SAFRAN
Morpho

# MORPHO

# SECURITY TARGET LITE FOR VITALE APPLICATION

Reference: 0000088820
Issue Date : 02/10/2015
Version : 03

# DOCUMENT EVOLUTION

| Date | Index | Author | Revision |
|---|---|---|---|
| 10/01/2012 | 01 | MORPHO | Document Creation |
| 25/06/2015 | 02 | MORPHO | Reevaluation |
| 02/10/2015 | 03 | MORPHO | Correction |

# Table of contents

# Table of figures

# Table of tables

# 1 TOE Reference

The Target Of Evaluation (TOE) is the smart card VITALE application, composed of embedded software developed by Morpho on top of the chip SB23ZL48, produced by STMicroelectronics.

The security target goal is to state the security requirements applicable to the smart card VITALE 2 application.

## 1.1 Security Target Identification

Security Target identification is described in the table below:

| **ST Identification** | **Security Target for VITALE application – Composant STMicroelectronics** |
|---|---|
| Version | 03 |
| Origin | Morpho |
| Product Identification | VITALE2/SB23ZL48/1_0_40 |
| Chip Identifier | SB23ZL48 with Neslib version 3.0 |
| Chip Ref. Certificate | **[R5]** |
| Assurance Level | 4+ |
| CC Version | 3.1 Release 3 |

## 1.2 TOE documentation

TOE documentation is described in the table below:

| **Reference** | **Description** |
|---|---|
| **[AGD_PRE]** | 0000086182 - AGD - VITALE2 - Preparative Procedures |
| **[AGD_OPE]** | 0000086181 - AGD - VITALE2 - Operational User Guidance |
| **[FSP_PRODUCT]** | 0000081785 - VITALE II - FSP – produit |
| **[FSP_VITALE]** | 0000081571 - VITALE II - FSP - Spécification fonctionnelle de Vitale |
| **[FSP_ADELE]** | 0000081342 - VITALE II - FSP - Spécification fonctionnelle de ADELE |
| **[FSP_AIP]** | 0000081638 - VITALE II - FSP - Spécification fonctionnelle de AIP |

# 2 TOE overview

In its operating environment, the VITALE application performs health services.

The VITALE application is the support of the developments of health services as defined in the VITALE context.
Within the context of health services, VITALE application also offers e-government services as defined in the documents **[R3]** and **[R4]**.

The VITALE 2 card must replace the VITALE 1 card that is currently in operation. Two previous version of the VITALE 2 smartcard have been developed based on Philips and ATMEL integrated circuit in 2006. This new version of the smartcard is based on STMicroelectronics integrated circuit.

The application VITALE thus provides services of electronic signature that meets the requirements of secure signature creation device (SSCD) in particular for the implementation of certificates known as "qualified."

This security target therefore specifies the security functional requirements and assurance requirements for Safety of electronic signature services called "secure" application VITALE.

In its operating environment, the application performs VITALE services secure electronic signature in accordance with European Directive **[R15]** transcribed in the Protection Profile **[R3]** and **[R4]**.
These functions are:

- The key pair generation of electronic signature (SCD / SVD)
- The destruction of two key electronic signature (SCD / SVD)
- Loading private key digital signature (DCS)
- The creation of electronic signatures

The assurance level of the product specified in this Security Target and its documentation is EAL 4 augmented assurance components AVA_VAN.5 and ALC_DVS.2, cf § 3.2 of the PP ES for SSD **[R2]**.

## 2.1 TOE type

This security target specifies the functional and security assurance requirements applicable to the **VITALE2/SB23ZL48/1_0_40** smart card. The **VITALE2/SB23ZL48/1_0_40** is comprised of embedded software masked on a referenced IC and its cryptographic library.

The IC and the cryptographic library have been evaluated separately. The TOE evaluation is thus a composite evaluation of embedded software on a certified IC with its cryptographic library.

Conforming to the Common Criteria, the TOE described in this security target is a composition:

- Embedded software designed by Morpho, including the Operating System, the Application Manager and the VITALE application (base, application and data),
- SB23ZL48: Integrated Circuit (IC) (dedicated software and hardware) designed by **STMicroelectronics**.

SB23ZL48 is evaluated under the French IT Security Evaluation and Certification Scheme [R9] and conformant to the Security IC Platform Protection Profile [R18]. The assurance level is EAL5 augmented with ALC_DVS.2 and AVA_VAN.5.

## 2.2 Usage and major security features of the TOE

The TOE is a secure signature-creation device (SSCD Type 2 and SSCD Type 3) according to Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures **[R15]**. The destruction of the Signature Creation Data (SCD) is mandatory before the TOE loads or generates a new pair SCD/Signature Verification Data (SVD).

The TOE provides the following functions necessary for devices involved in creating qualified electronic signatures:

- To generate the SCD and the correspondent (SVD)
- To create qualified electronic signatures:
    - After allowing for the data to be signed (DTBS) to be displayed correctly where the display function may either be provided by the TOE itself or by appropriate environment
    - Using appropriate hash functions that are, according to **[R16]**, agreed as suitable for qualified electronic signatures
    - After appropriate authentication of the signatory by the TOE.
    - Using appropriate cryptographic signature function that employs appropriate cryptographic parameters agreed as suitable according to **[R16]**.

## 2.3 SSCD types and modes of operation

### *2.3.1 SSCD*

**Figure 1** shows the structural perspective of the TOE and its environment. The SSCD, i.e. the TOE, comprises the underlying hardware, the operating system (OS), the SCD/SVD generation, SCD storage and use, and signature-creation functionality. The SCA and the CGA (and possibly other applications) are part of the immediate environment of the TOE. They shall communicate with the TOE over a trusted channel, a trusted path for the human interface provided by the SCA, respectively.

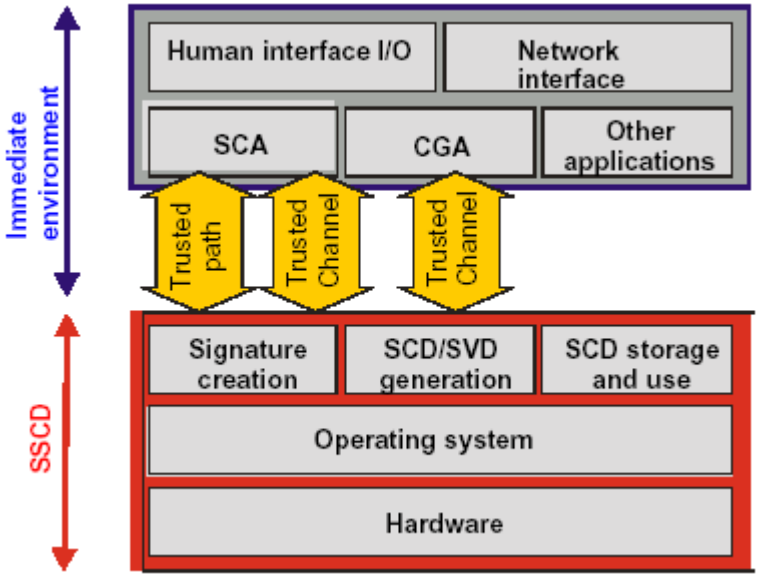



**Figure 1: Structural view of the SSCD**

**Application note 1**: This ST refers to qualified certificates as electronic attestation of the SVD corresponding to the signatory's SCD that is implemented by the TOE.

While the main application scenario of a SSCD will assume a qualified certificate to be used in combination with a SSCD, there still is a large benefit in the security when such SSCD is applied in other areas and such application is encouraged. This ST may as well be applied to environments where the certificates expressed as 'qualified certificates' in this ST do not fulfil the requirements laid down in Annex I and Annex II of the Directive [R12].

With this respect the notion of qualified certificates in this ST refers to the fact that when an instance of a SSCD is used with a qualified certificate, such use is from the technical point of view eligible for an electronic signature as referred to in Directive [R12], article 5, paragraph 1. As a consequence, this standard does not prevent a device itself from being regarded as a SSCD, even when used together with a non-qualified certificate.

### *2.3.2 SSCD types*

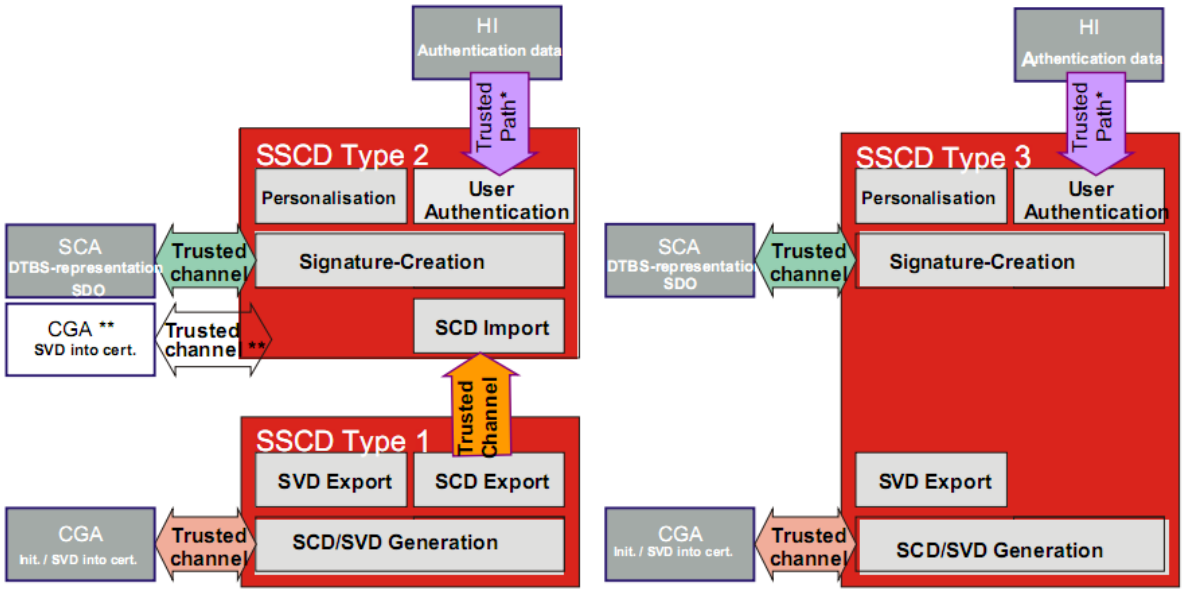



**Figure 2: Structural view of the SSCD**

As we can see in Figure 2, three different SSCD are defined, SSCD Type 1, Type 2 and Type 3.
As defined in the the protection profiles PPs **[R3]** & **[R4]**:

- SSCD Type 1 is not a personalized component in the sense that it may be used by a specific user only, but the SCD/SVD generation and export shall be initiated by authorized persons only (e.g., system administrator).
- SSCD Type 2 and Type 3 are personalized components which mean that they can be used for signature creation by one specific user – the signatory - only.

### *2.3.3 Link between SSCD Type 1/Type 2*

Signature generation by means of a SSCD Type 2 TOE requires that the SCD/SVD pair has been generated by and imported from a SSCD Type 1. Consequently, there is interdependence where a SSCD Type 1 constitutes the environment of the TOE.

The TOE implements all IT security functionalities which are necessary to ensure the secrecy of the SCD. To prevent the unauthorised usage of the SCD the TOE provides user authentication and access control. To this end, the TOE may implement IT measures to support a trusted path to a trusted human interface device.

The SSCD protects the SCD during the whole life cycle as to be solely used in the signature-creation process by the legitimate signatory. The TOE will be initialised for the signatory's use by:

- Import of the SCD or generating a SCD/SVD pair,

- Personalization for the signatory by means of the signatory's verification authentication data (VAD).

The SVD corresponding to the signatory's SCD will be included in the certificate of the signatory by the certificate-service-provider (CSP). The TOE will destroy the SCD if the SCD is no longer used for signature generation.

The TOE allows implementing a human interface for user authentication by a trusted human interface device connected via a trusted channel with the TOE.

## 2.4 Required non-TOE hardware/software/firmware

The TOE is a smart card in ISO format contact **[R11]**
Except this interface, the TOE does not require any hardware, software or firmware.

# 3 TOE description

## 3.1 Product Type

The VITALE 2 card is a smartcard product, consisting of the following hardware and software elements:

- Embedded software designed by Morpho
- An Integrated Circuit, developed by STMicroelectronics

The IC embeds a software whose features are listed below and including an operating system that includes security mechanisms, and applications performing the services of the Vitale 2 card and relying on the operating system.

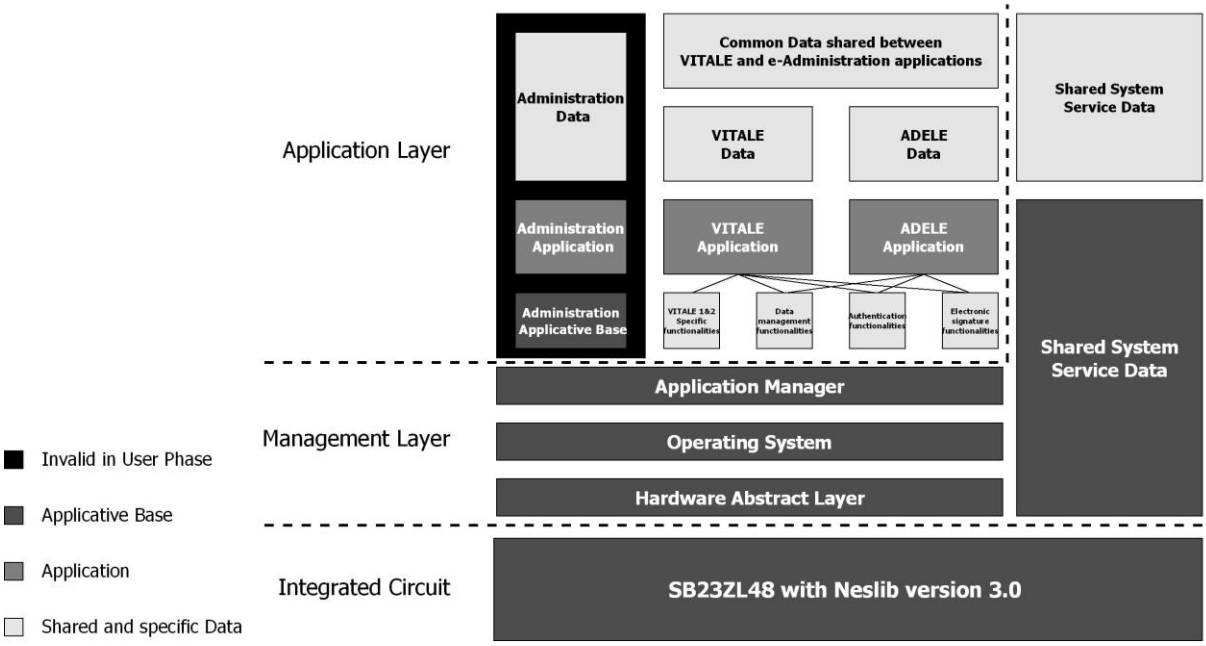



**Figure 3 Product architecture**

### *3.1.1 TOE architecture for the VITALE application*

The following figure presents the different modules composing the TOE for the VITALE application.

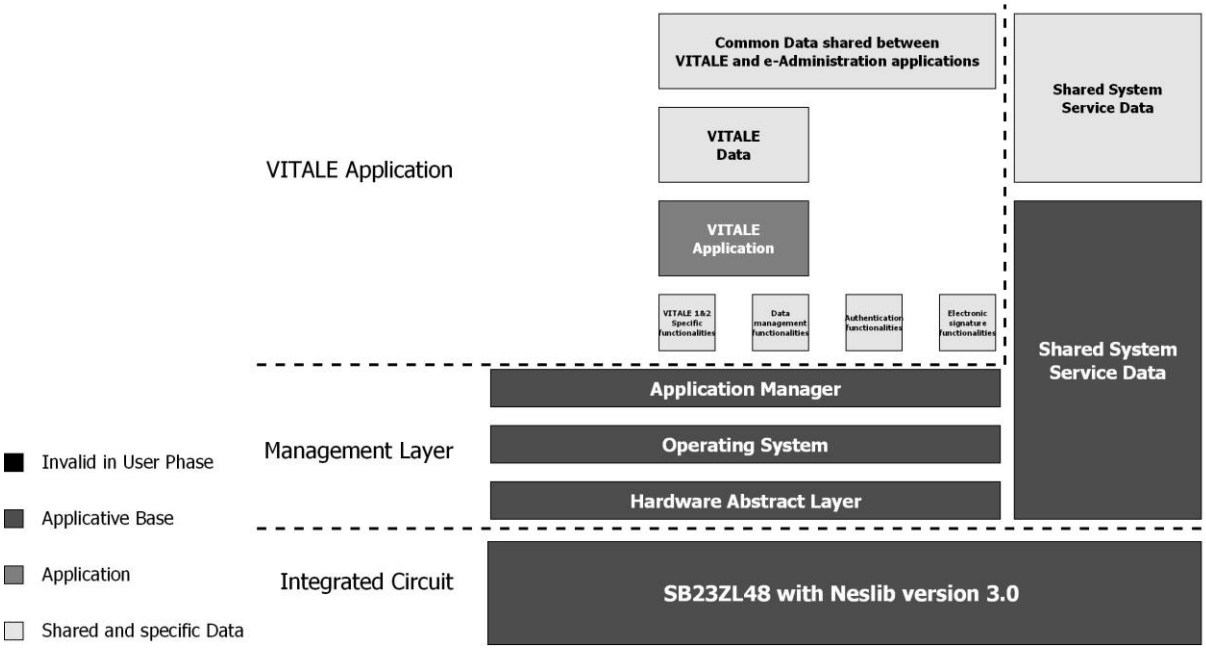



**Figure 4: TOE description**

## 3.2 Life cycle

The smart card product life-cycle is decomposed in 7 phases that describe the competent authorities for each of these phases. The purpose of the embedded software designed in phase 1 is to control and protect the TOE during phases 4 to 7 (product usage).

