ASE - Security Target
TOE - GXP3.2- E64PK-CC GemSafe V2
Product - GXP3.2-E64PK-CC
SSCD Type 2 (option a) and SSCD Type 3 (option b)

Certification ID : BSI-DSZ-CC-0281

UPDATES

Release	Date	Author	Modification
1.0	14 November 2005	Françoise FORGE	Public Security Target creation
2.01	20 February 2006	Françoise FORGE	Public Security Target update for Version 2.01

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

1.1 SECURITY TARGET IDENTIFICATION

Title:	Security Target
Reference:	ST GXP3-CC-GemSafeV2
Version:	2.01
Date of creation:	November 14th 2005
Date of modification:	20/02/06
Author:	GEMPLUS
TOE:	GXP3.2- E64PK-CC GemSAFE V2
TOE version:	2.01
Product:	GXP3.2-E64PK-CC
IT Security Evaluation scheme:	TÜViT German Scheme
IT Security Certification scheme:	BSI

This ST has been built with:

Common Criteria for Information Technology Security Evaluation Version 2.1 (ISO 15408), August 1999 which comprises [CCPART1], [CCPART2], and [CCPART3]

The CCIMB interpretation as of 01 December 2003 referenced in [AIS 32].

1.2 SECURITY TARGET OVERVIEW

The Target of Evaluation (TOE) is the GXP3 platform including the Digital Signature Application "GemSAFE V2" on. The platform includes the hardware and the operating system.

The **GXP3.2-E64PK-CC** product is a Smart Card Integrated Circuit (IC) with the GXP3 Gemplus Embedded Software (ES), that implements [JavaCard 2.1.1] and [GP2.0.1], GemSAFE V2 applet and ROMed application defined in Table 1.

All applications code are masked in ROM.
Except for **GemSAFE V2, MPCOS and GemSafe** other ROMed applications are locked and cannot be instantiated or personalized.

The Gemplus **GemSAFE V2** application is compliant with E-sign specifications (PK and SK authentication).
It covers the identity, digital signature and data storage services. The Digital signature key size is included between 512 bit and 2048 bit.

The Target Of Evaluation defined in this Security Target is the Secure Signature Creation Device (SSCD) functionalities provided by the GemSafe V2 application, supported by the GXP3 platform.
The other applications are not in the TOE Scope of Control and therefore not part of the evaluation.

TOE Components	**Version**	**Constructor**
Micro Controller	SLE66CX642P/m1485b16 with RSA 2048 V1.30	INFINEON
Embedded Software	GXP3.2-E64PK-CC version 3.2	GEMPLUS
Digital signature application	GemSAFE V2	GEMPLUS
Other non TOE Components	**Version**	**Constructor**
Instanciable ROMed applications	MPCOS version 3.01 GemSafe version 1.11	GEMPLUS GEMPLUS
Other Deactivated non-instanciable applications	GemID version 1.02 VSDC /PSE version 2.5 GS-CIS Dreifus C3 Applet Version 1.0.0.0	GEMPLUS VISA Dreifus

Table 1 – GXP3 Digital Signature Card components

This Security Target describes:

The Target Of Evaluation, the TOE components, the components in the TOE environment, the product type, the TOE environment and life cycle, the limits of the TOE.

The Assets to be protected and the threats to be countered by the TOE itself or its environment during the development and usage of the TOE.

The security objectives for the TOE and its environment

The security requirements the TOE security functional requirements and the TOE security assurance requirements

The security functions and the assurance measures

1.3 CC CONFORMANCE CLAIM

This Security Target is CC part2 extended with the SFR FPT_EMSEC.1 (see Appendix 1- PPSSCD Rationale) and CC part 3 conformant

The TOE includes an Integrated Circuit certified with CC EAL5 augmented with ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4. Certificate reference BSI-DSZ-CC-0315-2005.
It is a composite evaluation, evaluated with application of [AIS36] .

The TOE provides a Digital Signature application and claims compliance to the certified PP SSCD Type 2 and Type 3

Other Security Requirements have been added in this Security Target, to take into account the GXP3 platform services that support the Digital Signature GemSAFE V2,

The assurance level is EAL4 augmented with:

AVA_MSU.3 (Misuse- Analysis and testing of insecure states)

AVA_VLA.4 (Vulnerability Analysis-Highly resistant

ADV_IMP.2 (Implementation of the TSF)

The minimum strength level for the TOE security functions is "**SOF-high**".

