FTP_ITC.1/SVD*** *(Inter-TSF trusted channel)*, which requires the TOE to provide a trusted channel to the CGA.

Here below is the rationale for the security objectives borrowed from PP Part 5 [R12].

OT.TOE_TC_VAD_Imp *(TOE trusted channel for VAD import)* is met by ***FTP_ITC.1/VAD***, which requires the TSF to enforce a trusted channel to protect the VAD provided by the HID to the TOE.

OT.TOE_TC_DTBS_Imp *(TOE trusted channel for DTBS import)* is covered by ***FTP_ITC.1/DTBS***, which requires the TSF to enforce 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.

Here below is the rationale for the security objectives added in this security target to those defined in the PPs.

OT.AC_Init *(Access control for the initialization of the e-Document)* is covered by:

- ***FIA_UID.1*** and ***FIA_UAU.1***, which state that writing TOE initialization data requires a previous authentication on the part of the Initialization Agent;
- ***FMT_MTD.1/Init*** (based on ***FMT_SMR.1/Init*** and ***FMT_SMF.1***), which restricts the capability to write TOE initialization data to the Initialization Agent;

- ***FTP_ITC.1/Init***, which requires the TSF to enforce a trusted channel for the import of TOE initialization data, so as to ensure that the data actually written match those sent by the Initialization Agent.

OT.AC_Pers *(Access control for the personalization of the e-Document)* is covered by:

- ***FIA_UID.1*** and ***FIA_UAU.1***, which state that writing personalization data requires a previous authentication on the part of the Personalization Agent;
- ***FMT_MTD.1/Pers*** (based on ***FMT_SMR.1/Pers*** and ***FMT_SMF.1***), which restricts the capability to write personalization data to the Personalization Agent;
- ***FTP_ITC.1/Pers***, which requires the TSF to enforce a trusted channel for the import of personalization data, so as to ensure that the data actually written match those sent by the Personalization Agent.

10.3 Satisfaction of dependencies of security requirements

Table 10-2 Satisfaction of dependencies of security functional requirements

Requirement	Dependencies	Satisfied by
FCS_CKM.1/RSA	FCS_CKM.2 or FCS_COP.1	FCS_COP.1
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.1/ECDSA	FCS_CKM.2 or FCS_COP.1	FCS_COP.1
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1
FCS_COP.1/RSA	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1
	FCS_CKM.4	FCS_CKM.4
FCS_COP.1/ECDSA	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1
	FCS_CKM.4	FCS_CKM.4
FDP_ACC.1/ SCD/SVD_Generation	FDP_ACF.1	FDP_ACF.1/ SCD/SVD_Generation
FDP_ACF.1/ SCD/SVD_Generation	FDP_ACC.1	FDP_ACC.1/ SCD/SVD_Generation
	FMT_MSA.3	FMT_MSA.3

Requirement	Dependencies	Satisfied by
FDP_ACC.1/ SVD_Transfer	FDP_ACF.1	FDP_ACF.1/ SVD_Transfer
FDP_ACF.1/ SVD_Transfer	FDP_ACC.1	FDP_ACC.1/ SVD_Transfer
	FMT_MSA.3	FMT_MSA.3
FDP_ACC.1/ Signature_Creation	FDP_ACF.1	FDP_ACF.1/ Signature_Creation
FDP_ACF.1/ Signature_Creation	FDP_ACC.1	FDP_ACC.1/ Signature_Creation
	FMT_MSA.3	FMT_MSA.3
FDR_RIP.1	No dependencies	-
FDP_SDI.2/Persistent	No dependencies	-
FDP_SDI.2/DTBS	No dependencies	-
FDP_DAU.2/SVD	FIA_UID.1	FIA_UID.1
FDP_UIT.1/DTBS	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1/ Signature_Creation
	FTP_ITC.1 or FTP_TRP.1	FTP_ITC.1/DTBS
FIA_UID.1	No dependencies	-
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_API.1	No dependencies	-
FMT_SMR.1/QSCD	FIA_UID.1	FIA_UID.1
FMT_SMR.1/Init	FIA_UID.1	FIA_UID.1
FMT_SMR.1/Pers	FIA_UID.1	FIA_UID.1
FMT_SMF.1	No dependencies	-
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1/QSCD
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1/Admin	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1/ SCD/SVD_Generation