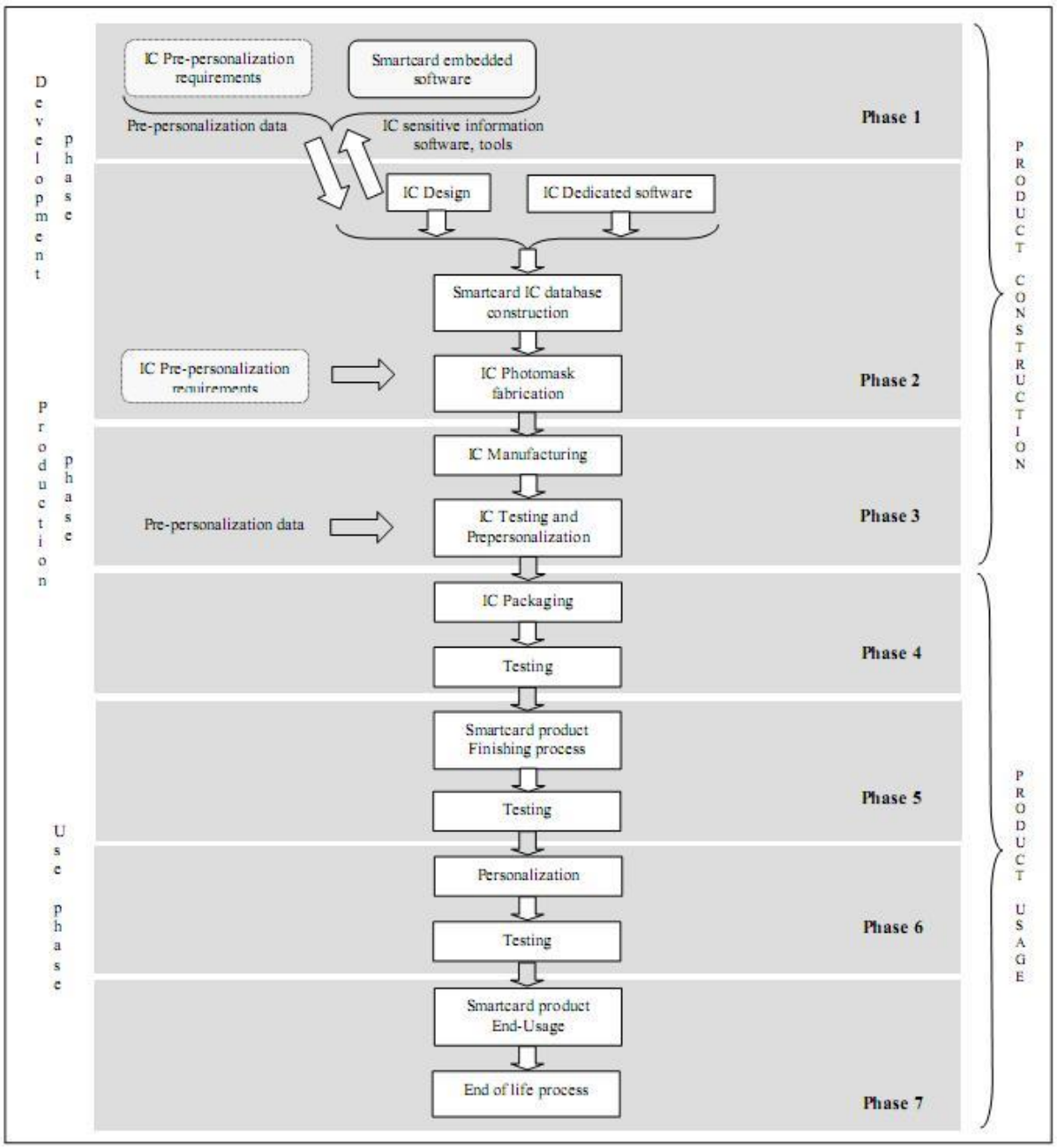



**Figure 5 Life cycle of the smart card product**

In Figure 5, TOE is designed in phase 1 and evaluated in usage in phase 7. These different phases may be performed at different sites. Procedures on the delivery process of the TOE must exist and be applied for every delivery within this phase or between phases.

### *3.2.1 Authorities*

The table below describes the roles of the different card authorities through the phases of the life-cycle.

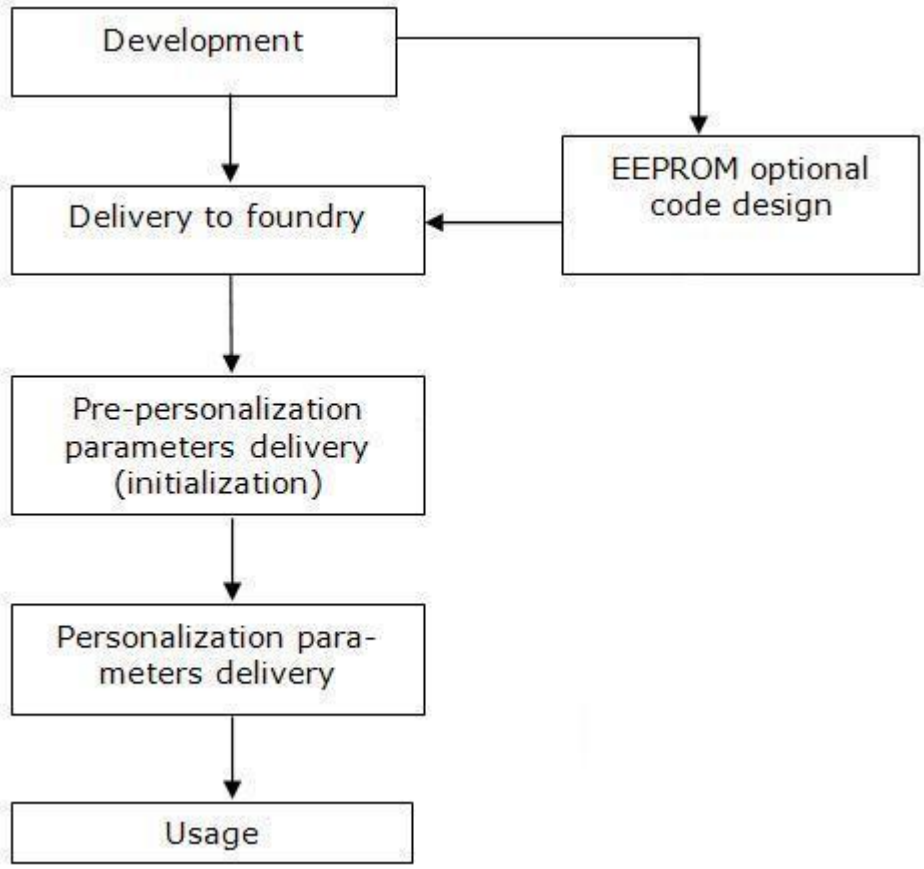
| Phase | Description | Authority |
|---|---|---|
| **Phase 1** | Smart card embedded software development | **Morpho** is responsible of the development of the software embedded in the smart card and of the specification of the integrated circuit personalization requirements. |
| **Phase 2** | Integrated Circuit (IC) development | **STMicroelectronics** designs the IC, develops the IC dedicated software and transmits the information, software and tools to the developer of the embedded software (**Morpho**) by trusted verification and delivery procedures.<br>From the integrated circuit, the dedicated software and embedded software, he builds the database of the integrated circuit of the smart card required for the construction of the photomask of the integrated circuit. |
| **Phase 3** | Manufacturing and testing of the integrated circuit | **STMicroelectronics** is responsible for the production of the integrated circuit that follows three main steps: manufacturing, testing and pre-personalization (including patch) of the integrated circuit by the founder. |
| **Phase 4** | Encapsulation and testing of the integrated circuit | The **packager of the integrated circuit** is responsible for the packaging (encapsulation) and testing of the integrated circuit. |
| **Phase 5** | Product finishing process | The **smart card product manufacturer** is responsible for the finishing process and testing of the smart card. |
| **Phase 6** | Smart card personalization | The **personalizer** is responsible of the personalization of the smart card and of the final tests. |
| **Phase 7** | Smart card usage | The **smart card Issuer** is responsible of the delivery of the product to the **end user**, as well as the end of the life cycle. |

**Table 1 Authorities of the smart card product**

**NB:**

- End of Phase 3: It is the TOE delivery point by Morpho

- Phases 4, 5 and 6: The TOE is pre-personalized and personalized. There is a construction of the TOE in a way of data loading. There is no modification of the TOE
- Phase 7: This phase is covered directly by this security target, it is the product delivery point
- More specifically, the diagram below presents the life-cycle of the application. This life-cycle concerns the phase 1.




-

**Figure 6 Application life cycle**

Application development is composed of the specification, conception, coding, testing and qualification phases.

If the development of a patch becomes necessary, it follows the same steps.

Delivery is composed of code delivery and foundry pre-personalization parameters delivery to foundry, as well as pre-personalization (initialization) and personalization parameters delivery. Usage is covered par the end-user usage of the card with the developed software.

# 4 Common Criteria conformance claim

## 4.1 Common Criteria conformance

This Security Target claims conformance to Common Criteria version 3.1 **[R1]**, with the following documents:

- "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model", Release 3, dated July 2009
- "Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional requirements", Release 3, dated July 2009
- "Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance requirements", Release 3, dated July 2009

Conformance is claimed as follows:

- Part 2: extended
- Part 3: conformant

## 4.2 Protection Profile and package claim

This Security Target is compliant with the following Protection Profiles:

- Protection Profile - Secure Signature-Creation Device Type 2 – Ref. PP0005, Version 1.04, 25 July 2001 **[R3]**.
- Protection Profile - Secure Signature-Creation Device Type 3 – Ref. PP0006, Version 1.05, 25 July 2001 **[R4]**.
- Protection Profile – Embedded software for smart secure devices **[R2]**

The conformance mode is the following:

| **Protection Profile** | **Conformance** |
|---|---|
| PP SSCD Type 2 | Demonstrable |
| PP SSCD Type 3 | Demonstrable |
| PP ES for SSD in basic configuration | Demonstrable |

**NB:**
The protection profile Embedded Software for smart secure devices is used in its basic configuration.

### *4.2.1 PP SSCD Type 2 and Type 3*

The two PPs SSCD are established by CEN/ISSS for use by the European Commission in accordance with the procedure laid down in Article 9 of the Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures **[R15]**, as generally recognised standard for electronic-signature products in the Official Journal of the European Community.

The intent of these PPs is to specify functional and assurance requirements defined in the Directive **[R15]**, Annex III for secure signature-creation devices (SSCD) which is the target of evaluation (TOE). Member States shall presume that there is compliance with the requirements laid down in Annex III of the Directive **[R15]** when an electronic signature product is evaluated to a Security Target (ST) that is compliant with one or both of those PPs.

### *4.2.2 PP ES for SSD*

The protection profile PP ES for SSD **[R2]** is a protection profile that defines the rules for developing embedded software on a smartcard.

## 4.3 Assurance package conformance

The set of assurance requirements is the package EAL4+ augmented by:

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

Assurance requirements are split in two packages, one for the TOE itself and one for its development environment, allowing for separate package assessment. However, both assessments must be combined in order to fulfill the whole set of CAS assurance requirements.

## 4.4 Protection profile conformance

### *4.4.1 CC v2.1 – CC v3.1*

This Security Target is compliant with the SSCD Type 2 and SSCD Type 3 Protection Profiles **[R3]** & **[R4]**.

These two protection profiles have been certified with the Common Criteria CC v2.1. The new protection profiles SSCD Type 2 and Type 3 are not yet satisfied, it is then necessary to use these PPs.

### *4.4.2 Evaluation Assurance Level*

The evaluation assurance level of this security target is EAL4+ augmented with ALC_DVS.2 "Sufficiency of security measures" and AVA_VAN.5 "Advanced methodical vulnerability analysis".

### *4.4.3 Protection Profile addition*

Concerning this evaluation, the security assurance requirements are compliant with an evaluation using CC v3.1 and an evaluation assurance level of EAL4+, augmented with ALC_DVS.2 and AVA_VAN.5.

The security functional requirements (SFR) that are present in this security target are the same that mentioned in the two protection profiles, updated in accordance with the CC v3.1.

**NB:**

- The SFR FPT_AMT.1 (present in the two PPs) has not been mentioned in this security target, because no longer mentioned in CC v3.1. Nevertheless, this SFR is still covered by the security function TSF_BOOT_AT_POWER_UP that manages the tests to be run at initial startup.

### *4.4.4 Protection Profile Claims rationale*

The differences between this Security Target and the two PPs SSCD, have been identified and justified in each impacted chapter. They have been recalled in the previous section.

The TOE type defined in this security target is exactly the same than the one defined in the PPs: an IC with embedded software, and the SSCD application conformant to the European directive **[R15]**.

In the following, the statements of the security problem definition, the security objectives, and the security requirements are consistent with those of the PPs SSCD.

The security problem definition presented in chapter 5 clearly shows the additions to the security problem statement of the PPs.

The security objectives rationale presented in chapter 6.3 clearly identifies modifications and additions made to the rationale presented in the PPs SSCD.

Similarly, the security requirements rationale presented in chapter 7.3 has been updated with respect to the protection profile.

All PP requirements have been shown to be satisfied in the extended set of requirements whose completeness, consistency and soundness has been argued in the rationale sections of the present document.

Some assignments operations in the SFRs are determined in the PPs, some are left with unspecified values. Assignments made by the PPs authors are marked as bold text, while assignments made by the ST author are marked as bold text and in italics.

## 4.5 Conformance with the CC supporting documents

This security target address a smart card TOE and therefore, the associated evaluation shall be performed in compliance with all CC mandatory supporting documents related to smart card evaluations:

### *4.5.1 Application of Attack Potential to Smart cards*

This document **[R17]** shall be used instead of the CEM **[R19]** when calculating the attack potential of the successful attack performed during AVA_VAN analysis. This document impacts only the vulnerability analysis performed by the ITSEF, and is not detailed here.

### *4.5.2 Composite product evaluation for Smart cards and similar devices*

This document **[R18]** shall be used in addition to the CC part 3 **[R1]** and to the CEM **[R19]**. This document specifies the additional information to be provided by a developer, and the additional checks to be performed by the ITSEF when performing a "composite evaluation". This is the case for the current TOE as the underlying IC **[R8]**.

## 4.6 Conformance Rationale for PP SSCD Type 2 and 3 and PP ES for SSD

This Security Target is demonstrably conformant with the SSCD Type 2 and SSCD Type 3 Protection Profiles **[R3]** & **[R4]**, which are compliant with the Common Criteria v2.3.

This security target includes all CC elements of PP SSCD Type 2 and PP SSCD Type 3, without any modification.

This security target is compliant with the SPD of PP SSCD as shown in the following table.

| | Type 2 | Type 3 | ES | Included? |
|---|---|---|---|---|
| **Assumptions** | | | | |
| A.CGA | X | X | | Yes |
| A.Protection_after_product_delivery | | | X | Yes |
| A.SCA | X | X | | Yes |
| A.SCD_Generate | X | | | Yes |
| **Threats** | | | | |
| T.Behaviour | | | X | Yes |
| T.Disclosure | | | X | Yes |
| T.DTBS_Forgery | X | X | | Yes |
| T.Hack_Phys | X | X | | Yes |
| T.Life_Cycle | | | X | Yes |
| T.Modification | | | X | Yes |
| T.RND | | | X | Yes |
| T.SCD_Derive | X | X | | Yes |
| T.SCD_Divulg | X | X | | Yes |
| T.Sig_Forgery | X | X | | Yes |
| T.Sig_Repud | X | X | | Yes |
| T.SigF_Misuse | X | X | | Yes |
| T.SVD_Forgery | X | X | | Yes |
| **Organisational security policy** | | | | |
| OSP.CSP_QCert | X | X | | Yes |
| OSP.MANAGEMENT_OF_SECRETS | | | X | Yes |
| OSP.QSign | X | X | | Yes |
| OSP.Sigy_SSCD | X | X | | Yes |

**Table 2 PP SSCD Type 2 and Type 3 SPD vs. ST**

This security target is compliant with the security objectives of PP ES for SSD as shown in the following table.

| Objectives | Type 2 | Type 3 | ES | Included? |
|---|---|---|---|---|
| **Objectives** | | | | |
| O.Atomicity | | | X | Yes |
| O.Confidentiality | | | X | Yes |
| O.Crypto | | | X | Yes |
| O.DTBS_Integrity_TOE | X | X | | Yes |
| O.EMSEC_Design | X | X | | Yes |
| O.Init | | X | | Yes |
| O.Integrity | | | X | Yes |
| O.Life_Cycle | | | X | Yes |
| O.Life-cycle_Security | X | X | | Yes |
| O.Monitoring | | | X | Yes |
| O.Operate | | | X | Yes |
| O.RND | | | X | Yes |
| O.SCD_Secrecy | X | X | | Yes |
| O.SCD_SVD_Corresp | X | X | | Yes |
| O.SCD_Transfer | X | | | Yes |
| O.SCD_Unique | | X | | Yes |
| O.Sig_Secure | X | X | | Yes |
| O.Sigy_SigF | X | X | | Yes |
| O.SVD_Auth_TOE | X | X | | Yes |
| O.Tamper_ID | X | X | | Yes |
| O.Tamper_Resistance | X | X | | Yes |
| **Objectives for OE** | | | | |
| OE.CGA_QCert | X | X | | Yes |
| OE.HI_VAD | X | X | | Yes |
| OE.Management_of_Secrets | | | X | Yes |
| OE.Physical | | | X | * |
| OE.Protection_After_Product_Delivery | | | X | Yes |
| OE.RND | | | X | * |
| OE.SCA_Data_Intend | X | X | | Yes |
| OE.SCD_SVD_Corresp | X | | | Yes |
| OE.SCD_Transfer | X | | | Yes |
| OE.SCD_Unique | X | | | Yes |
| OE.SVD_AUTH_CGA | X | X | | Yes |

**Table 3 PP SSCD Type 2 and Type 3 Security Objectives vs. ST**

NB:

- OE refers to Operational environment
- * refers to : “become on objective of the TOE”