2. TOE DESCRIPTION

2.1 PRODUCT TYPE

The TOE is part of the product described below.
The product is an Open Platform Smart Card that provides Digital Signature creation services.
As shown in Figure 1 the GXP3 Signature Card it is composed of:

- The Integrated Circuit, Infineon SLE66CX642P,
- The Embedded Software of the GXP3 Platform
- ROMed application GemSAFE V2 digital signature application,
- ROMed application MPCOS,
- Other ROMed applications deactivated during the Card Initialization phase and therefore cannot be personalized or used afterwards

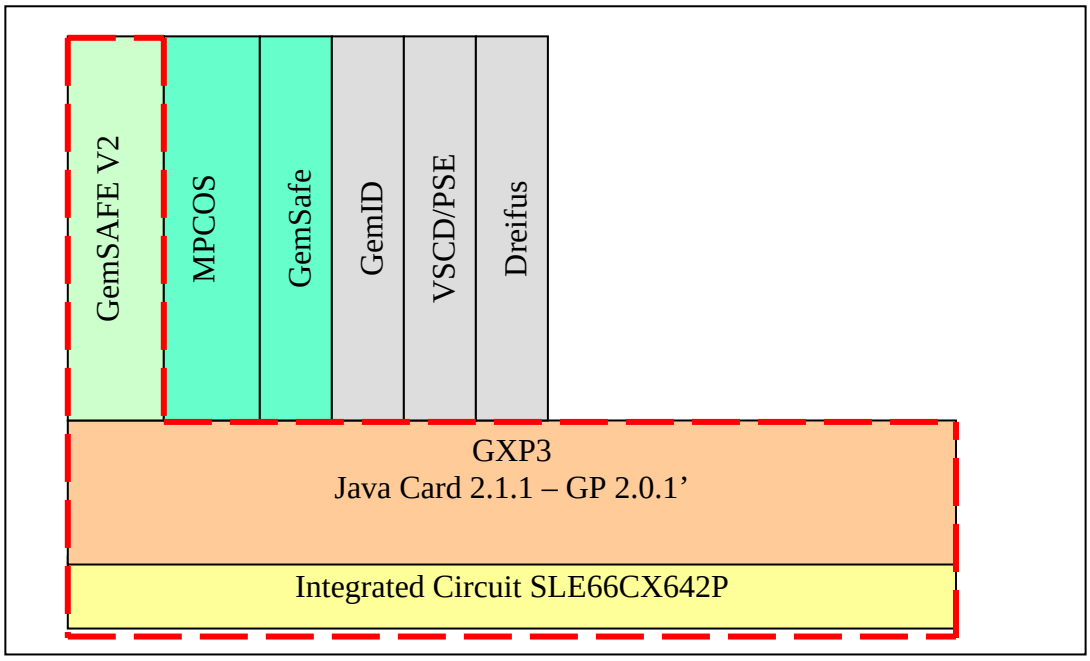

Figure 1 – GXP3 Digital Signature Card

- **The Integrated Circuit** is the SLE66CX642P/m1485b16 (short name SLE66CX642P) evaluated at EAL5+ level.
  The IC certificate ID is BSI-DSZ-CC-0315-2005
  The TOE Security Target is built using the Security Function provided by the IC and described in the IC Security Target reference : SLE66CX642P/m1485b16 With RSA 2048 V1.30
  The evaluation of the GXP3 Digital Signature Card is built upon the results of the evaluation of the SLE66CX642P.

- **GXP3 platform**, implements a Global Platform with a Java Card RTE and meets the following specifications :[JC 2.1.1] and [GP 2.0.1]

- **GemSAFE V2** is the Digital Signature applications, a Java Card type applet that meets [E-SIGN] specifications (PK and SK authentication schemes).
  It covers the identity, digital signature and data storage services. The Digital signature key size is included between 1024 bit and 2048 bit.

- **MPCOS** is a JavaCard Type application that provides Data Storage and e-purse services.
  MPCOS application relies also on the GXP3 GP JavaCard platform and uses interoperable interfaces.

- **VSDC**, VISA Smart Debit Credit application, is a JavaCard type application compliant with VISA specifications and provides EMV payment services

- **GemSafe** application is a JavaCard type application that provides also identity, digital signature and data storage services

- **GemID** is a JavaCard type application that provides identification/authentication services..

- **Dreifus** application is a JavaCard type application that provides also Digital Signature services.