Requirement	Dependencies	Satisfied by
	FMT_SMR.1	FMT_SMR.1/QSCD
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1/Signatory	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1/ Signature_Creation
	FMT_SMR.1	FMT_SMR.1/QSCD
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.2	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1/ SCD/SVD_Generation, FDP_ACC.1/ Signature_Creation
	FMT_MSA.1	FMT_MSA.1/Admin, FMT_MSA.1/Signatory
	FMT_SMR.1	FMT_SMR.1/QSCD
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1/Admin, FMT_MSA.1/Signatory
	FMT_SMR.1	FMT_SMR.1/QSCD
FMT_MSA.4	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1/ SCD/SVD_Generation, FDP_ACC.1/ Signature_Creation
FMT_MTD.1/Admin	FMT_SMR.1	FMT_SMR.1/QSCD
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.1/Signatory	FMT_SMR.1	FMT_SMR.1/QSCD
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.1/Init	FMT_SMR.1	FMT_SMR.1/Init
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.1/Pers	FMT_SMR.1	FMT_SMR.1/Pers
	FMT_SMF.1	FMT_SMF.1
FPT_EMS.1	No dependencies	-
FPT_FLS.1	No dependencies	-

Requirement	Dependencies	Satisfied by
FPT_PHP.1	No dependencies	-
FPT_PHP.3	No dependencies	-
FPT_TST.1	No dependencies	-
FTP_ITC.1/SVD	No dependencies	-
FTP_ITC.1/VAD	No dependencies	-
FTP_ITC.1/DTBS	No dependencies	-
FTP_ITC.1/Init	No dependencies	-
FTP_ITC.1/Pers	No dependencies	-

Table 10-3 Satisfaction of dependencies of security assurance requirements

Requirement	Dependencies	Satisfied by
EAL5 package	Dependencies of the EAL5 package are not reproduced here (cf. [R9])	By construction, all dependencies are satisfied in a CC EAL package
ALC_DVS.2	No dependencies	-
AVA_VAN.5	ADV_ARC.1	ADV_ARC.1[130]
	ADV_FSP.4	ADV_FSP.5
	ADV_TDS.3	ADV_TDS.4
	ADV_IMP.1	ADV_IMP.1
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1
	ATE_DPT.1	ATE_DPT.3

10.4 Rationale for security assurance requirements

The assurance level for this security target is EAL5 augmented. EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises, supported by moderate application of specialist security engineering

[130] This assurance component and the subsequent ones are all included in the EAL5 package.

techniques. Such a TOE will be designed and developed with the intent of achieving EAL5 assurance. EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach, without incurring unreasonable costs attributable to specialist security engineering techniques (cf. [R9]).

The TOE described in this security target is just such a product. Augmentation results from the selection of:

- ALC_DVS.2 "Sufficiency of security measures";
- AVA_VAN.5 "Advanced methodical vulnerability analysis".

The selection of component ALC_DVS.2 provides a higher assurance on the security of the development and manufacturing of the TOE.

The selection of component AVA_VAN.5 ensures that the TOE be resistant to penetration attacks performed by an attacker possessing a high attack potential, which is necessary to meet security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure (cf. section 5.1).

11. TOE summary specification

Table 11-1 describes how each Security Functional Requirement claimed in this Security Target is satisfied by the TOE.