This security target is compliant with the security functional requirements of PP SSCD and PP ES for SSD as shown in the following table (Table 4)

| SFR | Type 2 | Type 3 | ES | Included? |
|---|---|---|---|---|
| FAU_ARP.1/Monitoring | | | X | Yes |
| FAU_SAA.1/Monitoring | | | X | Yes |
| FCS_CKM.1 | X | X | | Yes |
| FCS_CKM.2/CGA | X | X | | Yes |
| FCS_CKM.3/CGA | X | X | | Yes |
| FCS_CKM.4 | X | X | X | Yes |
| FCS_CKM.4/Type1 | X | | | Yes |
| FCS_COP.1 | | | X | Yes |
| FCS_COP.1/CORRESP | X | X | | Yes |
| FCS_COP.1/MAC | | | | Yes |
| FCS_COP.1/SCA Hash | X | X | | Yes |
| FCS_COP.1/SIGNING | X | X | | Yes |
| FCS_COP.1/TDES | | | | Yes |
| FDP_ACC.1/Atomicity | | | X | Yes |
| FDP_ACC.1/Confidentiality | | | X | Yes |
| FDP_ACC.1/Initialization SFP | | X | | Yes |
| FDP_ACC.1/Integrity | | | X | Yes |
| FDP_ACC.1/Life_cycle | | | X | Yes |
| FDP_ACC.1/Personalization SFP | X | X | | Yes |
| FDP_ACC.1/SCD Export SFP | X | | | Yes |
| FDP_ACC.1/SCD Import SFP | X | | | Yes |
| FDP_ACC.1/Signature-Creation SFP | X | X | | Yes |
| FDP_ACC.1/SVD Transfer SFP | X | X | | Yes |
| FDP_ACF.1/Confidentiality | | | X | Yes |
| FDP_ACF.1/Initialization SFP | | X | | Yes |
| FDP_ACF.1/Integrity | | | X | Yes |
| FDP_ACF.1/Life_cycle | | | X | Yes |
| FDP_ACF.1/Personalization SFP | X | X | | Yes |
| FDP_ACF.1/SCD Import SFP | X | | | Yes |
| FDP_ACF.1/Signature-Creation SFP | X | X | | Yes |
| FDP_ACF.1/SVD Transfer SFP | X | X | | Yes |
| FDP_ETC.1/SVD Transfer SFP | X | X | | Yes |
| FDP_ITC.1/DTBS | X | X | | Yes |
| FDP_ITC.1/SCD | X | | | Yes |
| FDP_RIP.1 | X | X | | Yes |
| FDP_RIP.1/Confidentiality | | | X | Yes |
| FDP_ROL.1/Atomicity | | | X | Yes |
| FDP_SDI.2/DTBS | X | X | | Yes |
| FDP_SDI.2/Integrity | | | X | Yes |
| FDP_SDI.2/Persistent | X | X | | Yes |
| FDP_UCT.1/Confidentiality | X | | X | Yes |
| FDP_UCT.1/Receiver | X | | X | Yes |

| SFR | Type 2 | Type 3 | ES | Included? |
|---|---|---|---|---|
| FDP_UCT.1/Sender | X | | | Yes |
| FDP_UIT.1/Integrity | | | X | Yes |
| FDP_UIT.1/SCA DTBS | X | X | | Yes |
| FDP_UIT.1/SVD Import | X | X | | Yes |
| FDP_UIT.1/SVD Transfer | X | X | | Yes |
| FDP_UIT.1/TOE DTBS | X | X | | Yes |
| FIA_AFL.1 | X | X | | Yes |
| FIA_ATD.1 | X | X | | Yes |
| FIA_SOS.2/RND | | | X | Yes |
| FIA_UAU.1 | X | X | | Yes |
| FIA_UID.1 | X | X | X | Yes |
| FMT_MOF.1 | X | X | | Yes |
| FMT_MOF.1/Operate | | | X | Yes |
| FMT_MSA.1/Administrator | X | X | | Yes |
| FMT_MSA.1/Confidentiality | | | X | Yes |
| FMT_MSA.1/Integrity | | | X | Yes |
| FMT_MSA.1/Life_cycle | | | X | Yes |
| FMT_MSA.1/Signatory | X | X | | Yes |
| FMT_MSA.2 | X | X | | Yes |
| FMT_MSA.3 | X | X | | Yes |
| FMT_MSA.3/Confidentiality | X | X | X | Ratio, FMT_MSA.3 |
| FMT_MSA.3/Integrity | X | X | X | Ratio, FMT_MSA.3 |
| FMT_MSA.3/Life_cycle | X | X | X | Ratio, FMT_MSA.3 |
| FMT_MTD.1 | X | X | | Yes |
| FMT_MTD.1/Operate | | | X | Yes |
| FMT_SMR.1 | X | X | X | Yes |
| FPR_UNO.1/Confidentiality | | | X | Yes |
| FPT_AMT.1 | X | X | | No, this SFR does not exists in CC 3.1 |
| FPT_EMS.1 | X | X | | Yes |
| FPT_FLS.1 | X | X | | Yes |
| FPT_FLS.1/Operate | | | X | Yes |
| FPT_ITC.1/Confidentiality | | | X | Yes |
| FPT_ITI.1/Integrity | | | X | Yes |
| FPT_PHP.1 | X | X | | Yes |
| FPT_PHP.3 | X | X | | Yes |
| FPT_TST.1/Operate | | | X | Yes |
| FPTT_TST.1 | X | X | | Yes |
| FTP_ITC.1/DTBS Import | X | X | | Yes |
| FTP_ITC.1/SCD Export | X | | | Yes |
| FTP_ITC.1/SCD Import | X | | | Yes |
| FTP_ITC.1/SVD Import | X | X | | Yes |
| FTP_ITC.1/SVD Transfer | X | X | | Yes |
| FTP_TRP.1/SCA | X | X | | Yes |
| FTP_TRP.1/TOE | X | X | | Yes |
| FAU_ARP.1/Monitoring | | | X | Yes |

| SFR | Type 2 | Type 3 | ES | Included? |
|---|---|---|---|---|
| FAU_SAA.1/Monitoring | | | X | Yes |
| FCS_CKM.1 | X | X | | Yes |

**Table 4 PP SSCD Type 2-3 and ES vs. ST**

# 5 Security problem definition

## 5.1 Assets

The PP SSCD Type 2 and Type 3 share the assets described below.

### *5.1.1 Assets for the secure electronic signature*

**SCD**

Private key used to perform an electronic signature operation (confidentiality of the SCD must be maintained).

**SVD**

Public key linked to the SCD and used to perform an electronic signature verification (integrity of the SVD when it is exported must be maintained).

**DTBS and DTBS-representation**

Set of data, or its representation which is intended to be signed (their integrity must be maintained).

**VAD**

PIN entered by the end user to perform a signature operation (confidentiality and authenticity of the VAD as needed by the authentication method employed)

**RAD**

Reference PIN code used to identify and authenticate the end user (integrity and confidentiality of RAD must be maintained).

**Signature-creation function of the SSCD using the SCD**

The quality of the function must be maintained so that it can participate to the legal validity of electronic signatures.

**Electronic signature**

Unforgeability of electronic signatures must be assured.

## 5.2 Users / Subjects

The users of the TOE are entities, personal or material, that have an interaction with the TOE via its external interfaces.

### *5.2.1 Subjects Definition*

**S.User**

End user of the TOE which can be identified as S.Admin or S.Signatory

**S.Admin**

User who is in charge to perform the TOE Initialization, TOE personalization or other TOE administrative functions.

**S.Signatory**

User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents.

### *5.2.2 Threat agent*

**S.OFFCARD**

Attacker. A human or a process acting on his behalf being located outside the TOE. The main goal of the S.OFFCARD attacker is to access application sensitive information. The attacker has a high level potential attack and knows no secret.

### *5.2.3 VITALE*

#### 5.2.3.1 VITALE subjects

**SUB_GA**

Processus that receipts all the command that come from the terminal and dispatches to another processus (SUB_APPLI, SUB_AIP)

**SUB_AIP**

Processus activated by default by SUB_GA during initialization and personalization phases. SUB_AIP is an object for SUB_GA.

**SUB_APPLI**

Processus that performs VITALE application associated services and activated by SUB_GA during "user" phase, when the command is SELECT. SUB_APPLI is an object for SUB_GA.

**SUB_CRYPTO**

Processus activated by SUB_APPLI, that performs cryptographic operations or operations that use the embedder code. SUB_CRYPTO is an object for SUB_APPLI and SUB_AIP.

**SUB_GF**

Processus activated by SUB_APPLI that manages the objects OB_FILE. SUB_GF is an object for SUB_APPLI and SUB_AIP

**SUB_GT**

Processus activated by SUB_APPLI for managing objects OB_TLV. SUB_GT is an object for SUB_APPLI and SUB_AIP.

**SUB_GS**

Processus activated by SUB_APPLI for managing the objects OB_SECRET. SUB_GS is an object for SUB_APPLI and SUB_AIP.

#### 5.2.3.2 VITALE objects

**OB_FILE**

Object that generically defines OB_DFILE, OB_EFILE, OB_TLV, OB_SECRET. An OB_FILE is an object that is associated reading/writing access control and creation/deletion and state changement (except OB_TLV).

**OB_DFILE**

ADF or DF directory, stored in EEPROM that contains OB_DFILE or OB_EFILE.

**OB_EFILE**

EF elementary file stored in EEPROM that contains user or proprietary data.

**OB_TLV**

Data with the TLV type (Tag Length Value). This object stores the data with the type card parameter. When an access is given to this object, it is not possible to update it or read.

**OB_SECRET**

Object that stores a cryptographic key or a PIN code and security information associated. This object is stored in files OB_FILE (SECRET_INFO and SECRET_DATA).

**OB_TEMP**

Object that designates temporary data that are stored in RAM memory and use in secure operation.

**OB_IO**

Buffers used for external communication.

## 5.3 Threats

The PP SSCD Type 2 and Type 3 share the threats described in this chapter. This chapter contains the threats of the PP ES for SSD.

**T.Hack_Phys**

Physical attacks through the TOE interfaces.

An attacker interacts with the TOE interfaces to exploit vulnerabilities, resulting in arbitrary security compromises. This threat addresses all the assets.

**T.SCD_Divulg**

Storing, coping and releasing of the signature creation data.

An attacker can store, copy the SCD outside the TOE. An attacker can release the SCD during generation, storage and use for signature-Creation in the TOE.

**T.SCD_Derive**

Derive the signature-creation data.

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

**T.Sig_Forgery**

Forgery of the electronic signature.

An attacker forges the signed data object maybe together with its electronic signature created by the TOE and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature generated 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.

**T.Sig_Repud**

Repudiation of signatures.

If an attacker can successfully threaten any of the assets, then the non repudiation of the electronic signature is compromised. The signatory is able to deny having signed data using the SCD in the TOE under his control even if the signature is successfully verified with the SVD contained in his un-revoked certificate.

**T.SVD_Forgery**

Forgery of the signature-verification data.

An attacker forges the SVD presented by the TOE. This results in loss of SVD integrity in the certificate of the signatory.

**T.DTBS_Forgery**

Forgery of the DTBS-representation.

An attacker modifies the DTBS-representation sent by the SCA. Thus the DTBS-representation used by the TOE for signing does not match the DTBS the signatory intends to sign.

**T.SigF_Misuse**

Misuse of the signature-creation function of the TOE.

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

**T.RND**

An attacker predicts or obtains information about random numbers generated by the product. This may occur for instance by a lack of entropy of the random numbers generated by the product, or because the attacker forces the output of a predefined value.

Assets related: Random numbers.

**T.Behaviour**

An attacker modifies the behaviour of the product, e.g. by unauthorized use of commands (one or many incorrect commands, undefined commands, hidden commands) or buffer overflow attacks (overwriting buffer content to modify execution contexts or gaining system privileges).

An attacker performs perturbation attacks thus causing a malfunction of the product (for instance, by applying environmental stress) in order to deactivate or modify security features or functions of the product.

**T.Disclosure**

An attacker discloses/accesses sensitive code or data by means of logical or physical attacks, for instance:

- brute force attacks;
- undocumented or undefined set of commands;
- input/output interfaces;
- access to residual data;
- clock frequency;
- power analysis (e.g. SPA, DPA).

**T.Life_Cycle**

An attacker accesses to product functionalities outside of their expected availability range thus violating irreversible life cycle phases of the product (for instance, an attacker re-personalizes the product).

An attacker enters the Security IC test mode and uses the test features or interfaces to access or to modify sensitive data or security features.

**T.Modification**

An attacker modifies sensitive Embedded Software code or data by performing logical attacks (for instance, executing malicious code).

An attacker modifies sensitive Embedded Software code or data by performing perturbation attacks (for instance, modifying a value read from memory or changing the output of a computation whose result is written in memory).

An attacker modifies or disables security features of the product, using invasive attacks. These attacks may be performed using physical probing or physical manipulation of the hardware (reverse engineering, manipulation of memory cells, manipulation of hardware security parts).

## 5.4 Organisational Security Policies

This chapter presents the organisation security policy for the TOE and described in the protection profiles PP SSCD Type 2 and Type 3 and PP ES for SSD.

In the two Protection Profiles, Secure Signature Creation Device Type 2 and Type 3, Objectives are prefixed with "P". For more convenience, objectives are prefixed with "OSP".

| TOE OSP | SSCD Type 2 | SSCD Type 3 | ES for SSD |
|---|---|---|---|
| OSP.CSP_QCert | x | x | |
| OSP.QSign | x | x | |
| OSP.Sigy_SSCD | x | x | |
| OSP.Management_of_secrets | | | x |

**OSP.CSP_QCert**

Qualified certficate.

The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Annex I of the Directive, i.e., inter alia 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 is evident with signatures through the certificate or other publicly available information.

**OSP.QSign**

Qualified electronic signatures.

The signatory uses a signature-creation system to sign data with qualified electronic signatures. The DTBS are presented to the signatory by the SCA. The qualified electronic signature is based on a qualified certificate and is created by a SSCD.

**OSP.Sigy_SSCD**

TOE as secure signature-creation device.

The TOE implements and stores the SCD used for signature creation under sole control of the signatory. The SCD used for signature generation can practically occur only once.

**OSP.Management_of_secrets**

Management of secret data (e.g. generation, storage, distribution, destruction, loading into the product of cryptographic private keys, symmetric keys, user authentication data) performed outside the product on behalf of the TOE or Product Manufacturer shall comply with security organisational policies that enforce integrity and confidentiality of these data.

Secret data shared with the user of the product shall be exchanged through trusted channels that protect the data against unauthorized disclosure and modification and allow detecting potential security violations.

## 5.5 Assumptions

The table below presents how the assumptions of the TOE is constructed from the protection profiles SSCD type 2 and 3 and ES for SSD.

| TOE Assumptions | SSCD Type 2 | SSCD Type 3 | ES for SSD |
|---|---|---|---|
| A.CGA | x | x | |
| A.SCA | x | x | |
| A.SCD_Generate | x | | |
| A.Protection_after_product_delivery | | | x |

**A.CGA**

Trustworthy certification-generation application.

The CGA protects the authenticity of the signatory's name and the SVD in the qualified certificate by an advanced signature of the CSP.

**A.SCA**

Trustworthy signature-creation application

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

**A.SCD_Generate**

Trustworthy SCD/SVD generation.

If a party other than the signatory generates the SCD/SVD-pair of a signatory, then

This party will use a SSCD for SCD/SVD-generation,

Confidentiality of the SCD will be guaranteed until the SCD is under the sole control of the signatory and

The SCD will not be used for signature-creation until the SCD is under the sole control of the signatory.

The generation of the SCD/SVD is invoked by authorised users only

The SSCD Type1 ensures the authenticity of the SVD it has created an exported

**A.Protection_after_product_delivery**

The product is assumed to be protected by the environment after delivery (may range from Phase 3 to 6) and before entering the final usage phase (Phase 7 of the life cycle). It is assumed that the persons manipulating the product in the operational environment follow the product guides (user and administrator guidance of the product, installation documentation and personalization guide). It is also assumed that the persons responsible for the application of the procedures contained in the guides, and the persons involved in delivery and protection of the product have the required skills and are aware of the security issues.

Note: The product certificate is valid only when the guides are applied. For instance, for pre-personalization or personalization guides, only the described set-up configurations or personalization profiles are covered by the certificate; any divergence would not be covered by the certificate.

# 6 Security Objectives

## 6.1 Security Objectives for the TOE

The PP SSCD Type 2 and Type 3 share the Security Objectives described in the following part.

This section identifies and defines the security objectives for the TOE and its environment. Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organisational security policies and assumptions.

In the PP SSCD Type 2 and Type 3, Objectives are prefixed with "OT". For more convenience, this security target presents objectives prefixed with "O".

| TOE Objectives | SSCD Type 2 | SSCD Type 3 | ES for SSD |
|---|---|---|---|
| O.EMSEC_Design | x | x | |
| O.Life-cycle_Security | x | x | |
| O.SVD_Auth_TOE | x | x | |
| O.SCD_Secrecy | x | x | |
| O.SCD_SVD_Corresp | x | x | |
| O.SCD_Transfer | x | | |
| O.DTBS_Integrity_TOE | x | x | |
| O.Sigy_SigF | x | x | |
| O.Sig_Secure | x | x | |
| O.Tamper_ID | x | x | |
| O.Tamper_Resistance | x | x | |
| O.Init | | x | |
| O.SCD_Unique | | x | |
| O.Atomicity | | | x |
| O.Confidentiality | | | x |
| O.Crypto | | | x |
| O.Integrity | | | x |
| O.Life_cycle | | | x |
| O.Monitoring | | | x |
| O.Operate | | | x |
| O.RND | | | x |

**O.EMSEC_Design**

Provide physical emanations security

Design and build the TOE in such a way as to control the production of intelligible emanations within specified limits.

**O.Life-cycle_Security**

Life-cycle security

The TOE shall detect flaws during the Initialization, personalization and operational usage. The TOE shall provide safe destruction techniques for the SCD in case of re-import and in case of re-generation.

**O.SVD_Auth_TOE**

TOE ensures authenticity of the SVD

The TOE provides means to enable the CGA to verify the authenticity SVD that has been exported by that TOE.

**O.SCD_Secrecy**

Secrecy of the signature-creation data

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

**O.SCD_SVD_Corresp**

Correspondence between SVD and SCD

The TOE shall ensure the correspondence between the SVD and the SCD. The TOE shall verify on demand the correspondence between the SCD stored in the TOE and the SVD if it has been sent to the TOE.

**O.SCD_Transfer**

Secure transfer of SCD between SSCD

The TOE shall ensure the confidentiality of the SCD transferred between SSCDs.

**O.DTBS_Integrity_TOE**

Verification of the DTBS-representation integrity

The TOE shall verify that the DTBS-representation received from the SCA has not been altered in transit between the SCA and the TOE. The TOE itself shall ensure that the DTBS-representation is not altered by the TOE as well. Note, that this does not conflict with the signature-creation process where the DTBS itself could be hashed by the TOE.

**O.Sigy_SigF**

Signature generation function for the legitimate signatory only

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

**O.Sig_Secure**

Cryptographic security of the electronic signature

The TOE generates electronic signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD cannot be reconstructed using the electronic signatures. The electronic signatures shall be resistant against these attacks, even when executed with a high attack potential.

**O.Tamper_ID**

Tamper detection

The TOE provides system features that detect physical tampering of a system component, and use those features to limit security breaches.

**O.Tamper_Resistance**

Tamper resistance

The TOE prevents or resists physical tampering with specified system devices and components.

**O.Init**

SCD/SVD generation

The TOE provides security features to ensure that the generation of the SCD and the SVD is invoked by authorised users only.

**O.SCD_Unique**

Uniqueness of the signature-creation data

The TOE shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context "practically occur once" means that the probability of equal SCDs is negligible low.

**O.Atomicity**

The TOE shall provide a means to perform memory operations atomically.

**O.Confidentiality**

The TOE shall ensure that confidential information processed and stored by the TOE is protected against unauthorized disclosure.

**O.Crypto**

The TOE shall provide cryptographic services conformant to the cryptographic quality requirements specified in national schemes.

**O.Integrity**

The TOE shall ensure that the Embedded Software code and data are protected against unauthorized modification.