2.2 TOE COMPONENTS

The red dot line in Figure 1 shows the limit of the TOE.
The TOE is limited to the Digital Signature provided by GemSAFE V2, the GXP3 services available to install and support GemSAFE V2, and the IC that supports the GXP3 platform.

As stated in section 1.2, GemID, VSDC, and Dreifus applications shown in gray in Figure 1 are locked during Card Initialization and cannot be installed or personalized. These applications are out of the TOE and the TOE environment.

The MPCOS and GemSafe applications, shown in green in Figure 1, are not part of the TOE either. These applications can be installed and personalized using GXP3 platform services. The platform ensures that these applications do not interfere with the GemSAFE V2 signature application.
These applications are tested according their specifications. Test plan and test results will be provided by the developer . These application byte code is verified conformant to Java Card specifications.

The IC full description is available in the IC Security Target referenced SLE66CX642P/m1485b16 With RSA 2048 V1.30

The following sections describes GXP3 platform and the GemSAFE V2 signature applet.

2.2.1 GXP3 platform description

The GXP3-CC is Java Open Platform that complies with 2 major industry standards

- Sun's Java Card 2.1.1, which consists of the Java Card 2.1.1 Virtual Machine, Java Card 2.1.1 Runtime Environment and the Java Card 2.1.1 Application Programming Interface.

- The GlobalPlatform Card Specification Version 2.0.1' that defines the card management, enhanced by the additional security features described in the Open Platform 2.0.1' Visa Card Implementation Requirements Configuration 2 -compact with PK. Wherever this reference manual refers to OP 2.0.1', this means the combination of the two documents.

The platform with the following components:

- The Operating System that provides the basic card functionalities with
  - Native layer libraries interfacing with the dedicated IC,
  - The cryptographic library proving DES and RSA algorithms, Hash algorithm and true random numbers.

- The Java Card Runtime Environment, which provides a secure framework for the execution of Java Card programs and data access management (firewall).

- The Open Platform Card Manager, which provides card and application management functions and security control.

The GXP3 platform card architecture is described in Figure 2
Further description of GXP3 functionalities is available in **[GemXpresso PRO R3]** Card Reference Manual

The platform is built upon the SLE66CX642P IC with a 64K EEPROM size. The EEPROM size can be limited to 36K by software configuration during personalization.
The TOE has two configurations . One configuration with a 64K EEPROM and one configuration with 36K EEPROM.
The GXP3 platform will provide the following services:

- Initialization of the GP card Manager and management the GP Card Life Cycle,
- Lock of the LOAD command to avoid loading of other applets in EEPROM in any life cycle state,
- Secure installation of the application under Card Manager control,
- Secure Messaging services during Applet personalization
- Extradition services to allow several Applet instances to share a dedicated Security Domain,
- Deletion of application instances under Card manager control
- Secure operation of the Applet instances through Java Card/ API
- Card basic security services as:
  - Environmental operating conditions check through information provided by the IC,
  - Life Cycle consistency check,
  - Integrity and confidentiality of Keys in PIN stored for the applet
  - Random generation
  - Secure data object handling and backup mechanisms,

- ROM and EEPROM integrity check,
- Memory content management,
- Mechanisms to prohibit other applets to interfere with GemSAFE V2 applet.