Table 11-1 Implementation of the security functional requirements in the TOE

Security functional requirement	Implementation
FCS_CKM.1/RSA FCS_CKM.1/ECDSA	The SCD/SVD key pairs are generated using specific cryptographic features of the platform (cf. [R39]).
FCS_CKM.4	Cryptographic keys are destroyed by calling a dedicated interface of the Crypto Library.
FCS_COP.1/RSA FCS_COP.1/ECDSA	The digital signature creation is performed using specific cryptographic features of the platform (cf. [R39]).
FDP_ACC.1/SCD/SVD_Generation FDP_ACF.1/SCD/SVD_Generation	The generation of SCD/SVD key pairs is restricted to Administrator and Signatory by means of GAP.
FDP_ACC.1/SVD_Transfer FDP_ACF.1/SVD_Transfer	The export of SVD keys is restricted to Administrator and Signatory by means of GAP.
FDP_ACC.1/Signature_Creation FDP_ACF.1/Signature_Creation	The digital signature creation is restricted to the Signatory by means of PIN verification (VAD) after successful GAP. Moreover, signature creation is forbidden unless the key is activated.
FDP_RIP.1	Any volatile copy of a private key meant for signature creation is overwritten with zeros upon the completion of either the generation of the key or the creation of a signature with the key.
FDP_SDI.2/Persistent	The private/public key objects contain a CRC, which is checked whenever the keys are used for signature creation or public key export. In case such a check fails, an exception is raised, so to inform the user about the integrity error.
FDP_SDI.2/DTBS	The volatile data structure storing the DTBS/R contains a CRC, which is checked upon signature creation. In case such a check fails, an exception is raised, so to inform the user about the integrity error.
FDP_DAU.2/SVD	As a means to generate evidence that can be used by the CGA as a guarantee of the validity of SVD, as well as of the identity of the corresponding legitimate Signatory, the TOE supports GAP.
FDP_UIT.1/DTBS	DTBS/R import must be executed over the trusted channel opened by means of GAP.

Security functional requirement	Implementation
FIA_UID.1 FIA_UAU.1	The TOE provides user identification and user authentication prior to enabling access to authorized functions. For the trusted channel between CGA or HID and the TOE this is accomplished using GAP, whether for Initialization Agent's terminal and Personalization Agent's terminal and the TOE this is accomplished using SCP03.
FIA_AFL.1	The thresholds for authentication failures with respect to the RAD are set by the Personalization Agent. The behaviour occurring if the thresholds are reached is specified in the statement of the SFR.
FIA_API.1	Cf. section 2.2.1.
FMT_SMR.1/QSCD	The Administrator and Signatory roles are distinguished by the usage of specific certificates used in GAP.
FMT_SMR.1/Init FMT_SMR.1/Pers	The Initialization Agent and Personalization Agent roles are implicitly identified via the corresponding authentication key.
FMT_SMF.1	Cf. section 2.2.
FMT_MOF.1	The Signatory alone can activate the signature creation function for each single private key, as specified for SFR FMT_MSA.1/Signatory.
FMT_MSA.1/Admin FMT_MSA.1/Signatory FMT_MSA.2 FMT_MSA.3 FMT_MSA.4	The management of SCD/SVD key pairs is restricted to Signatory by means of GAP and PIN verification.
FMT_MTD.1/Admin	The Administrator cannot create the RAD.
FMT_MTD.1/Signatory	The ability to create, modify and unblock the RAD are restricted to the Signatory role, as specified in SFRs definitions, according to the usage of specific certificates used in GAP.
FMT_MTD.1/Init	The command APDUs available for the writing of TOE initialization data (cf. section 2.3.2) require user authentication with respect to the initialization key.
FMT_MTD.1/Pers	The command APDUs available for the writing of personalization data, including the RAD, (cf. section 2.3.3) require user authentication with respect to the personalization key.
FPT_EMS.1	Leakage of confidential data through side channels is prevented by the security features of the Platform, in accordance with the security recommendations contained in the Platform guidance documentation [R39].

Security functional requirement	Implementation
FPT_FLS.1	In case self-test fails or a physical attack is detected, the Applet enters an endless loop, so that all cryptographic operations and data output interfaces are inhibited.
FPT_PHP.1 FPT_PHP.3	Detection of physical attacks is ensured by the security features of the Platform, in accordance with the security recommendations contained in the Platform guidance documentation [R39].
FPT_TST.1	During initial start-up, the Applet automatically is selected, and it checks that it is running on the expected platform JCOP 4 P71, using a specific function provided by the platform. The attack logger is checked too. Furthermore, at the initial start-up the platform performs self-checks as described in [R39]
FTP_ITC.1/SVD	Cf. Application Note 35.
FTP_ITC.1/VAD	Cf. Application Note 36.
FTP_ITC.1/DTBS	Cf. Application Note 37.
FTP_ITC.1/Init	Cf. Application Note 38.
FTP_ITC.1/Pers	Cf. Application Note 39.