**O.Life_cycle**

The TOE shall manage its own life cycle states as well as reversible and irreversible transitions between them. The TOE shall reject operations unexpected in its current life cycle.

**O.Monitoring**

The TOE shall monitor security registers and system flags made available to the IC and it shall respond to potential security violations in a way that preserves a secure state.

**O.Operate**

The TOE shall ensure the correct operation of its security functions, prevent the unauthorized use of commands and ensure that patches to the code are not bypassed.

**O.RND**

The TOE shall provide random numbers, resulting from an appropriate combination of hardware and/or software mechanisms, that are not predictable and that have sufficient entropy.

The TOE shall ensure that no information about the provided random numbers is available to an attacker since they might be used to generate cryptographic keys.

Random numbers shall be conformant to the quality requirements specified in national schemes.

## 6.2 Security objectives for the Operational Environment

| TOE OE | Type 2 | Type 3 | ES |
|---|---|---|---|
| OE.SCD_SVD_Corresp | x | | |
| OE.SCD_Transfer | x | | |
| OE.SCD_Unique | x | | |
| OE.CGA_QCert | x | x | |
| OE.SVD_AUTH_CGA | x | x | |
| OE.HI_VAD | x | x | |
| OE.SCA_Data_Intend | x | x | |
| OE.Physical | | | x |
| OE.RND | | | x |
| OE.Management_of_secrets | | | x |
| OE.Protection_After_Product_Delivery | | | x |

**OE.SCD_SVD_Corresp**

Correspondence between SVD and SCD

The SSCD Type1 shall ensure the correspondence between the SVD and the SCD. The SSCD Type1 shall verify the correspondence between the SCD sent to the TOE and the SVD sent to the CGA or TOE.

**OE.SCD_Transfer**

Secure transfer of SCD between SSCD

The SSCD Type1 shall ensure the confidentiality of the SCD transferred to the TOE. The SSCD Type1 shall prevent the export of a SCD that already has been

used for signature generation by the SSCD Type2. The SCD shall be deleted from the SSCD Type1 whenever it is exported into the TOE.

**OE.SCD_Unique**

Uniqueness of the signature-creation data

The SSCD Type1 shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context "practically occur once" means that the probability of equal SCDs is negligible low.

**OE.CGA_QCert**

Generation of qualified certificates

The CGA generates qualified certificates which include inter alia

(a) the name of the signatory controlling the TOE,

(b) the SVD matching the SCD implemented in the TOE under sole control of the signatory,

(c) the advanced signature of the CSP.

**OE.SVD_Auth_CGA**

CGA verifies the authenticity of the SVD

The CGA verifies that the SSCD is the sender of the received SVD and the integrity of the received SVD. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

**OE.HI_VAD**

Protection of the VAD

If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed.

**OE.SCA_Data_Intend**

Data intended to be signed

The SCA

- generates the DTBS-representation 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-representation to the TOE and enables verification of the integrity of the DTBS-representation by the TOE
- attaches the signature produced by the TOE to the data or provides it separately.

**OE.Physical**

The Security IC shall detect and respond to invasive physical attacks, to environmental stress and to attempts to access Security IC unauthorised functionality. The Security IC shall prevent leakage of information. The Security IC shall manage its life cycle states and transitions between them; in particular the Security IC shall not allow Test Mode functions once the Security IC has entered the User Mode. The Security IC security features shall resist to high attack potential as defined in [CC AP]. A Security IC that complies with [PP0035] meets this objective.

**OE.RND**

The Security IC shall provide a random number generator conformant with the quality requirements specified in national schemes. Random numbers output by this generator shall not be predictable and shall have sufficient entropy. The Security IC shall ensure that no information about the produced random numbers is available to an attacker since they might be used to generate cryptographic keys.

**OE.Management_of_Secrets**

The secret User or TSF data managed outside the TOE shall be protected against unauthorised disclosure and modification.

**OE.Protection_After_Product_Delivery**

Procedures and controlled environment shall ensure protection of the product and related information after delivery. Procedures shall ensure that people involved in product delivery and protection have the required skills. The persons using the product in the operational environment shall apply the product guides (user and administrator guidance of the product, installation documentation and personalization guide).

## 6.3 Security Objectives Rationale

### *6.3.1 Threats*

**T.Hack_Phys** T.Hack_Phys (Exploitation of physical vulnerabilities) deals with physical attacks exploiting physical vulnerabilities of the TOE. O.SCD_Secrecy preserves the secrecy of the SCD. Physical attacks through the TOE interfaces or observation of TOE emanations are countered by O.EMSEC_Design. O.Tamper_ID and O.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tamper attacks.

**T.SCD_Divulg** T.SCD_Divulg (storing and copying and releasing of the signature-creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the Directive [R18], recital (18). This threat is countered by O.SCD_Secrecy which assures the secrecy of the SCD used for signature generation.

O.SCD_Transfer and OE.SCD_Transfer ensure the confidentiality of the SCD transferred between SSCDs.

**T.SCD_Derive** T.SCD_Derive (derive the signature-creation data) deals with attacks on the SCD via public known data produced by the TOE. This threat is countered by OE.SCD_Unique (if SCD is imported) or by O.SCD_Unique (if SCD/SVD pair is generated) that provides cryptographic secure generation of the SCD/SVD-pair. O.Sig_Secure ensures cryptographic secure electronic signatures.

**T.Sig_Forgery** T.Sig_Forgery (Forgery of the electronic signature) deals with non-detectable forgery of the electronic signature. This threat is in general addressed by OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed), OE.CGA_QCert (Generation of qualified certificates), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.SCD_Transfer (Secure transfer of SCD between SSCD), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance) and OT.Lifecycle_Security (Lifecycle security), as follows:

OT.Sig_Secure ensures by means of robust encryption techniques that the signed data and the electronic signature are securely linked together. OE.SCA_Data_Intend provides that the methods used by the SCA (and therefore by the verifier) for the generation of the DTBS-representation is appropriate for the cryptographic methods employed to generate the electronic signature. The combination of OE.CGA_QCert, OT.SCD_SVD_Corresp, OT.SVD_Auth_TOE, and OE.SVD_Auth_CGA provides the integrity and authenticity of the SVD that is used by the signature verification process. OT.Sig_Secure, OT.SCD_Secrecy, OT.SCD_Transfer, OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD and thus prevent forgery of the electronic signature by means of knowledge of the SCD.

**T.Sig_Repud** T.Sig_Repud (Repudiation of electronic signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in his un-revoked certificate. This threat is in general addressed by OE.CGA_QCert (Generation of qualified certificates), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SCD_Unique (Uniqueness of the signature-creation data), OT.SCD_Transfer (Secure transfer of SCD between SSCD), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance), OT.Lifecycle_Security (Lifecycle security), OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends

representation of data intended to be signed) and OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity). OE.CGA_QCert ensures qualified certificates which allow to identify the signatory and thus to extract the SVD of the signatory. OE.CGA_QCert, OT.SVD_Auth_TOE and OE.SVD_Auth_CGA ensure the integrity of the SVD. OE.CGA_QCert and OT.SCD_SVD_Corresp ensure that the SVD in the certificate correspond to the SCD that is implemented by the SSCD of the signatory. OT.SCD_Unique provides that the signatory's SCD can practically occur just once. OT.Sig_Secure, OT.SCD_Transfer, OT.SCD_Secrecy, OT.Tamper_ID, OT.Tamper_Resistance, OT.EMSEC_Design, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD. OT.Sigy_SigF provides that only the signatory may use the TOE for signature generation. OT.Sig_Secure ensures by means of robust cryptographic techniques that valid electronic signatures may only be generated by employing the SCD corresponding to the SVD that is used for signature verification and only for the signed data. OE.SCA_Data_Intend and OT.DTBS_Integrity_TOE ensure that the TOE generates electronic signatures only for DTBS-representations which the signatory has decided to sign as DTBS.

**T.SVD_Forgery** T.SVD_Forgery (Forgery of the signature-verification data) deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate. T.SVD_Forgery is addressed by O.SVD_Auth_TOE which ensures that the TOE sends the SVD in a verifiable form to the CGA, as well as by OE.SVD_Auth_CGA which provides verification of SVD authenticity by the CGA.

**T.DTBS_Forgery** T.DTBS_Forgery (Forgery of the DTBS-representation) addresses the threat arising from modifications of the DTBS-representation sent to the TOE for signing which then does not correspond to the DTBS-representation corresponding to the DTBS the signatory intends to sign. The TOE counters this threat by the means of O.DTBS_Integrity_TOE by verifying the integrity of the DTBS-representation. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.SCA_Data_Intend.

**T.SigF_Misuse** T.SigF_Misuse (Misuse of the signature-creation function of the TOE) addresses the threat of misuse of the TOE signature-creation function to create SDO by others than the signatory to create SDO for data the signatory has not decided to sign, as required by the Directive [R18], Annex III, paragraph 1, literal (c). This threat is addressed by the O.Sigy_SigF (Signature generation function for the legitimate signatory only), OE.SCA_Data_Intend (Data intended to be signed), O.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity), and OE.HI_VAD (Protection of the VAD) as follows: O.Sigy_SigF ensures that the TOE provides the signature-generation function for the legitimate signatory only. OE.SCA_Data_Intend ensures that the SCA sends the DTBS-representation only for data the signatory intends to sign. The combination of O.DTBS_Integrity_TOE and OE.SCA_Data_Intend counters the misuse of the signature generation function by means of manipulation of the channel between the SCA and the TOE. If the SCA provides the

human interface for the user authentication, OE.HI_VAD provides confidentiality and integrity of the VAD as needed by the authentication method employed.

**T.RND** OE.RND requires a random number generator from the IC that meets national standards and O.RND requires providing random numbers by an appropriate combination of hardware and software mechanisms that also meets national quality metrics. OE.Physical ensures the protection of IC security features, including random number generation. O.Monitoring ensures that the TOE shall react to any security alert made available by the IC, including those that could have an impact on the quality of random numbers generated by the IC. The fulfillment of all these objectives allows to remove the threat.

**T.Behaviour** OE.Physical requires protection against physical attacks corrupting the execution of the Embedded Software code. O.Monitoring ensures that the TOE shall react to any security alert made available by the IC, including those that could indicate execution perturbation. O.Operate requires the correct execution of Embedded Software code and ensures that only correct commands shall be processed and that patches are applied, if any. O.Atomicity prevents reaching inconsistent states through the interruption of memory operations. The fulfillment of all these objectives allows to remove the threat.

**T.Disclosure** OE.Physical requires preventing the leakage of Embedded Software code and data by the IC. It covers the hardware aspects of the threat. The objective O.Monitoring ensures that the TOE shall react to any security alert made available by the IC, including those that could indicate information leakage. O.Confidentiality requires the protection of confidential data (Embedded Software TSF or User data) from unauthorised disclosure by the TOE. O.Crypto requires cryptographic capacities from the TOE, which can be used to enforce data confidentiality. The fulfillment of all these objectives allows to remove the threat.

**T.Life_Cycle** OE.Physical and O.Life_cycle require the control the IC and TOE life cycles, respectively, to prevent abuse of functionality by physical and logical means. The fulfillment of all these objectives allows to remove the threat.

**T.Modification** OE.Physical requires ensuring the integrity of the Embedded Software code and data by the IC. It covers the hardware aspects of the threat. The objective O.Monitoring ensures that the TOE shall react to any security alert made available by the IC, including those that could indicate information modification. O.Integrity requires the protection of integer data (Embedded Software TSF or User data) from unauthorised modification by the TOE. O.Crypto requires cryptographic capacities from the TOE that can be used to enforce data integrity. The fulfillment of all these objectives allows to remove the threat.

### *6.3.2 Organisational Security Policies*

**OSP.CSP_QCert** OSP.CSP_QCert (CSP generates qualified certificates) establishes the qualified certificate for the signatory and provides that the SVD matches the SCD that is implemented in the SSCD under sole control of this signatory. OE.CSP_QCert is addressed by the TOE by O.SCD_SVD_Corresp and OE.SCD_SVD_Corresp concerning the correspondence between the SVD and the SCD, in the TOE IT environment, by OE.CGA_QCert for generation of qualified certificates by the CGA, respectively.

**OSP.QSign** OSP.QSign (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with qualified electronic signatures, as defined by the Directive [R18], article 5, paragraph 1. Directive [R18], recital (15) refers to SSCDs to ensure the functionality of advanced signatures. The requirement of qualified electronic signatures being based on qualified certificates is addressed by OE.CGA_QCert. OE.SCA_Data_Intend provides that the SCA presents the DTBS to the signatory and sends the DTBS-representation to the TOE. O.Sig_Secure and O.Sigy_SigF address the generation of advanced signatures by the TOE.

**OSP.Sigy_SSCD** OSP.Sigy_SSCD (TOE as secure signature-creation device) establishes the TOE as secure signature-creation device of the signatory with practically unique SCD. This is addressed by O.Sigy_SigF ensuring that the SCD is under sole control of the signatory and OE.SCD_Unique (if SCD is imported) or O.SCD_Unique (if SCD/SVD pair is generated) ensuring the cryptographic quality of the SCD/SVD pair for the qualified electronic signature., O.Init provides that generation of the SCD/SVD pair is restricted to authorised users.

**OSP.Management_of_secrets** OE.Management_of_Secrets directly covers the organisational security policy.

### *6.3.3 Assumptions*

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

**A.SCA** A.SCA (Trustworthy signature-creation application) establishes the trustworthiness of the SCA according to the generation of DTBS-representation. This is addressed by OE.SCA_Data_Intend (Data intended to be signed) which ensures that the SCA generates the DTBS-representation of the data that has 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.SCD_Generate** A.SCD_Generate (Trustworthy SCD/SVD generation) establishes a trustworthy SCD/SVD pair. This requires that the SCD must be unique, objective met by OE.SCD_Unique, that the SCD and the SVD must correspond, objective met by OE.SCD_SVD_Corresp. The secrecy of the SCD must be maintained while it is transferred to the TOE before being deleted, OE.SCD_Transfer.

**A.Protection_after_product_delivery** OE.Protection_After_Product_Delivery directly covers the assumption.

### *6.3.4 Security Objectives for the TOE*

**O.RND** T.RND requires providing random numbers by an appropriate combination of hardware and software mechanisms that also meets national quality metrics.

### *6.3.5 Security objectives for the Operational Environment*

**OE.Physical** A.Protection_after_product_delivery ensures the protection after the product delivery.

**OE.RND** T.RND represents the threat over OE.RND that could happen to the product. OSP.Management_of_secrets and A.Protection_after_product_delivery provide security concerning the product.

### *6.3.6 SPD and Security Objectives*

| Threats | Security Objectives | Rationale |
|---|---|---|
| T.Hack_Phys | O.EMSEC_Design, O.SCD_Secrecy, O.Tamper_ID, O.Tamper_Resistance | Section 6.3.1 |
| T.SCD_Divulg | O.SCD_Transfer, O.SCD_Secrecy, OE.SCD_Transfer | Section 6.3.1 |
| T.SCD_Derive | O.Sig_Secure, O.SCD_Unique, OE.SCD_Unique | Section 6.3.1 |
| T.Sig_Forgery | O.EMSEC_Design, O.Life-cycle_Security, O.SCD_Secrecy, O.SCD_SVD_Corresp, O.SVD_Auth_TOE, O.Tamper_ID, O.Tamper_Resistance, O.SCD_Transfer, O.Sig_Secure, OE.SCD_SVD_Corresp, OE.SCD_Transfer, OE.CGA_QCert, OE.SVD_Auth_CGA, OE.SCA_Data_Intend | Section 6.3.1 |

| | | |
|---|---|---|
| T.Sig_Repud | O.EMSEC_Design, O.Life-cycle_Security, O.SCD_Secrecy, O.SCD_SVD_Corresp, O.SVD_Auth_TOE, O.Tamper_ID, O.Tamper_Resistance, O.SCD_Transfer, O.SCD_Unique, O.DTBS_Integrity_TOE, O.Sigy_SigF, O.Sig_Secure, OE.SCD_SVD_Corresp, OE.SCD_Transfer, OE.SCD_Unique, OE.CGA_QCert, OE.SVD_Auth_CGA, OE.SCA_Data_Intend | Section 6.3.1 |
| T.SVD_Forgery | O.SVD_Auth_TOE, OE.SVD_Auth_CGA | Section 6.3.1 |
| T.DTBS_Forgery | O.DTBS_Integrity_TOE, OE.SCA_Data_Intend | Section 6.3.1 |
| T.SigF_Misuse | O.DTBS_Integrity_TOE, O.Sigy_SigF, OE.HI_VAD, OE.SCA_Data_Intend | Section 6.3.1 |
| T.RND | OE.SCD_Unique, O.SCD_Secrecy, O.RND, OE.RND | Section 6.3.1 |
| T.Behaviour | O.Atomicity, O.Operate, O.Monitoring | Section 6.3.1 |
| T.Disclosure | O.Confidentiality, O.Crypto, O.Monitoring | Section 6.3.1 |
| T.Life_Cycle | O.Life_cycle | Section 6.3.1 |
| T.Modification | O.Crypto, O.Integrity, O.Monitoring, OE.Physical | Section 6.3.1 |

**Table 5 Threats and Security Objectives - Coverage**

| Security Objectives | Threats | Rationale |
|---|---|---|
| O.EMSEC_Design | T.Hack_Phys, T.Sig_Forgery, T.Sig_Repud | |
| O.Life-cycle_Security | T.Sig_Forgery, T.Sig_Repud | |
| O.SVD_Auth_TOE | T.Sig_Forgery, T.Sig_Repud, T.SVD_Forgery | |
| O.SCD_Secrecy | T.Hack_Phys, T.SCD_Divulg, T.Sig_Forgery, T.Sig_Repud, T.RND | |
| O.SCD_SVD_Corresp | T.Sig_Forgery, T.Sig_Repud | |
| O.SCD_Transfer | T.SCD_Divulg, T.Sig_Forgery, T.Sig_Repud | |
| O.DTBS_Integrity_TOE | T.Sig_Repud, T.DTBS_Forgery, T.SigF_Misuse | |
| O.Sigy_SigF | T.Sig_Repud, T.SigF_Misuse | |
| O.Sig_Secure | T.SCD_Derive, T.Sig_Forgery, T.Sig_Repud | |
| O.Tamper_ID | T.Hack_Phys, T.Sig_Forgery, T.Sig_Repud | |
| O.Tamper_Resistance | T.Hack_Phys, T.Sig_Forgery, T.Sig_Repud | |
| O.Init | | |
| O.SCD_Unique | T.SCD_Derive, T.Sig_Repud | |
| O.Atomicity | T.Behaviour | |
| O.Confidentiality | T.Disclosure | |
| O.Crypto | T.Disclosure, T.Modification | |
| O.Integrity | T.Modification | |

| Security Objectives | Threats | Rationale |
|---|---|---|
| O.Life_cycle | T.Life_Cycle | |
| O.Monitoring | T.Behaviour, T.Disclosure, T.Modification | |
| O.Operate | T.Behaviour | |
| O.RND | T.RND | Section 6.3.4 |
| OE.SCD_SVD_Corresp | T.Sig_Forgery, T.Sig_Repud | |
| OE.SCD_Transfer | T.SCD_Divulg, T.Sig_Forgery, T.Sig_Repud | |
| OE.SCD_Unique | T.SCD_Derive, T.Sig_Repud, T.RND | |
| OE.CGA_QCert | T.Sig_Forgery, T.Sig_Repud | |
| OE.SVD_Auth_CGA | T.Sig_Forgery, T.Sig_Repud, T.SVD_Forgery | |
| OE.HI_VAD | T.SigF_Misuse | |
| OE.SCA_Data_Intend | T.Sig_Forgery, T.Sig_Repud, T.DTBS_Forgery, T.SigF_Misuse | |
| OE.Physical | T.Modification | Section 6.3.5 |
| OE.RND | T.RND | Section 6.3.5 |
| OE.Management_of_Secrets | | |
| OE.Protection_After_Product_Delivery | | |

**Table 6 Security Objectives and Threats - Coverage**

| Organisational Security Policies | Security Objectives | Rationale |
|---|---|---|
| OSP.CSP_QCert | OE.SCD_SVD_Corresp, O.SCD_SVD_Corresp, OE.CGA_QCert | Section 6.3.2 |
| OSP.QSign | O.Sigy_SigF, O.Sig_Secure, OE.CGA_QCert, OE.SCA_Data_Intend | Section 6.3.2 |
| OSP.Sigy_SSCD | O.Sigy_SigF, O.Init, O.SCD_Unique, OE.SCD_Unique | Section 6.3.2 |
| OSP.Management_of_secrets | OE.Management_of_Secrets | Section 6.3.2 |

**Table 7 OSPs and Security Objectives - Coverage**

| Security Objectives | Organisational Security Policies |
|---|---|
| O.EMSEC_Design | |
| O.Life-cycle_Security | |
| O.SVD_Auth_TOE | |
| O.SCD_Secrecy | |
| O.SCD_SVD_Corresp | OSP.CSP_QCert |
| O.SCD_Transfer | |
| O.DTBS_Integrity_TOE | |
| O.Sigy_SigF | OSP.QSign, OSP.Sigy_SSCD |
| O.Sig_Secure | OSP.QSign |
| O.Tamper_ID | |
| O.Tamper_Resistance | |
| O.Init | OSP.Sigy_SSCD |
| O.SCD_Unique | OSP.Sigy_SSCD |
| O.Atomicity | |
| O.Confidentiality | |
| O.Crypto | |
| O.Integrity | |
| O.Life_cycle | |
| O.Monitoring | |
| O.Operate | |
| O.RND | |
| OE.SCD_SVD_Corresp | OSP.CSP_QCert |
| OE.SCD_Transfer | |
| OE.SCD_Unique | OSP.Sigy_SSCD |
| OE.CGA_QCert | OSP.CSP_QCert, OSP.QSign |
| OE.SVD_Auth_CGA | |
| OE.HI_VAD | |
| OE.SCA_Data_Intend | OSP.QSign |
| OE.Physical | |
| OE.RND | |
| OE.Management_of_Secrets | OSP.Management_of_secrets |

| Security Objectives | Organisational Security Policies |
|---|---|
| OE.Protection_After_Product_Delivery | |

**Table 8 Security Objectives and OSPs - Coverage**

| Assumptions | Security objectives for the Operational Environment | Rationale |
|---|---|---|
| A.CGA | OE.CGA_QCert, OE.SVD_Auth_CGA | Section 6.3.3 |
| A.SCA | OE.SCA_Data_Intend | Section 6.3.3 |
| A.SCD_Generate | OE.SCD_SVD_Corresp, OE.SCD_Transfer, OE.SCD_Unique | Section 6.3.3 |
| A.Protection_after_product_delivery | OE.Protection_After_Product_Delivery, OE.Physical | Section 6.3.3 |

**Table 9 Assumptions and Security Objectives for the Operational Environment - Coverage**

| Security objectives for the Operational Environment | Assumptions | Rationale |
|---|---|---|
| OE.SCD_SVD_Corresp | A.SCD_Generate | |
| OE.SCD_Transfer | A.SCD_Generate | |
| OE.SCD_Unique | A.SCD_Generate | |
| OE.CGA_QCert | A.CGA | |
| OE.SVD_Auth_CGA | A.CGA | |
| OE.HI_VAD | | |
| OE.SCA_Data_Intend | A.SCA | |
| OE.Physical | A.Protection_after_product_delivery | Section 6.3.5 |
| OE.RND | | |
| OE.Management_of_Secrets | | |
| OE.Protection_After_Product_Delivery | A.Protection_after_product_delivery | |

**Table 10 Security Objectives for the Operational Environment and Assumptions - Coverage**

# 7 Extended requirements

## 7.1 Extended families

### *7.1.1 Extended family FPT_EMS - TOE Emanation*

#### 7.1.1.1 Description

The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE?s electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations.

#### 7.1.1.2 Extended components

**Extended component FPT_EMS.1**

*Description*

Family behaviour:

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMSEC.1 TOE Emanation has two constituents:

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

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions identified that should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.

Hierarchical component:

No other component

*Definition*

| **FPT_EMS.1 TOE Emanation** |
| --- |

**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].

Dependencies: No dependencies.

# 8 Security Functional Requirements

## 8.1 Security Functional Requirements

This part presents the SFR that come from the PP SSCD Type 2 and Type 3. The Type 3 part detailled specifically the SFR when they are not present in the PP SSCD Type 2. Whether, the common SFR are mentionned in Type 2 part and editorially refined to be compliant with the two PPs.

Some of the SFR listed below are shared between PP SSCD Type 2 and PP SSCD Type 3:

- The SFR that are strictly similar, have been written in the part PP SSCD Type 2 and mentionned in part Type 3.
- The SFR that are different have been modified or editiorally refined in the PP SSCD Type 2 and mentionned in part Type 3.

For convenience of the reader, the following list presents the SFR in the second case that have been modified or editorially refined:

FSC_CKM.4 - Cryptographic Key Destruction

FIA_UAU.1 - Timing of authentication

FIA_UID.1 - Timing of identification

FMT_MSA.1/Administrator - Management of security attributes

FTP_ITC.1/SVD Transfer - Inter-TSF trusted channel

### *8.1.1 TOE Security Functional Requirements*

#### 8.1.1.1 FCS: Cryptographic support

**FCS_CKM.4 Cryptographic key destruction**

**FCS_CKM.4.1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **Key overwriting, using random, of the EEPROM that stores the keys** that meets the following: **None**.

*Refinement:*

SCD are destruct on demand of the signatory or administrator. The destruction of the existant SCD is mandatory before the re-generation by the TOE of the pair SCD/SVD or the reloading of the SCD in the TOE. Concerning the VITALE application, the signatory or administrator are able to destruct on demand the secrets.

*Application note:*

The cryptographic key SCD will be destroyed on demand of the Signatory or Administrator. The destruction of the SCD is mandatory before the SCD is re-

imported or re-generated into the TOE. The destruction of the SCD is mandatory before the SCD/SVD pair is re-generated by the TOE.

**FCS_COP.1 Cryptographic operation**

**FCS_COP.1.1** The TSF shall perform **[cf infra]** in accordance with a specified cryptographic algorithm **[cf infra]** and cryptographic key sizes **[cf infra]** that meet the following: **[cf infra]**.

*Refinement:*

The assignment of the cryptographic operation are described in the table below:

| Cryptographic operation | Algorithms | Key size | Norms |
|---|---|---|---|
| Cryptogram for authentication | MAC Retail | 112 | ISO 9797-1 |
| VITALE 1 certificate calculation | MAC Retail | 112 | ISO 9797-1 |
| VITALE 2 certificate calculation | CBC TDES | 224 | ISO 9797-1 |
| MAC calculation | MAC Retail | 112 | ISO 9797-1 |
| Ciphering/deciphering | TDES | 112 | ISO 10116/X.9.52-1998 |
| Card authentication cryptogram calculation | RSA | 1024-2048 | ISO 9796-2 |
| SSL authentication cryptogram calculation | RSA | 1024-2048 | Signature PKCS#1 v2.1-padding v1.5 |
| Asymetric deciphering | RSA | 1024-2048 | Ciphering PKCS#1 v2.1-padding v1.5 |
| SCD/SVD correspondance verification | RSA key | 1024-2048 | Signature PKCS#1 v2.1-padding v1.5 |
| Electronic signature creation | RSA | 1024-2048 | Signature PKCS#1 v2.1-padding v1.5 |
| HASH calculation | DTBS-Hash | N/A | SHA-1 and SHA-2 |
| DH key exchange | DH | 1024-2048 | SHA-1 and SHA-2 |

#### 8.1.1.2 FDP: User data protection

The security attributes for the user, TOE components and related status are described below.

During Initialization attribute group:

The subject User has the role SCD-SVD management. He is an administrator but not a signatory.

The subject SCD has the role secure SCD import allowed. He is a signatory but not an administrator.

During signature-creation attribute group.

The subject SCD has the role SCD operational. He is a signatory but not an administrator.

The subject DTBS has the role sent by an authorized SCA. He is a signatory but not an administrator.

The following table represents the security attribute for the user, TOE components and related status.

General attribute:

| Type | Attribute | Status |
|---|---|---|
| User | Role | Administrator, Signatory |

Initialization attribute group:

| Type | Attribute | Status |
|---|---|---|
| User | SCD / SVD management | authorised, not authorised |
| SCD | secure SCD import allowed | not authorised, authorised |

Signature-creation attribute group:

| Type | Attribute | Status |
|---|---|---|
| SCD | SCD operational | not authorised, authorised |
| DTBS | sent by an authorised SCA | not authorised, authorised |

**FDP_ACC.1/SVD Transfer Subset access control**

**FDP_ACC.1.1/SVD Transfer** The TSF shall enforce the **SVD Transfer SFP** on **import and on export of SVD by User (PP SSCD Type 2) or on export of SVD by User (PP SSCD Type 3)**.

*Application note:*

FDP_ACC.1/SVD Transfer will be required only, if the TOE is to import the SVD from a SSCD Type1 so it will be exported to the CGA for certification.

**FDP_ACC.1/SCD Import SFP Subset access control**

**FDP_ACC.1.1/SCD Import SFP** The TSF shall enforce the **SCD Import SFP** on **SCD import by User**.

**FDP_ACC.1/Initialization SFP Subset access control**

**FDP_ACC.1.1/Initialization SFP** The TSF shall enforce the **Initialization SFP** on **generation of SCD/SVD pair by User**.

**FDP_ACC.1/Personalization SFP Subset access control**

**FDP_ACC.1.1/Personalization SFP** The TSF shall enforce the **Personalization SFP** on **the RAD creation by Administrator**.

**FDP_ACC.1/Signature-Creation SFP Subset access control**

**FDP_ACC.1.1/Signature-Creation SFP** The TSF shall enforce the **Signature-creation SFP** on

**DTBS-representation sending by SCA,**

**DTBS-representation signing by Signatory**.

**FDP_ACF.1/Initialization SFP Security attribute based access control**

**FDP_ACF.1.1/Initialization SFP** The TSF shall enforce the **Initialization SFP** to objects based on the following: **General attribute and Initialization attribute**.

**FDP_ACF.1.2/Initialization SFP** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **The user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to "authorised" is allowed to generate SCD/SVD pair**.

**FDP_ACF.1.3/Initialization SFP** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **None**.

**FDP_ACF.1.4/Initialization SFP** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **The user with the**

**security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair**.

**FDP_ACF.1/SVD Transfer Security attribute based access control**

**FDP_ACF.1.1/SVD Transfer** The TSF shall enforce the **SVD Transfer SFP** to objects based on the following: **General attribute**.

**FDP_ACF.1.2/SVD Transfer** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **The user with the security attribute "role" set to "Administrator" or to "Signatory" is allowed to export SVD**.

**FDP_ACF.1.3/SVD Transfer** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **None**.

**FDP_ACF.1.4/SVD Transfer** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **None**.

*Application note:*

FDP_ACF.1/SVD Transfer will be required only, if the TOE holds the SVD and the SVD is exported to the CGA for certification.

**FDP_ACF.1/SCD Import SFP Security attribute based access control**

**FDP_ACF.1.1/SCD Import SFP** The TSF shall enforce the **SCD Import SFP** to objects based on the following: **General attribute and Initialization attribute group**.

**FDP_ACF.1.2/SCD Import SFP** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "authorised" is allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes"**.

**FDP_ACF.1.3/SCD Import SFP** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **None**.

**FDP_ACF.1.4/SCD Import SFP** The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

**The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "not authorised" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes".**

**The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "authorised" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "no"**.

**FDP_ACF.1/Personalization SFP Security attribute based access control**

**FDP_ACF.1.1/Personalization SFP** The TSF shall enforce the **Personalization SFP** to objects based on the following: **General attribute**.

**FDP_ACF.1.2/Personalization SFP** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **User with the security attribute "role" set to "Administrator" is allowed to create the RAD**.

**FDP_ACF.1.3/Personalization SFP** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **None**.

**FDP_ACF.1.4/Personalization SFP** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **None**.

**FDP_ACF.1/Signature-Creation SFP Security attribute based access control**

**FDP_ACF.1.1/Signature-Creation SFP** The TSF shall enforce the **Signature-creation SFP** to objects based on the following: **General attribute and Signature-creation attribute group**.

**FDP_ACF.1.2/Signature-Creation SFP** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **User with the security attribute "role" set to "Signatory" is allowed to create electronic signatures for DTBS sent by an authorised SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes"**.

**FDP_ACF.1.3/Signature-Creation SFP** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **None**.

**FDP_ACF.1.4/Signature-Creation SFP** The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

**User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS which is not sent by an authorised SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes".**

**User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS sent by an authorised SCA with SCD by the Signatory which security attribute "SCD operational" is set to "no"**.

**FDP_ETC.1/SVD Transfer Export of user data without security attributes**

**FDP_ETC.1.1/SVD Transfer** The TSF shall enforce the **SVD transfer SFP** when exporting user data, controlled under the SFP(s), outside of the TOE.

**FDP_ETC.1.2/SVD Transfer** The TSF shall export the user data without the user data's associated security attributes

*Application note:*

FDP_ETC.1/SVD Transfer will be required only, if the TOE holds the SVD and the SVD is exported to the CGA for certification.

**FDP_ITC.1/SCD Import of user data without security attributes**

**FDP_ITC.1.1/SCD** The TSF shall enforce the **SCD Import SFP** when importing user data, controlled under the SFP, from outside of the TOE.

**FDP_ITC.1.2/SCD** The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

**FDP_ITC.1.3/SCD** The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **SCD shall be sent by an authorised SSCD**.

*Application note:*

A SSCD of Type 1 is authorised to send SCD to a SSCD of Type 2, if it is designated to generate the SCD for this SSCD of Type 2 and to export the SCD for import into this SSCD of Type 2. Authorised SSCD of Type 1 are able to establish a trusted channel to the SSCD of Type 2 for SCD transfer as required by FTP_ITC.1.3/SCD export.

**FDP_ITC.1/DTBS Import of user data without security attributes**

**FDP_ITC.1.1/DTBS** The TSF shall enforce the **Signature-creation SFP** when importing user data, controlled under the SFP, from outside of the TOE.

**FDP_ITC.1.2/DTBS** The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

**FDP_ITC.1.3/DTBS** The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **DTBS-representation shall be sent by an authorised SCA**.

*Application note:*

A SCA is authorised to send the DTBS-representation if it is actually used by the Signatory to create an electronic signature and able to establish a trusted channel to the SSCD as required by FTP_ITC.1.3/SCA DTBS.

**FDP_RIP.1 Subset residual information protection**

**FDP_RIP.1.1** The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **SCD, VAD, RAD**.

**FDP_SDI.2/Persistent Stored data integrity monitoring and action**

**FDP_SDI.2.1/Persistent** The TSF shall monitor user data stored in containers controlled by the TSF for **integrity error** on all objects, based on the following attributes: **integrity checked persistent stored data**.

**FDP_SDI.2.2/Persistent** Upon detection of a data integrity error, the TSF shall

**Prohibit the use of the altered data**

**Inform the Signatory about integrity error**.

**FDP_SDI.2/DTBS Stored data integrity monitoring and action**

**FDP_SDI.2.1/DTBS** The TSF shall monitor user data stored in containers controlled by the TSF for **integrity error** on all objects, based on the following attributes: **integrity checked stored data**.

**FDP_SDI.2.2/DTBS** Upon detection of a data integrity error, the TSF shall

**Prohibit the use of the altered data**

**Inform the Signatory about integrity error**.

**FDP_UCT.1/Receiver Basic data exchange confidentiality**

**FDP_UCT.1.1/Receiver** The TSF shall enforce the **SCD import SFP** to **receive** user data in a manner protected from unauthorised disclosure.

**FDP_UIT.1/SVD Transfer Data exchange integrity**

**FDP_UIT.1.1/SVD Transfer** The TSF shall enforce the **SVD Transfer SFP** to **transmit** user data in a manner protected from **modification and insertion** errors.

**FDP_UIT.1.2/SVD Transfer** The TSF shall be able to determine on receipt of user data, whether **modification and insertion** has occurred.

**FDP_UIT.1/TOE DTBS Data exchange integrity**

**FDP_UIT.1.1/TOE DTBS** The TSF shall enforce the **Signature-creation SFP** to **receive** user data in a manner protected from **modification, deletion and insertion** errors.

**FDP_UIT.1.2/TOE DTBS** The TSF shall be able to determine on receipt of user data, whether **modification, deletion and insertion** has occurred.

#### 8.1.1.3 FIA: Identification and authentication

**FIA_AFL.1 Authentication failure handling**

**FIA_AFL.1.1** The TSF shall detect when

**3 successive attempts to authenticate the Bearer**

**5 succesive attempts to authenticate the Sender**

**5 succesive attempts to authenticate the Signatory**

unsuccessful authentication attempts occur related to **consecutive failed authentication attempts**.

**FIA_AFL.1.2** When the defined number of unsuccessful authentication attempts has been **met and surpassed**, the TSF shall

**Block the PIN**

**Block the PUK**

**When the RAD is blocked, any new authentication attempt fails**.

**FIA_ATD.1 User attribute definition**

**FIA_ATD.1.1** The TSF shall maintain the following list of security attributes belonging to individual users: **RAD**.

**FIA_UAU.1 Timing of authentication**

**FIA_UAU.1.1** The TSF shall allow

**Identification of the user by means of TSF required by FIA_UID.1.**

**Establishing a trusted channel between the TOE and a SSCD of Type 1 by means of TSF required by FTP_ITC.1/SCD import. (not applicable for SSCD Type 3)**

**Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE.**

**Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import**

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.