12. References

12.1 Acronyms

AA	Active Authentication
AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
ASCII	American Standard Code for Information Interchange
BAC	Basic Access Control
CC	Common Criteria
CGA	Certificate Generation Application
CRC	Cyclic Redundancy Check
CSP	Certification Service Provider
DF	Dedicated/Directory File
DFA	Differential Power Analysis
DTBS	Data To Be Signed
DTBS/R	Data To Be Signed Representation
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EF	Elementary File
FID	File Identifier
GAP	General Authentication Procedure
HID	Human Interface Device
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
LDS	Logical Data Structure
MAC	Message Authentication Code
MF	Master File
MRTD	Machine Readable Travel Document
OS	Operating System
OSP	Organizational Security Policy
PACE	Password Authenticated Connection Establishment
PP	Protection Profile

PUC	Personal Unblocking Code
QSCD	Qualified Signature Creation Device
RAD	Reference Authentication Data
RSA	Rivest-Shamir-Adleman
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SCD	Signature Creation Data
SCS	Signature Creation System
SDO	Signed Data Object
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMT	Signature Management Terminal
SPA	Simple Power Analysis
SSCD	Secure Signature Creation Device
ST	Signature Terminal
SVD	Signature Verification Data
TDES	Triple DES
TOE	Target Of Evaluation
TR	Technical Report
TSF	TOE Security Functionality
VAD	Verification Authentication Data

12.2 Technical references

[R1] **ACSIEL:** *Technical Report - Signature creation and administration for eIDAS Token, Version 1.0, July 2015*

[R2] **BSI:** *Certification Report BSI-DSZ-CC-1136-V3-2022 for NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) from NXP Semiconductors Germany GmbH, 7 September 2022*

[R3] **BSI:** *Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, Part 1: eMRTDs with BAC/PACEv2 and EACv1, version 2.20, February 2015*

[R4] **BSI:** *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, December 2016*

[R5] **BSI:** *Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, Part 3: Common Specifications, version 2.21, December 2016*

[R6] **BSI:** *Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.10, 2018-06-01*

[R7] **CCMB:** *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, version 3.1, revision 5, April 2017, ref. CCMB-2017-04-001*

[R8] **CCMB:** *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, version 3.1, revision 5, April 2017, ref. CCMB-2017-04-002*

[R9] **CCMB:** *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, version 3.1, revision 5, April 2017, ref. CCMB-2017-04-003*

[R10] **CEN:** *Protection profiles for secure signature creation device, Part 2: Device with Key Generation, version 2.0.1, EN 419211-2:2013 (certificate BSI-CC-PP-0059-2009-MA-02)*

[R11] **CEN:** *Protection profiles for secure signature creation device, Part 4: Extension for device with key generation and trusted communication with certificate generation application, version 1.0.1, EN 419211-4:2013 (certificate BSI-CC-PP-0071-2012-MA-01)*

[R12] CEN: *Protection profiles for secure signature creation device, Part 5: Extension for device with key generation and trusted communication with signature creation application, version 1.0.1, EN 419211-5:2013 (certificate BSI-CC-PP-0072-2012-MA-01)*

[R13] European Parliament: *Regulation (EU) No 910/2014 of the European Parliament and of the Council, 23 July 2014*

[R14] European Parliament: *Commission Implementing Decision (EU) 2016/650, 25 April 2016*

[R15] European Parliament: *Directive 1999/93/EC on a Community framework for electronic signatures, December 1999*

[R16] GlobalPlatform: *GlobalPlatform Card Specification 2.3, GPC_SPE_034, GlobalPlatform Inc., October 2015*

[R17] GlobalPlatform: *GlobalPlatform Card Technology, Secure Channel Protocol '03', Card Specification v 2.2 - Amendment D v1.1.1, July 2014.*

[R18] HID Global: *Security Target for HIDApp-eDoc suite – ICAO Application – Basic Access Control, v. 1.5, ref. TCAE210001*

[R19] HID Global: *Security Target for HIDApp-eDoc suite – ICAO Application – EAC-PACE-AA, v. 1.5, ref. TCAE210002*

[R20] HID Global: *Security Target for HIDApp-eDoc suite – eIDAS eSign Application, v. 1.5, ref. TCAE210003*