*Application note:*

"Local user" mentioned in component FIA_UAU.1.1 is the user using the trusted path provided between the SGA in the TOE environment and the TOE as indicated by FTP_TRP.1/SCA and FTP_TRP.1/TOE.

**FIA_UID.1 Timing of identification**

**FIA_UID.1.1** The TSF shall allow

**Establishing a trusted channel between the TOE and a SSCD of Type 1 by means of TSF required by FTP_ITC.1/SCD import.**

**Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE. (not applicable for SSCD Type 3)**

**Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import**

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

**FIA_UID.1.2** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

#### 8.1.1.4 FMT: Security management

**FMT_MOF.1 Management of security functions behaviour**

**FMT_MOF.1.1** The TSF shall restrict the ability to **enable** the functions **signature-creation function** to **Signatory**.

**FMT_MSA.1/Administrator Management of security attributes**

**FMT_MSA.1.1/Administrator** The TSF shall enforce the **SCD Import SFP (SSCD Type 2) and the Initialization SFP (SSCD Type 3)** to restrict the ability to **modify** the security attributes **SCD / SVD management and secure SCD import allowed** to **Administrator**.

**FMT_MSA.1/Signatory Management of security attributes**

**FMT_MSA.1.1/Signatory** The TSF shall enforce the **Signature-creation SFP** to restrict the ability to **modify** the security attributes **SCD operational** to **Signatory**.

**FMT_MSA.2 Secure security attributes**

**FMT_MSA.2.1** The TSF shall ensure that only secure values are accepted for **security attributes**.

**FMT_MSA.3 Static attribute initialisation**

**FMT_MSA.3.1** The TSF shall enforce the **SCD Import SFP, Initialization SFP and Signature-creation SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

*Refinement:*

The security attribute of the SCD "SCD operational" is set to "no" after import of the SCD. The security attribute of the SCD "SCD operational" is set to "no" after generation of the SCD.

**FMT_MSA.3.2** The TSF shall allow the **Administrator** to specify alternative initial values to override the default values when an object or information is created.

**FMT_MTD.1 Management of TSF data**

**FMT_MTD.1.1** The TSF shall restrict the ability to **modify** the **RAD** to **Signatory**.

**FMT_SMR.1 Security roles**

**FMT_SMR.1.1** The TSF shall maintain the roles **Administrator and Signatory**.

**FMT_SMR.1.2** The TSF shall be able to associate users with roles.

#### 8.1.1.5 FPT: Protection of the TSF

### FPT_EMS.1 TOE Emanation

**FPT_EMS.1.1** The TOE shall not emit **side channel** in excess of **state of the art** enabling access to **RAD** and **SCD**.

**FPT_EMS.1.2** The TSF shall ensure **any user** are unable to use the following interface **external interface** to gain access to **RAD** and **SCD**.

*Application note:*

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

### FPT_FLS.1 Failure with preservation of secure state

**FPT_FLS.1.1** The TSF shall preserve a secure state when the following types of failures occur:

**Exposure to out-of-range operating conditions where therefore a malfunction could occur,**

**Failure detected by TSF according to FPT_TST.1**.

### FPT_PHP.1 Passive detection of physical attack

**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.

**FPT_PHP.3 Resistance to physical attack**

**FPT_PHP.3.1** The TSF shall resist

**Reducing the clock to stop the TOE during a specific operation**

**Raising of the clock to corrupt the TOE**

**Changing the temperature in order to corrupt operations of the TOE**

**Changing the voltage in order to corrupt operations of the TOE**

to the **TSF** by responding automatically such that the SFRs are always enforced.

*Application note:*

The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic response" means here

Assuming that there might be an attack at any time and

Countermeasures are provided at any time.

**FPT_TST.1 TSF testing**

**FPT_TST.1.1** The TSF shall run a suite of self tests **during initial start-up** to demonstrate the correct operation of **the TSF**.

**FPT_TST.1.2** The TSF shall provide authorised users with the capability to verify the integrity of **TSF data**.

**FPT_TST.1.3** The TSF shall provide authorised users with the capability to verify the integrity of **stored TSF executable code**.

#### 8.1.1.6 FTP: Trusted path/channels

**FTP_ITC.1/SCD Import Inter-TSF trusted channel**

**FTP_ITC.1.1/SCD Import** The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

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

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

**FTP_ITC.1/SVD Transfer Inter-TSF trusted channel**

**FTP_ITC.1.1/SVD Transfer [Editorially Refined]** The TSF shall provide a communication channel between itself and another trusted IT product (SSCD Type 2) CGA (SSCD Type 3) 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 Transfer [Editorially Refined]** The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

**FTP_ITC.1.3/SVD Transfer** The TSF shall initiate communication via the trusted channel for **transfer of SVD (SSCD Type 2) or export SVD (SSCD Type 3)**.

**FTP_ITC.1/DTBS Import Inter-TSF trusted channel**

**FTP_ITC.1.1/DTBS Import** The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

**FTP_ITC.1.2/DTBS Import [Editorially Refined]** The TSF shall permit **SCA** to initiate communication via the trusted channel.

**FTP_ITC.1.3/DTBS Import** The TSF shall initiate communication via the trusted channel for **signing DTBS-representation**.

**FTP_TRP.1/TOE Trusted path**

**FTP_TRP.1.1/TOE** The TSF shall provide a communication path between itself and **local** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **modification and disclosure**.

**FTP_TRP.1.2/TOE** The TSF shall permit **local users** to initiate communication via the trusted path.

**FTP_TRP.1.3/TOE** The TSF shall require the use of the trusted path for **initial user authentication**.

### *8.1.2 Security Requirements for the IT environment*

#### 8.1.2.1 Signature key generation (SSCD Type 1)

FCS_COP.1/CORRESP is also contained in this category. The same description is done, so Morpho let the SFR in the first mentioned part.

**FCS_CKM.1 Cryptographic key generation**

**FCS_CKM.1.1** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[R20] [R21]** and specified cryptographic key sizes **from 512 to 2048 bits with 64 bits of difference between two keys** that meet the following: **[R18]**.

**FCS_CKM.4/Type 1 Cryptographic key destruction**

**FCS_CKM.4.1/Type 1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **Key overwriting** that meets the following: **None**.

**FCS_COP.1/CORRESP Cryptographic operation**

**FCS_COP.1.1/CORRESP** The TSF shall perform **SCD / SVD correspondence verification** in accordance with a specified cryptographic algorithm **(cf FCS_COP.1)** and cryptographic key sizes **(cf FCS_COP.1)** that meet the following: **(cf FCS_COP.1)**.

**FDP_ACC.1/SCD Export SFP Subset access control**

**FDP_ACC.1.1/SCD Export SFP** The TSF shall enforce the **SCD Export SFP** on **export of SCD by Administrator**.

**FDP_UCT.1/Sender Basic data exchange confidentiality**

**FDP_UCT.1.1/Sender** The TSF shall enforce the **SCD Export SFP** to **transmit** user data in a manner protected from unauthorised disclosure.

**FTP_ITC.1/SCD Export Inter-TSF trusted channel**

**FTP_ITC.1.1/SCD Export** The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

**FTP_ITC.1.2/SCD Export [Editorially Refined]** The TSF shall permit **The TSF (the SSCD type 1)** to initiate communication via the trusted channel.

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

*Application note:*

If the TOE exports the SVD to a SSCD Type 2 and the SSCD Type 2 holds the SVD then the trusted channel between the TOE and the SSCD type 2 will be required.

#### 8.1.2.2 Certification Generation Application (CGA)

**FCS_CKM.2/CGA Cryptographic key distribution**

**FCS_CKM.2.1/CGA** The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **qualified certificate** that meets the following: **[R18]**.

**FCS_CKM.3/CGA Cryptographic key access**

**FCS_CKM.3.1/CGA** The TSF shall perform **Access to SCD/SVD in reading/writing to perform SCD/SVD generation or destruction operation**

**and loading of SCD/SVD for cryptographic treatment concerning electronic signature generation** in accordance with a specified cryptographic key access method **Access inreading/writing of the executed code stored in ROM to a key stored in EEPROM through the RAM that is protected in integrity and confidentiality** that meets the following: **[R20], [R21]**.

**FDP_UIT.1/SVD Import Data exchange integrity**

**FDP_UIT.1.1/SVD Import** The TSF shall enforce the **SVD Import SFP** to **receive** user data in a manner protected from **modification and insertion** errors.

**FDP_UIT.1.2/SVD Import** The TSF shall be able to determine on receipt of user data, whether **modification and insertion** has occurred.

**FTP_ITC.1/SVD Import Inter-TSF trusted channel**

**FTP_ITC.1.1/SVD Import** The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

**FTP_ITC.1.2/SVD Import [Editorially Refined]** The TSF shall permit **The TSF (the CGA)** to initiate communication via the trusted channel.

**FTP_ITC.1.3/SVD Import** The TSF shall initiate communication via the trusted channel for **import of SVD**.

#### 8.1.2.3 Signature Creation Application (SCA)

**FCS_COP.1/SCA Hash Cryptographic operation**

**FCS_COP.1.1/SCA Hash** The TSF shall perform **hashing the DTBS** in accordance with a specified cryptographic algorithm

**SHA-1**

**SHA-256**

and cryptographic key sizes **none** that meet the following: **List of approved algorithms and parameters**.

**FDP_UIT.1/SCA DTBS Data exchange integrity**

**FDP_UIT.1.1/SCA DTBS** The TSF shall enforce the **Signature-creation SFP** to **transmit** user data in a manner protected from **modification, deletion and insertion** errors.

**FDP_UIT.1.2/SCA DTBS** The TSF shall be able to determine on receipt of user data, whether **modification, deletion and insertion** has occurred.

**FTP_ITC.1/SCA DTBS Inter-TSF trusted channel**

**FTP_ITC.1.1/SCA DTBS** The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

**FTP_ITC.1.2/SCA DTBS** The TSF shall permit **the TSF** to initiate communication via the trusted channel.

**FTP_ITC.1.3/SCA DTBS** The TSF shall initiate communication via the trusted channel for **signing DTBS-representation by means of the SSCD**.

**FTP_TRP.1/SCA Trusted path**

**FTP_TRP.1.1/SCA** The TSF shall provide a communication path between itself and **local** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **modification and disclosure**.

**FTP_TRP.1.2/SCA [Editorially Refined]** The TSF shall permit **The TSF (the SCA)** to initiate communication via the trusted path.

**FTP_TRP.1.3/SCA** The TSF shall require the use of the trusted path for **initial user authentication**.

### *8.1.3 Basic TOE*

This section presents the security functional requirements for the Basic TOE, applicable to PPES Basic.

#### 8.1.3.1 Atomicity

The Security Functional Requirements of this section support the objective O.Atomicity. They address the rollback of incomplete memory writings upon software or hardware interruption.

The goal of SFRs is the following:

definition of the operations for which rollback is allowed, through FDP_ACC.1;

rollback rules through FDP_ROL.1.

**FDP_ROL.1/Atomicity Basic rollback**

**FDP_ROL.1.1/Atomicity** The TSF shall enforce **Access Control Policy for Atomicity** to permit the rollback of the **update** on the **file system and secret**.

**FDP_ROL.1.2/Atomicity** The TSF shall permit operations to be rolled back within the **same session and the user is authenticated**.

**FDP_ACC.1/Atomicity Subset access control**

**FDP_ACC.1.1/Atomicity** The TSF shall enforce the **Access Control Policy for Atomicity** on **File system update (EEPROM) and secret update**.

#### 8.1.3.2 Confidentiality

The Security Functional Requirements of this section support the objective O.Confidentiality. They address confidential TSF and User data during processing and transfer as well as when data is stored in memories.

The goal of the SFRs is the following:

access control through FDP_ACC.1 and FDP_ACF.1: any confidential TSF or User data must be protected against unauthorized access. Depending on the kind of data and their persistence, access control may translate for instance, into credentials for granting access or into encryption rules. These SFRs apply both to User and TSF confidential data. The requirements FMT_MSA.1 and FMT_MSA.3 allow specifying the management of the security attributes;

protected communication of confidential through FDP_UCT.1 (User data) and through FPT_ITC.1 (TSF data). Depending on the data and on the characteristics of the environment, the communication rules may imply, for instance, encryption of confidential data or strong authentication of the receptor;

no residual confidential information available through FDP_RIP.1. This SFR applies to TSF and User confidential data without distinction;

protection of confidential data during processing through FDP_UNO.1. This SFR applies to TSF and User confidential data without distinction.

This is a minimum set of SFRs, for which the ST author shall provide a complete instantiation.

**FDP_ACC.1/Confidentiality Subset access control**

**FDP_ACC.1.1/Confidentiality** The TSF shall enforce the **Access Control Policy for Confidentiality** on

**Subjects:**

**SUB_APPLI, SUB_CRYPTO, SUB_GS**

**Objects:**

**SUB_GS, OB_FILE, OB_SECRET, SUB_CRYPTO**

**Operations:**

**SUB_CRYPTO and SUB_APPLI are the only two subjects that can access to OB_SECRET by the intermediaty of SUB_GS**

**SUB_GS never accesses in read to the symmetric key values or asymetric bi-keys privtate keys or PIN code, that are stored in OB_SECRET for SUB_APPLI**

**SUB_GS creates for SUB_APPLI an OB_SECRET in OB_DFILE current directory is tha accesses conditions and its status for the creation are verified**

**SUB_APPLI or SUB_CRYPTO if OB_SECRET is in state created or activated and if the accesses conditions and its status for a writing operation are verified**

**SUB_GS accesses for SUB_APPLI to the activation, deactivation and termination operation to OB_SECRET object if the status of the object is coherent with the operation and if the access condition for the operation for this object are verified**

**SUB_GS accesse for SUB_APPLI to the unblock operation of an OB_SECRET if the status is coherent with the operation and accesses conditions for the operation on the secrets counters are verified**

**SUB_GS transferes in the cryptographic block the OB_SECRET for SUB_CRYPTO if the accesses conditions for the use of the secret are verified and if the OB_SECRET is integrate and not blocked**

**SUB_CRYPTO performs for SUB_APPLI a cryptographic operation with OB_SECRET transfered in the cryptographic blocks**

**SUB_APPLI accesses to SUB_CRYPTO for cryptographic operations with OB_SECRET files if the key and algorithm used are coherent with cryptographic operations**.

**FDP_ACF.1/APPLI Security attribute based access control**

**FDP_ACF.1.1/APPLI** The TSF shall enforce the **Access control SFP for "VITALE" services** to objects based on the following:

**Attribute security list:**

**Header command**

**Services table**

**Card life cycle**

**Application status**

**File/directory checksum**

**File status**.

**FDP_ACF.1.2/APPLI** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

**Rules:**

**SUB_GEST activates SUB_APPLI on a "SELECT" command reception, if:**

**Command header is coherent with the status of the card life cycle phase**

**Command header is valid and correspond to a "SELECT" command of the VITALE application**

**File/directory checksum of SUB_APPLI is correct**

**SUB_GEST forbides the call to a service, if:**

**Called subject and calling subject are not in coherence with the services table**

**SUB_APPLI treats the received command, if:**

**Command header is coherent with the life cycle status and the ADF file status is selected**

**Command header is coherent with the application status of SUB_APPLI**.

**FDP_ACF.1.3/APPLI** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

**Specific rules:**

**SUB_GEST always activates VITALE application by default if the received command is a VITALE 1 command**.

**FDP_ACF.1.4/APPLI** The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

**Specific rules:**

**SUB_GEST does not activate SUB_AIP, if:**

**Card life cycle is: USER, BLOCKED, END OF FILE**.

**FDP_ACF.1/FILE Security attribute based access control**

**FDP_ACF.1.1/FILE** The TSF shall enforce the **File access control SFP** to objects based on the following:

**Attribute security list:**

**Header command**

**Object type**

**DAC and complementary DAC**

**Level protection**

**Card security state**

**File/directory checksum**

**File status**.

**FDP_ACF.1.2/FILE** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

**Rules:**

**SUB_APPLI activates SUB_GF to perform creation/suppression/read/write/activation/deactivation/termination operations of an OB_DFILE/OB_EFILE if the command header and object type are coherent**

**SUB_GF performs creation operation of an OB_DFILE/OB_EFILE in a current OB_DFILE, if:**

**File object type created is a DF or EF**

**Current file "file state" is coherent with the operation**

**DAC and complementary DAC associated to the current protection level applicable to the current OB_DFILE are in coherence with the card security state**

**SUB_GF performs suppression operation of a current OB_DFILE/OB_EFILE, if:**

**Object type of the deleted file is different from MF**

**Current file status to be suppress is coherent with the operation**

**DAC and complementary DAC associated to the current protection level applicable to the current OB_DFILE are in coherence with the card security state**

**OB_DFILE must not contain objects or objects with types SECRET or TLV (whether destructed)**

**SUB_GF performs read/write operation in the current OB_DFILE/OB_EFILE, if:**

**File/directory checksum of the accedded file is correct**

**File status of the accedded file is coherent with the operation**

**DAC and complementary DAC associated to the current protection level applicable to the current OB_DFILE are in coherence with the card security state**

**SUB_GF performs activation/deactivation/termination operation of the current OB_DFILE/OB_EFILE, if:**

**Object type of the suppressed file is different from the MF**

**File status of the accedded file is coherent with the operation**.

**FDP_ACF.1.3/FILE** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **No rules**.

**FDP_ACF.1.4/FILE** The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

**Specific rules:**

**SUB_GF never accesses in creation/read/write/activation/deactivation/termination operation if the accessed OB_FILE object type is SECRET or TLV**

**SUB_GF never accesses in user phase in creation of an OB_EFILE/OB_DFILE in the current OB_DFILE, if:**

**Card life cycle is BLOCKED or END OF LIFE**

**Card security state does not indicate that the SMI is valid**

**Created file is of type MF or ADF**

**Current OB_DFILE file status is Deactivated or Terminated**

**SUB_GF never accesses in suppression to an OB_DFILE/OB_EFILE in the current OB_DFILE, if:**

**Card life cycle is BLOCKED or END OF LIFE**

**Object to be suppress is of type MF, ADF**

**SUB_GF never accesses in activation to the current OB_DFILE/OB_EFILE, if:**

**Current file status is TERMINATED**

**SUB_GF never accesses in deactivation to the current OB_DFILE/OB_EFILE, if:**

**Current file status is TERMINATED**

**Current file type is MF type**

**SUB_GF never accesses in termination of an OB_DFILE/OB_EFILE, if:**

**The file is of type MF**

**The file concerned is not the current file**.

**FDP_ACF.1/TLV Security attribute based access control**

**FDP_ACF.1.1/TLV** The TSF shall enforce the **TLV parameters access control SFP** to objects based on the following:

**Attribute security list:**

**Header command**

**Object type**

**DAC and complementary DAC**

**Card security state**

**TLV checksum**

**File status**.

**FDP_ACF.1.2/TLV** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

**Rules:**

**SUB_APPLI activates SUB_GT to perform creation/read/write operations in an OB_TLV, if the command header and the object type are coherent:**

**SUB_GT performs creation in an OB_TLV in the current OB_DFILE, if:**

**Current OB_DFILE file status is coherent with the operation**

**DAC and complementary DAC associated to the current OB_DFILE protection level are coherent with the card security state**

**SUB_GT performs read/write operation in OB_TLV for SUB_APPLI, if:**

**TLV checksum of the OB_TLV is correct**

**DAC is coherent with card security status**.

**FDP_ACF.1.3/TLV** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **No rules**.

**FDP_ACF.1.4/TLV** The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

**Specific rules:**

**SUB_GT never accesses in deletion to an OB_TLV**.

**FDP_ACF.1/SEC Security attribute based access control**

**FDP_ACF.1.1/SEC** The TSF shall enforce the **Secrets access control** to objects based on the following:

**Attribute security list:**

**Key type**

**Algorithm type**

**Ratification group**

**File/directory checksum**

**DAC**

**Card security state**

**Secret status**

**File status**.

**FDP_ACF.1.2/SEC** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

**Rules:**

**SUB_APPLI activates SUB_GS in order to access to OB_SECRET if the command header and object type are coherent**

**SUB_GS performs creation operation of an OB_SECRET in the current OB_DFILE, if:**

**Current OB_DFILE file status is coherent for the operation**

**DAC and complementary DAC associated to the protection level applied to the current OB_DFILE are coherent with the card security state**

**SUB_GS accesses to an OB_SECRET in read/write/unblock/activation/deactivation/termination, if:**

**OB_SECRET secret state is coherent with the opeation**

**Ratification group or use counter of OB_SECRET don't indicate "block" of the secret for read/write/activation/deactivation/termination operations**

**The secret DAC is coherent with the card security state for the operation**

**SUB_GS performrms activation/deactivation or termination operations of an OB_SECRET, if:**

**Secret status is coherent with the operation**

**Secret DAC is coherent with the card security state**

**SUB_GS accesses to the transfert of an OB_SECRET in cryptographic treatment blocks for SUB_CRYPTO, if:**

**Key type and algorithm type are coherent**

**Ratification group and use couter are coherent**

**Ratification counter or use counter or errors counter don't indicate "block" of the secret**

**File/directory checksum containing OB_SECRET is correct**

**Secret status of OB_SECRET is activated**

**OB_SECRET DAC is coherent with the card security state**.

**FDP_ACF.1.3/SEC** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **No rules**.

**FDP_ACF.1.4/SEC** The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

**Specific rules:**

**SUB_GS never accesses in read operation for SUB_APPLI to the symmetric key values, private asymmetric key values or PIN code that are stored in OB_SECRET**

**SUB_GS never accesses in write operation to OB_SECRET for SUB_APPLI, if the card security status does not indicate that SMI or SMC are valid.**

**SUB_GS never suppresses OB_SECRET**.

**FDP_RIP.1/Confidentiality Subset residual information protection**

**FDP_RIP.1.1/Confidentiality** The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects:

**OB_SECRET**

**OB_FILE**

**OB_TLV**

**OB_I/O**

**OB_TEMP**.

**FDP_UCT.1/Confidentiality Basic data exchange confidentiality**

**FDP_UCT.1.1/Confidentiality** The TSF shall enforce the **Access control for Confidentiality** to **transmit and receive** user data in a manner protected from unauthorised disclosure.

**FMT_MSA.1/Confidentiality Management of security attributes**

**FMT_MSA.1.1/Confidentiality** The TSF shall enforce the

**Access control SFP to "VITALE" services**

**Access control SFP to files**

**Access control SFP to TLV parameters**

**Access control SFP to secrets**

to restrict the ability to **[Operations, cf infra]** the security attributes **[Security attributes, cf infra]** to **[Authorized identified roles, cf infra]**.

*Refinement:*

The TSF restricts:

Transmitter and domain authority, the capacity to re-initialise the ratification counter (PTC) of the attributes "ratification group" and "use counter"

Transmitter and domain authority, the capacity to modify the attribute "secret state" to activated

Transmitter, the capacity to modify the attribute "application status"

Transmitter or embedder, the capacity to modify the attribute "current protection mode"

Transmitter or domain authority, the capacity to load attributes "file type", "file status", "DAC" and "protection mode" during creation of a directory or a file in a directory that belongs to its domain

Domain authority or transmitter the capacity to load attributes "key type", "DAC", "secret status" during the addition of a secret

**FPR_UNO.1/Confidentiality Unobservability**

**FPR_UNO.1.1/Confidentiality** The TSF shall ensure that **all users** are unable to observe the operation **[Operations, cf infra]** on **[Object, cf infra]** by **[Users/Subjects, cf infra]**.

*Refinement:*

Concerning all the subjects, two protections are defined, one for the private life concerning the VITALE data and one for the SSCD. The following operations are protected from unobservability.

VITALE data protection:

Update operation on OB_SECRET by SUB_GS

Use operation on OB_SECRET by SUB_CRYPTO

SSCD data protection:

Generation operation on SCD/SVD by the signatory or administrator

Use operation on SCD by the signatory

Update operation on the RAD by the administrator

**FPT_ITC.1/Confidentiality Inter-TSF confidentiality during transmission**

**FPT_ITC.1.1/Confidentiality** The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

*Refinement:*

"TSF data" stands for TSF data with confidentiality constraints.

**FMT_MSA.3/Confidentiality Static attribute initialisation**

**FMT_MSA.3.1/Confidentiality** The TSF shall enforce the **Access Control Policy for Confidentiality** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

**FMT_MSA.3.2/Confidentiality** The TSF shall allow the **Administrator** to specify alternative initial values to override the default values when an object or information is created.

### 8.1.3.3 Cryptography

The Security Functional Requirements of this section support the objective O.Crypto, as well as O.Disclosure and O.Integrity. They address the cryptographic functionalities of the TSF. This PP assumes that the TOE implements at least one cryptographic function.

The goal of the SFRs is the following:

specification of the cryptographic operations implemented by the TOE through FCS_COP.1;

specification of the key destruction mechanisms through FCS_CKM.4.

**FDP_ITC.1 Import of user data without security attributes**

**FDP_ITC.1.1** The TSF shall enforce the

**Access control SFP list:**

**Access control to "VITALE service"**

**Access control to files**

**Access control to TLV parameters**

**Access control to secrets**

**Access control for SSCD:**

**Importation SFP of SCD**

when importing user data, controlled under the SFP, from outside of the TOE.

**FDP_ITC.1.2** The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

**FDP_ITC.1.3** The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

**Access control SFP list:**

**no rules**

**Access control for SSCD:**

**SCD must be send by an authorized SSCD**.

#### 8.1.3.4 Integrity

The Security Functional Requirements of this section support the objective O.Integrity. They address TSF and User data with integrity constraints (referred to as "integer data" in the following) during processing, transfer and storage in memories. They address also TSF code.

The goal of the SFRs is the following:

- access control through FDP_ACC.1 and FDP_ACF.1: integer data must be protected against unauthorized modification. Depending on the kind of data and their persistence, access control may translate for instance, into credentials for granting modification or into cryptographic rules that mandate integrity checking before using the data. These SFRs apply both to User and TSF integer data. The requirements FMT_MSA.1 and FMT_MSA.3 allow specifying the management of the security attributes;
- protected communication of integer data through FDP_UIT.1 (User data) and FPT_ITI.1 (TSF data). Depending on the data and on the characteristics of the environment, the communication rules may imply, for instance, the use of cryptographic mechanisms or strong authentication of the receptor;
- integrity monitoring through FDP_SDI.2 (applied both to TSF and User integer data) and FPT_TST.1 (applied to TSF and User data as well as to TSF code).

**FDP_ACC.1/Integrity Subset access control**

**FDP_ACC.1.1/Integrity** The TSF shall enforce the **Access Control Policy for Integrity** on **All the subjects, objects and operations, by means of a CRC/LRC calculation**.

**FDP_SDI.2/Integrity Stored data integrity monitoring and action**

**FDP_SDI.2.1/Integrity** The TSF shall monitor user data stored in containers controlled by the TSF for **Integrity errors on checksum and deciphering** on all objects, based on the following attributes:

**All secrets (keys, PIN,...)**

**File system**

**Proprietary data**

**I/O buffer**.

**FDP_SDI.2.2/Integrity** Upon detection of a data integrity error, the TSF shall **refuse the usage of corrupted data**.

**FDP_UIT.1/Integrity Data exchange integrity**

**FDP_UIT.1.1/Integrity** The TSF shall enforce the **Access Control Policy for Integrity** to **transmit and receive** user data in a manner protected from **modification, deletion, replay and insertion** errors.

**FDP_UIT.1.2/Integrity** The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred.

**FMT_MSA.1/Integrity Management of security attributes**

**FMT_MSA.1.1/Integrity** The TSF shall enforce the

**Access control SFP to "VITALE" services**

**Access control SFP to files**

**Access control SFP to TLV parameters**

**Access control SFP to secrets**

to restrict the ability to **change_default, query, modify, delete and [Operations, cf infra]** the security attributes **[Security attributes, cf infra]** to **[Authorized identified roles, cf infra]**.

*Refinement:*

The TSF restricts:

Transmitter and domain authority, the capacity to re-initialise the ratification counter (PTC) of the attributes "ratification group" and "use counter"

Transmitter and domain authority, the capacity to modify the attribute "secret state" to activated

Transmitter, the capacity to modify the attribute "application status"

Transmitter or embedder, the capacity to modify the attribute "current protection mode"

Transmitter or domain authority, the capacity to load attributes "file type", "file status", "DAC" and "protection mode" during creation of a directory or a file in a directory that belongs to its domain

Domain authority or transmitter the capacity to load attributes "key type", "DAC", "secret status" during the addition of a secret

**FPT_ITI.1/Integrity Inter-TSF detection of modification**

**FPT_ITI.1.1/Integrity** The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: **Retail MAC**.

**FPT_ITI.1.2/Integrity** The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform **Retail MAC** if modifications are detected.

**FMT_MSA.3/Integrity Static attribute initialisation**

**FMT_MSA.3.1/Integrity** The TSF shall enforce the **Access Control Policy for Integrity** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

**FMT_MSA.3.2/Integrity** The TSF shall allow the **Administrator** to specify alternative initial values to override the default values when an object or information is created.

#### 8.1.3.5 Life cycle

The Security Functional Requirements of this section support the objective O.Life_cycle. They address the control of the life cycle states of the TSF and the transitions between them.

The goal of the SFRs is the definition of the states of the life cycle and access control rules to the operations in each state through FDP_ACC.1 and FDP_ACF.1. The transitions between states are among the operations. The requirements FMT_MSA.1 and FMT_MSA.3 allow to specify the management of the security attributes.

**FDP_ACC.1/Life_cycle Subset access control**

**FDP_ACC.1.1/Life_cycle** The TSF shall enforce the **Access control policy for life cycle** on

**Subjects:**

**All the subjects**

**Objects:**

**All the objects**

**Operations:**

**User phase. In this phase, the user can access to a set of functionalities**

**End of life. In this phase, the card is deactivated. No functionalities are accessible**.

**FDP_ACF.1/Life_cycle Security attribute based access control**

**FDP_ACF.1.1/Life_cycle** The TSF shall enforce the **Access Control Policy for Life Cycle** to objects based on the following: **SUB_PARAM, SUB_ADMIN, OB_CPLC and OB_CARD_STATE based on the following security attributes:**

**card status,**

**CRC OTP**.

**FDP_ACF.1.2/Life_cycle** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

**SUB_PARAM shall access to the OTP zone for OB_CPLC and OB_CARD_STATE objects recording only if the card status is initialized,**

**SUB_ADMIN shall access to OB_CPLC and OB_CARD_STATE only if the CRC attributes of the OTP zone are valid**

**SUB_GA shall forbid access to all subjects in the card terminated state**.

**FDP_ACF.1.3/Life_cycle** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **no rule**.

**FDP_ACF.1.4/Life_cycle** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **no rule**.

**FMT_MSA.1/Life_cycle Management of security attributes**

**FMT_MSA.1.1/Life_cycle** The TSF shall enforce the **Access Control Policy for Life Cycle** to restrict the ability to

**Modificate**

**Create**

**Usage**

the security attributes **all** to **all subjects in phase 7 (in terminated state, the card is deactivated)**.

**FMT_MSA.3/Life_cycle Static attribute initialisation**

**FMT_MSA.3.1/Life_cycle** The TSF shall enforce the **Access Control Policy for Life Cycle** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

**FMT_MSA.3.2/Life_cycle** The TSF shall allow the **All** to specify alternative initial values to override the default values when an object or information is created.

#### 8.1.3.6 Monitoring

The Security Functional Requirements of this section support the objective O.Monitoring. They address the monitoring of the potential security violations detected by the underlying IC.

The goal of the SFRs is the detection and response to potential security violations through FAU_ARP.1 and FAU_SAA.1. For each of the audited events, the developer shall provide the response implemented by the TSF.

**FAU_ARP.1/Monitoring Security alarms**

**FAU_ARP.1.1/Monitoring** The TSF shall take

**Invalidate objects**

**EEPROM deletion**

**Reset**

**End of life switching**

upon detection of a potential security violation.

**FAU_SAA.1/Monitoring Potential violation analysis**

**FAU_SAA.1.1/Monitoring** The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

**FAU_SAA.1.2/Monitoring** The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of

**Mode operation modification by the environment (sensor),**

**Access control violation attempt,**

**Memory self-test failure (ROM, EEPROM, RAM),**

**Cryptographic self-test failures**

**Integrity error, concernning:**

**file/directory**
**file header**
**TLV object**
**I/O buffer**
**Key**
**PIN code**
**Random number generator**
**Cryptographic processor**

known to indicate a potential security violation;

b) **not applicable**.

#### 8.1.3.7 Operate

The Security Functional Requirements of this section support the objective O.Operate. They address the correct execution of the TSF.

The goal of the SFRs is the following:

testing of critical functionalities and detection of integrity errors in TSF data or executable code through FPT_TST.1;

secure state in case of failure through FPT_FLS.1;

controlled activation, deactivation and configuration of functionality and data through FMT_MOF.1 and FMT_MTD.1.

| **FMT_MOF.1/Operate Management of security functions behaviour** |
|---|

**FMT_MOF.1.1/Operate** The TSF shall restrict the ability to **determine the behaviour of, disable, enable and modify the behaviour of** the functions **[List of functions, cf infra]** to **[Authorized identified roles, cf infra]**.

*Refinement:*

The patches of the TOE, uniquely referenced in the Configuration List, are excluded from the list of functions that can be enabled or disabled: the TOE patches are necessarily enabled. Instead, the functionalities implemented by these patches can be configured, if applicable.

*Refinement:*

| Behaviour | Functions | Roles |
|---|---|---|
| Activate/deactivate | Initialization operation | Pre-personalizer |
| Activate/deactivate | Personalization operation | Personalizer |
| Activate | Secret creation | Domain authority or Transmitter |
| Activate | File/directory creation or suppression | Domain authority or Transmitter |
| Activate | File/directory life cycle management | Domain authority or Transmitter |
| Activate | Secret life cycle management | Domain authority or Transmitter |
| Deactivate | Cryptographic key blocking | Domain authority or Transmitter |
| Deactivate | PIN code blocking | Transmitter |
| Activate | Code PIN changing | Transmitter or bearer |
| Activate/deactivate | Cryptographic key blocking (except SCD/SVD) | Domain authority or Transmitter |
| Activate/deactivate | SCD/SVD cryptographic key blocking | Transmitter |
| Activate | Changing (loading) of a cryptographic key (except SCD/SVD) | Domain authority or Transmitter |
| Activate | Changing (loading or generation) of a SCD/SVD cryptographic key | Transmitter or signatory |
| Activate/deactivate | Application blocking | Transmitter |
| Activate | Card blocking | Transmitter |

**FMT_MTD.1/Operate Management of TSF data**

**FMT_MTD.1.1/Operate** The TSF shall restrict the ability to **[cf infra]** the **[cf infra]** to **[cf infra]**.

*Refinement:*

TSF data management:

Code PIN value modification by the Transmitter or the bearer

Cryptographic key modification by the Transmitter or domain authority

Secret creation by the Transmitter or domain authority

Block/Unblock of a cryptographic key by the Transmitter or domain authority

Unblock of a PIN code by the Transmitter

Block/Unblock of an application by the Transmitter

Block/Unblock of the card by the Transmitter

**FPT_FLS.1/Operate Failure with preservation of secure state**

**FPT_FLS.1.1/Operate** The TSF shall preserve a secure state when the following types of failures occur:

**unexpected TSF execution interruption due to external events (power, tear-off),**

**integrity failure (OTP memories, files structure),**

**EEPROM programming failure**.

**FPT_TST.1/Operate TSF testing**

**FPT_TST.1.1/Operate** The TSF shall run a suite of self tests **during initial start-up** to demonstrate the correct operation of **TSF**.

**FPT_TST.1.2/Operate** The TSF shall provide authorised users with the capability to verify the integrity of **TSF data**.

**FPT_TST.1.3/Operate** The TSF shall provide authorised users with the capability to verify the integrity of **TSF**.

### 8.1.3.8 Random numbers

The Security Functional Requirements of this section support the objective O.RND.

The goal of the FIA_SOS.2 requirement is to state the characteristics of the random numbers provided by the TOE.

**FIA_SOS.2/RND TSF Generation of secrets**

**FIA_SOS.2.1/RND** The TSF shall provide a mechanism to generate secrets that meet **ANSI X9.31 standard for RNG [R22]**.

**FIA_SOS.2.2/RND** The TSF shall be able to enforce the use of TSF generated secrets for **TSF_RANDOM_NUMBERS enforces the corresponding IC TSF for generating random numbers**.

#### 8.1.3.9 Roles

The Security Functional Requirements of this section support the objectives O.Atomicity, O.Confidentiality, O.Integrity, O.Life_cycle and O.Operate.

The goal of the SFRs is as follows:

- definition of the roles involved in the management of the security attributes (FMT_MSA.1 and FMT_MSA.3), of the security functions (FMT_MOF.1) and of TSF data (FMT_MTD.1);
- specification of the functionality of the TOE before user identification by means of FIA_UID.1.

**FIA_UID.1/Basic Timing of identification**

**FIA_UID.1.1/Basic** The TSF shall allow **all TSF-mediated actions** on behalf of the user to be performed before the user is identified.