[R21] HID Global: *Initialization Guidance for HIDApp-eDoc suite, v. 1.4, ref. TCAE210007*

[R22] HID Global: *Personalization Guidance for HIDApp-eDoc suite – ICAO Application, v. 1.6, ref. TCAE210008*

[R23] HID Global: *Personalization Guidance for HIDApp-eDoc suite – eIDAS eSign Application, v. 1.6, ref. TCAE210009*

[R24] HID Global: *Operational User Guidance for HIDApp-eDoc suite – ICAO Application, v. 1.5, ref. TCAE210010*

[R25] HID Global: *Operational User Guidance for HIDApp-eDoc suite – eIDAS eSign Application, v. 1.5, ref. TCAE210011*

[R26] HID Global: *Secure Delivery Procedure for HIDApp-eDoc suite, ref. TCAE210012*

[R27] **ICAO:** *Doc 9303, Machine Readable Travel Documents, Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC), Eighth Edition, 2021*

[R28] **ICAO:** *Doc 9303, Machine Readable Travel Documents, Part 11: Security Mechanisms for MRTDs, Eighth Edition, 2021*

[R29] **ICAO:** *Doc 9303, Machine Readable Travel Documents, Part 12: Public Key Infrastructure for MRTDs, Eighth Edition, 2021*

[R30] **IETF Network Working Group:** *Request for Comments 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997*

[R31] **ISO/IEC:** *International Standard 14443, Identification cards - Contactless integrated circuit cards - Proximity cards, 2008*

[R32] **ISO/IEC:** *International Standard 7816-2, Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimensions and location of the contacts*

[R33] **ISO/IEC:** *International Standard 7816-4, Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange*

[R34] **JIWG:** *Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, version 1.5.1, May 2018*

[R35] **NIST:** *FIPS PUB 180-4, Federal Information Processing Standards Publication, Secure Hash Standard (SHS), March 2012*

[R36] **NIST:** *FIPS PUB 186-4, Federal Information Processing Standards Publication, Digital Signature Standard (DSS), July 2013*

[R37] **NXP:** *JCOP 4 P71, Security Target Lite for JCOP 4 P71 / SE050 Rev. 4.11 – 03 January 2023*

[R38] **NXP:** *NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4), Security Target Lite Rev. 2.6 – 13 June 2022.*

[R39] **NXP:** *JCOP 4 P71, User manual for JCOP 4 P71, Rev. 4.3, DocNo 469543, 08 September 2022, NXP Semiconductors.*

[R40] **Oracle:** *Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5, May 2015*

[R41] **Oracle:** *Java Card 3 Platform, Runtime Environment Specification, Classic Edition, Version 3.0.5, May 2015*

[R42] Oracle: *Java Card 3 Platform, Virtual Machine Specification, Classic Edition, Version 3.0.5, May 2015*

[R43] RSA Laboratories: *PKCS #1: RSA Cryptography Standard, version 2.2, October 2012*

[R44] TUV: *Certification Report NSCIB-CC-180212-5MA1 for JCOP 4 P71 from NXP Semiconductors Germany GmbH, 23 January 2023*

Appendix A Platform identification

The platform on which the TOE is based (cf. [R34]) is the NXP JCOP 4 P71.

The platform includes:

- The certified microcontroller NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (cf. [R2])
- The Security IC Dedicated Software, composed by:
  - MC FW (Micro Controller Firmware) [R38]
  - Crypto Library [R38]
- The Security IC Embedded Software, composed by
  - JCOP 4 P71 OS, consisting of:
    - JCVM, JCRE and JCAPI implemented according to Java Card Specification Version 3.0.5 Classic
    - GP framework implemented according GlobalPlatform Version 2.3 and Amendment D, Secure Channel Protocol ’03’ Version 1.1.1
- Additionally proprietary APIs, described in the document [R39]

The TOE configuration used for the TOE HIDApp-eDoc is the Configuration Banking & Secure ID, JCOP 4 P71 v4.7 R1.01.4.

The platform has obtained a Common Criteria certification at Evaluation Assurance Level EAL6 augmented by ASE_TSS.2 and ALC_FLR.1:

- Certification ID: NSCIB-CC-180212-5MA1
- Security Target: [R37]
- Certification Report: [R44].

END OF DOCUMENT