**FIA_UID.1.2/Basic** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

*Refinement:*

TSF_AUTHENTICATION manages the identification of the user.

**FMT_SMR.1/Basic Security roles**

**FMT_SMR.1.1/Basic** The TSF shall maintain the roles

**TSF Administrator**

**TSF Signatory**

**TSF User**.

**FMT_SMR.1.2/Basic** The TSF shall be able to associate users with roles.

### *8.1.4 Conclusion*

The following SFR are Security functional requirements for the Non-IT environment.

**R.Administrator_Guide - Application of Administrator Guidance** The implementation of the requirements of the Directive [R18], ANNEX II "Requirements for certification-service-providers issuing qualified certificates", literal (e), stipulates employees of the CSP or other relevant entities to follow the Administrator guidance provided for the TOE. Appropriate supervision of the CSP or other relevant entities shall ensures the ongoing compliance.

**R.Sigy_Guide - Application of User Guidance** The SCP implementation of the requirements of the Directive [R18], ANNEX II "Requirements for certification-service-providers issuing qualified certificates", literal (k), stipulates the signatory to follow the user guidance provided for the TOE.

**R.Sigy_Name - Signatory's name in the Qualified Certificate** The CSP shall verify the identity of the person to which a qualified certificate is issued according to the Directive [R18], ANNEX II "Requirements for certification-service-providers issuing qualified certificates", literal (d). The CSP shall verify that this person holds the SSCD which implements and stores the SCD corresponding to the SVD to be included in the qualified certificate.

## 8.2 Security Assurance Requirements

The security assurance requirement level is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

# 9 TOE Summary Specification

## 9.1 TOE Summary Specification

Development security is concerned with physical, procedural, personal and other technical measures that may be used in the development environment to protect the TOE. This assurance component is a higher hierarchical component to EAL4 (only ALC_DVS.1). Due to the nature of the TOE, there is a need for any justification of the sufficiency of these procedures to protect the confidentiality and integrity of the TOE.

ALC_DVS.2 has no dependencies.Due to the definition of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by the AVA_VAN.5 component.

Advanced methodical vulnerability analysis is based on highly detailed technical information. The attacker is assumed to be thoroughly familiar with the specific implementation of the TOE. The attacker is presumed to have a high level of technical sophistication. AVA_VAN.5 has dependencies with ADV_ARC.1 "Security architecture description", ADV_FSP.2 "Security-enforcing functional specification", ADV_IMP.1 "Implementation representation of the TSF", ADV_TDS.3 "Basic modular design", AGD_PRE.1 "Preparative procedures" and AGD_OPE.1 "Operational user Guidance".

All these dependencies are satisfied by EAL4. This section provides a summary of the security functions implemented by the TOE in order to fulfil the security functional requirements. The summary is structured in security functions.

This chapter presents the product security functionality. Organization and choices are oriented following the PPES [R26] and the chip public security target [R8].

**In the chip public security target, the following security functionalities are present:**

**TSF_INIT_A**, manages hardware initialization and TOE attribute initialization
**TSF_CONFIG_A**, manages the TOE configuration switching and control
**TSF_INT_A**, manages the TOE logical integrity
**TSF_TEST_A**, manages tests of the TOE
**TSF_FWL_A**, manages memory firewall
**TSF_PHT_A**, manages physical tampering protection
**TSF_ADMINIS_A**, manages security violation administrator
**TSF_OBS_A**, manages the unobservability
**TSF_SKCS_A**, manages the symmetric key cryptography support
**TSF_ASKCS_A**, manages the asymmetric key cryptography support
**TSF_ALEAS_A**, manages the unpredictable number generation support.

**The TOE contains the following security functionalities:**

**TSF_BOOT_AT_POWER_UP**

This security functionality manages the initialization of the TOE that happens after each reset warm or cold.

This security feature performs the following operations:

Test of the following items:

ROM memory segment

RAM memory

Random Number Generator

Crypto-processor

ATR issuing

Initialization of all modules and applications

**TSF_MONITORING**

This Security Functionality monitors all the events generated by the security IC physical detectors:

Bad CPU usage

integrity loss in EEPROM, ROM, OTP or RAM,

code signature alarm,

fault injection attempt,

watchdog timeout,

access attempt to unavailable or reserved memory areas,

MPU errors,

clock and voltage supply operating changes by the environment,

TOE physical integrity abuse.

Executable code integrity is controlled during its execution through the addition of code redundancies and specific tests. Code consistency is then ensured.

Automatic answers are provided when an error is detected. In order to perform this, this security functionality allows generating traces, containing the identity of the actor, concerning some transactions for the VITALE and ADELE applications. It also allows reacting to detected faults.

**TSF_EXECUTION_ENVIRONMENT**

This security functionality provides a secure execution environment based on the secure operation of CPU that controls the execution flow, detects and reacts to potential security violations.

After start-up, this function calls TSF_BOOT_AT_POWER_UP and waits for a terminal command. This command is either processed or redirected to another item. In particular, TSF_EXECUTION_ENVIRONMENT manages:

Application selection

Applications management (firewall)

A security group by application (PIN status, Key status, SECURE MESSAGING status)

Before sending a command to an application, this function tests its (syntaxic) validity. This function initializes a transaction with a previously selected application. Then, the managed security attributes are:

- When a transaction begins, the allocation of security attribute context and the initialization of all the security group status (set to FALSE)
- When a transaction ends, the release of the security attribute context (memory erasure with TSF_MEMORY_MANAGEMENT)
- The PIN status is set to TRUE on PINOK presentation
- The Key status is set to TRUE if mutual authentication has succedeed
- The Secure Messaging status is set to TRUE if the current command uses the Secure Messaging, is authenticated and checked for integrity
- The Secure Messaging status is set to FALSE after each processed command

**TSF_MEMORY_MANAGEMENT**

This security functionality manages the persistent and volatile memories of the product according to the capacities of the underlying security IC, so as to control access to sensitive content protected by the TOE.

TSF_MEMORY_MANAGEMENT manages the access to objects (files, directories, data and secrets) stored in EEPROM. Access for read or write to RAM and ROM is impossible from the outside, refer to TSF_IO_MANAGEMENT for more information.

The access in reading, writing is impossible from outside to:

- The ROM
- The RAM

This function manages access to files, directories, proprietary data (TLV) and stored keys in EEPROM.

**TSF_IO_MANAGEMENT**

This security functionality manages Input/Output interfaces by way of contact.

**TSF_LIFE_CYCLE_MANAGEMENT**

This security functionality manages the life cycle of the product and provides a secure transition mechanism between states. The various phases to be recognized are pre-personalization, personalization, usage and end of life.

The life cycle of the product is composed of 7 phases, more information is available in the dedicated paragraph 3.2.

At the end of the fabrication phase, after a test phase, chip test mode is inhibited in a non-reversible way: the data (system or user) are completely under the control of the card operating system.

**TSF_RANDOM_NUMBERS**

This security functionality provides random numbers. The random number generation is in conformance to the quality requirements:

A random number generator compliant with ANSI X9.31 for RNG

**TSF_ADMINISTRATION**

In User phase, the Administration application is not selectable anymore and no administration function is possible.

**TSF_AUTHENTICATION**

This security functionality manages mutual authentication and Issuer authentication.

The authentication can be performed using

MAC computation and a TDES key, on the complete message, computed by the terminal and submitted for verification to the card.

PIN verification

**TSF_CRYPTOGRAPHIC_OPERATIONS**

This security functionality provides a secure implementation of the following cryptographic operations:

Key generation, destruction and verification

Perform cryptographic operations

The following cryptographic algorithms are used by the application:

**RSA** PKCS#1 V2.1? padding v 1.5 and ISO 9796

**DES and 3DES** 3DES is used in ECB mode, with 128 bits key size, according with]

Secure messaging - Message Authentication Code (MAC), in accordance with the specified algorithm ANSI X9.19 (Retail MAC) and cryptographic key size: 128 bits.

CRC16 (Cyclic Redundancy Checks of 16 bits length) to perform integrity check

Random Number Generator (RNG) is compliant with Random Number Generator AIS31 (refer to TSF_RANDOM_NUMBERS)

Standard hash functions:

SHA-1 and SHA-256 in conformance with [FIPS180-2], in order to calculate a hash value.

**Encryption/decryption of data:** This operation relies on the use of TDES keys and is used in the following cases:

Encrypted keys transmission

Encryption/decryption of data

SMC use

**Decryption of secrets:** TSF_CRYPTOGRAPHIC_OPERATIONS uses TDES or RSA for deciphering an encrypted secret and imported in the card.

**Production/checking of authentication cryptograms:** TSF_CRYPTOGRAHPIC_OPERATIONS uses a CBC DES in retail mode for the trusted channel (SM) establishment. Cryptogram is used for the mutual au-

thentication and acts against the replay (ISO 9797-1). The functionality uses RSA for generate the card authentication cryptogram (RSA PKCS 1.5 and ISO 9796-2).

**VITALE 1 and 2 seal production:** TSF_CRYPTOGRAPHIC_OPERATIONS uses CBC DES in Retail mode for VITALE 1 seal production and CBC TDES for VITALE 2 seal production from

**Integrity checks on cryptographic keys and data:** TSF_CRYPTOGRAPHIC_OPERATIONS uses a CBC DES in retail mode. It ensures the integrity of data to which it is applied to the SMI.

**Secured electronic signature generation on external data:** TSF_CRYPTOGRAPHIC_OPERATIONS uses RSA PKCS#1 v2.1 - padding v 1.5 to generate an electronic signature on external data (hashed data).

**Electronic signature verification:** TSF_CRYPTOGRAPHIC_OPERATIONS uses RSA PKCS#1 v2.1 - padding v 1.5 to verify the certificate.

**PIN/PUK verification:** TSF_CRYPTOGRAPHIC_OPERATIONS performs PIN/PUK verification when it is presented to the card (For electronic signature, PIN code presented corresponds to the VAD that is compared to the reference value stored in the card).

**TSF_KEY_MANAGEMENT**

This security functionality provides a secure implementation of the following cryptographic operations:

Key generation, destruction and verification

Perform cryptographic operations

The following cryptographic algorithms are used by the application:

**RSA** PKCS#1 V2.1 padding v 1.5 and ISO 9796

**DES and 3DES** 3DES is used in ECB mode, with 128 bits key size, according with]

Secure messaging - Message Authentication Code (MAC), in accordance with the specified algorithm ANSI X9.19 (Retail MAC) and cryptographic key size: 128 bits.

CRC16 (Cyclic Redundancy Checks of 16 bits length) to perform integrity check

Random Number Generator (RNG) is compliant with Random Number Generator AIS31 (refer to TSF_RANDOM_NUMBERS)

Standard hash functions:

SHA-1 and SHA-256 in conformance with [FIPS180-2], in order to calculate a hash value.

**Encryption/decryption of data:** This operation relies on the use of TDES keys and is used in the following cases:

Encrypted keys transmission

Encryption/decryption of data

SMC use

**Decryption of secrets:** TSF_CRYPTOGRAPHIC_OPERATIONS uses TDES or RSA (up to 2048 bits) for deciphering an encrypted secret and imported in the card.

**Production/checking of authentication cryptograms:** TSF_CRYPTOGRAHPIC_OPERATIONS uses a CBC DES in retail mode for the trusted channel (SM) establishment. Cryptogram is used for the mutual authentication and acts against the replay (ISO 9797-1). The functionality uses RSA (up to 2048 bits) for generate the card authentication cryptogram (RSA PKCS 1.5 and ISO 9796-2).

**Integrity checks on cryptographic keys and data:** TSF_CRYPTOGRAPHIC_OPERATIONS uses a CBC DES in retail mode. It ensures the integrity of data to which it is applied to the SMI.

**Secured electronic signature generation on external data:** TSF_CRYPTOGRAPHIC_OPERATIONS uses RSA PKCS#1 v2.1 - padding v 1.5 (up to 2048 bits) to generate an electronic signature on external data (hashed data).

**Electronic signature verification:** TSF_CRYPTOGRAPHIC_OPERATIONS uses RSA PKCS#1 v2.1 - padding v 1.5 (up to 2048 bits) to verify the certificate.

**PIN/PUK verification:** TSF_CRYPTOGRAPHIC_OPERATIONS performs PIN/PUK verification when it is presented to the card (For electronic signature, PIN code presented corresponds to the VAD that is compared to the reference value stored in the card).

**TSF_ATOMIC_OPERATIONS**

This security functionality provides means of performing atomic operations, for instance, writing or easing of individual or multiple memory locations. The TOE shall guarantee that atomic operations are either performed completely or have no effect in case of interruption.

.

# 10 Appendix

## 10.1 Definitions

This section provides definitions about terms frequently used in this document. The definition of the Common Criteria related terms is specified in [R1] (Part 1, § 4).

## 10.2 Abbreviations

| | |
|---|---|
| **AC** | Autorité de Certification |
| **ADAE** | Agence pour le Développement de l'Administration Electronique |
| **ADF** | Application Directory File |
| **AMC** | Assurance Maladie Complémentaire |
| **AMO** | Assurance Maladie Obligatoire |
| **ARR** | Access Rules References |
| **APDU** | Application Protocol Data Unit |
| **ATR** | Answer To Reset |
| **CC** | Critères Communs |
| **CGA** | Certification Generation Application |
| **CMD/RSP** | Commande / Réponse |
| **CPS** | Carte Professionnel de Santé |
| **CSP** | Certification Service Provider |
| **CVC** | Certificat Vérifiable par une Carte |
| **DAC** | Data Access Conditions |
| **DES** | Data Encryption Standard |
| **DF** | Directory File |
| **DH** | Diffie-Helmann |
| **DTBS** | Data To Be Signed |
| **EAL** | Evaluation Assurance Level |
| **EF** | Elementary File |
| **EV** | Electronic Value |
| **FCI** | File Control Information |
| **GIE-SV** | GIE SESAM VITALE |
| **IAS** | Identification Authentification Signature |
| **MF** | Master File |
| **MOC** | Match On Card |
| **OTP** | One Time Programmable |
| **PIN** | Personal Identification Number |
| **PS** | Professionnels de santé |
| **PUK** | |
| **RAD** | Reference Authentication Data |
| **RSA** | Rivest Shamir Adelman |
| **SOF** | Strength of function |
| **SCA** | Signature-Creation Application |
| **SCD** | Signature-Creation Data |

| | |
|---|---|
| **AC** | Autorité de Certification |
| **SDO** | Signed Data Object |
| **SM** | Secure Messaging |
| **SSC** | Secure Signature Creation |
| **SSCD** | Secure Signature-Creation Device |
| **ST** | Security Target |
| **SVD** | Signature-Verification Data |
| **TI** | Technologies de l'Information |
| **TOE** | Target Of Evaluation |
| **TSF** | TOE Security Functions |
| **TSP** | TOE Security Policy |
| **VAD** | Validation Authentication Data |

## 10.3References

| Ref. | Document title |
|---|---|
| [R1] | *"Common Criteria for Information Technology Security Evaluation*<br>- *Part 1: Introduction and general model*<br>- *Part 2: Security functional requirements*<br>- *Part 3: Security assurance requirements"*<br>Version 3.1 Revision 3, July 2009 |
| [R2] | *"Protection Profile Embedded software for Smart Secure Devices Basic and Extended configurations"*<br>Version 1.0 November 2009<br>ANSSI-CC-PP-ESforSSD_Basic / ANSSI-CC-PP-ESforSSD_Extended |
| [R3] | *"Protection Profile - Secure Signature-Creation Device Type 2"*<br>Version 1.04 – July 2001 |
| [R4] | *"Protection Profile - Secure Signature-Creation Device Type 3"*<br>Version 1.05 – July 2001 |
| [R5] | *"Microcontrôleurs sécurisés SA23ZL48/34/18A et SB23ZL48/34/18A, incluant la bibliothèque cryptohraphique NesLib v2.0 ou v3.0, en configuration SA ou SB"*<br>EAL 5+, augmented with ALC_DVS.2 and AVA_VAN.5<br>ANSSI-CC-2010/08 – 08/03/2010 |
| [R6] | *"Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms with standard robustness level"*<br>Version 1.10 – September 2007 - ANSSI |
| [R7] | *"Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren."*<br>Version 1 – 25.09.2001 |
| [R8] | *"SA/SB23ZL48/34/18 Security Target – Public Version"*<br>Rev 01.00 – November 2009<br>SMD_ST23ZLxx_ST_09_002_ Rev 01.00 |
| [R9] | *Application Note : "Utilisation de la méthode AIS31"*<br>Version 3 – 07/03/07<br>NOTE/05.3 |
| [R10] | *"ISO/IEC 1443 Identification cards – Contactless integrated circuit cards – Proximity cards:*<br>- *ISO/IEC 14443-1:2008 : Physical characteristics*<br>- *ISO/IEC 14443-2:2001 : Radio frequency power and signal interface*<br>- *ISO/IEC 14443-3:2001 : Initialization and anticollision*<br>- *ISO/IEC 14443-4:2008 : Transmission protocol"* |
| [R11] | *"ISO 7816 Smart Card standard:*<br>- *ISO 7816-1: Physical characteristics*<br>- *ISO 7816-2: Dimensions and locations of the contacts*<br>- *ISO 7816-3: Electronic signals and transmission protocols*<br>- *ISO 7816-4: Industry commands for interchange*<br>- *ISO 7816-5: Number system and registration procedure for application identifiers*<br>- *ISO 7816-6: Interindustry data elements"* |

| Ref. | Document title |
|---|---|
| [R12] | *"Security IC Platform Protection Profile"* Version 1.0 – June 2007 BSI-PP-0035 |
| [R13] | *"Joint Interpretation Library, Application of Attack Potential to Smart Cards, supporting document for Common Criteria Interpretation"* Version 1.0 – March 2002 |
| [R15] | *"DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures Passports with Biometric Identification Capability."* December 1999 |
| [R16] | *"Algorithms and parameters for algorithms, list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the 'Electronic Signature Committee' in the Directive."* |
| [R17] | *"Supporting Document - Mandatory Technical Document - Application of Attack Potential to Smartcards"* Version 2.5 revision 1 – April 2008 |
| [R18] | *"Supporting Document - Mandatory Technical Document - Composite product evaluation for Smartcards and similar devices"* Version 1.0 Revision 1 – September 2007 |
| [R19] | *"Common Methodology for Information Technology Security Evaluation, Evaluation Methodology"* |
| [R20] | *"CWA 14890-1: Application Interface for smart cards used as Secure Signature Creation Devices – Part 1: Basic requirements – (AREA-K-1)"* April 2004 |
| [R21] | *"CWA 14890-2: Application Interface for smart cards used as Secure Signature Creation Devices – Part 2: Additional Services – (AREA-K-2)"* May 2004 |

# Index