The limit of the TOE is marked with a red dot line

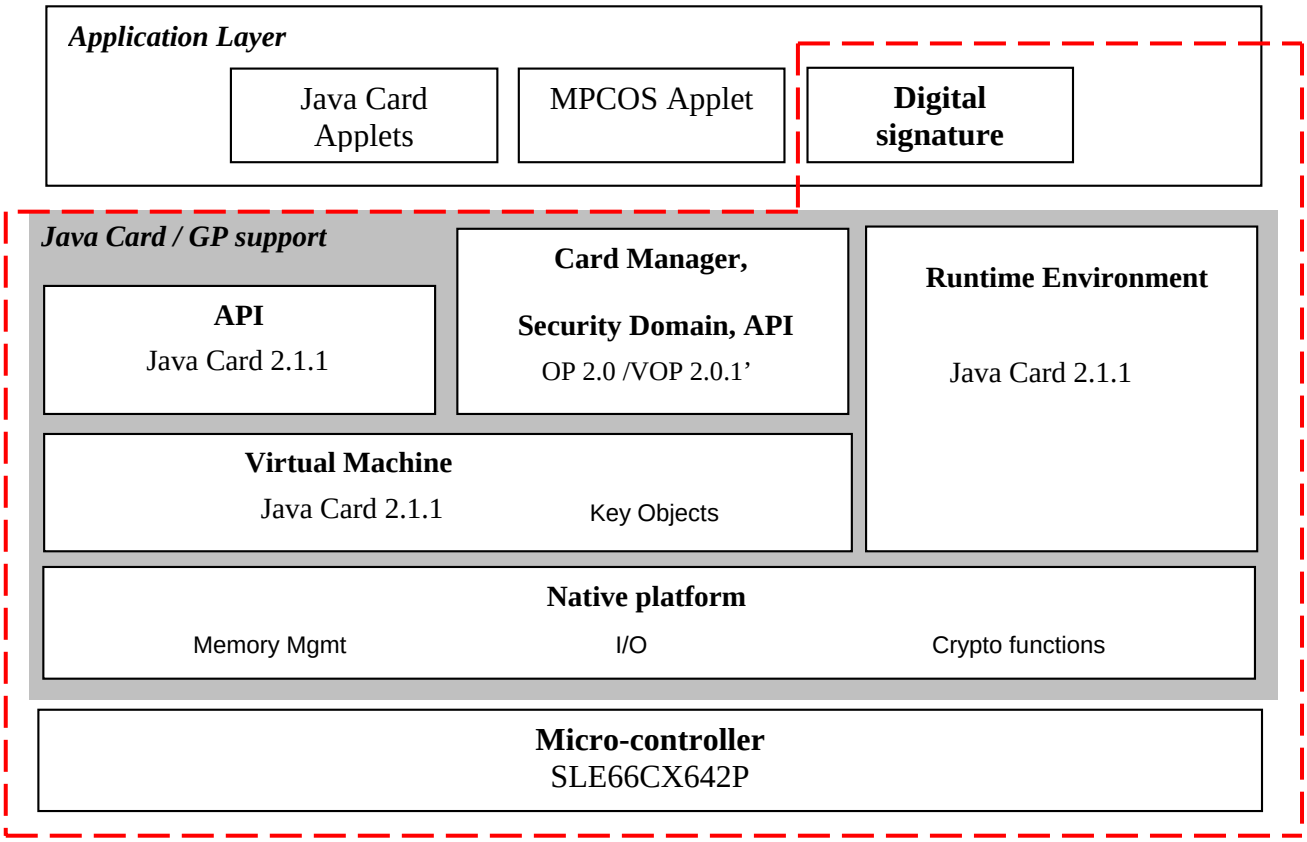

Figure 2 – GXP3 platform architecture

2.2.2 GemSAFE V2description

GemSAFE V2 is a Java Card application that provides a Secure Signature Creation Device [SSCD] as defined in the DIRECTIVE 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures" [DIRECTIVE].

Three Protection Profiles have been defined The SSCD PP for a TOE Type 1, which is a SCD/SVD generation component without signature creation and verification. The SCD generated on a SSCD Type 1 shall be exported to a SSCD Type 2 over a trusted channel [PP SSCD1].

- The SSCD PP for a TOE Type 2, which is a Signature creation and verification component [PP SSCD2]. This device imports the SCD from a SSCD Type 1
- The SSCD PP for a TOE Type 3, which is combination of the TOE Type 1 and Type 2 – i.e Generation and Signature creation/verification component. [PP SSCD3].

The **GemSAFE V2** application is compliant to a TOE Type 2 and Type 3 and supports

- The generation of SCD/SVD pairs on-board (option b) [PP SSCD3] during the personalization process of the card, or
- The import of the SCD (option a) via a trusted channel [PP SSCD2].
- The generation of electronic signatures.

GemSAFE V2 features the following options:

- Generation of digital signature with PK or SK schemes
- Instantiation of Stand Alone applet

GemSAFE V2 is aimed to create legal valid signatures and therefore provides mechanisms to ensure the Secure Signature Creation as:

- Authentication of the signatory,
- Authentication of the administrators,
- Integrity of access conditions to protected data
- Integrity of the Data to be Signed.
- External communication protection against disclosure and corruption (secure messaging).
- Access control to commands and data by authorized users.

2.3 TOE LIFE CYCLE

The TOE is composed of a Java Card Open Platform and a ROMed Java Card Applet.
The Open Platform and Applet global life cycle is described in Figure 3.

This figure represents the different step of the TOE, which follows a standard Smart Card life cycle.
For this product, the platform Software and Applet Software are designed at the same time and masked in ROM during IC manufacturing.
The figure indicates also the possibility of adding patches after masking and during the IC Initialization phase (3).

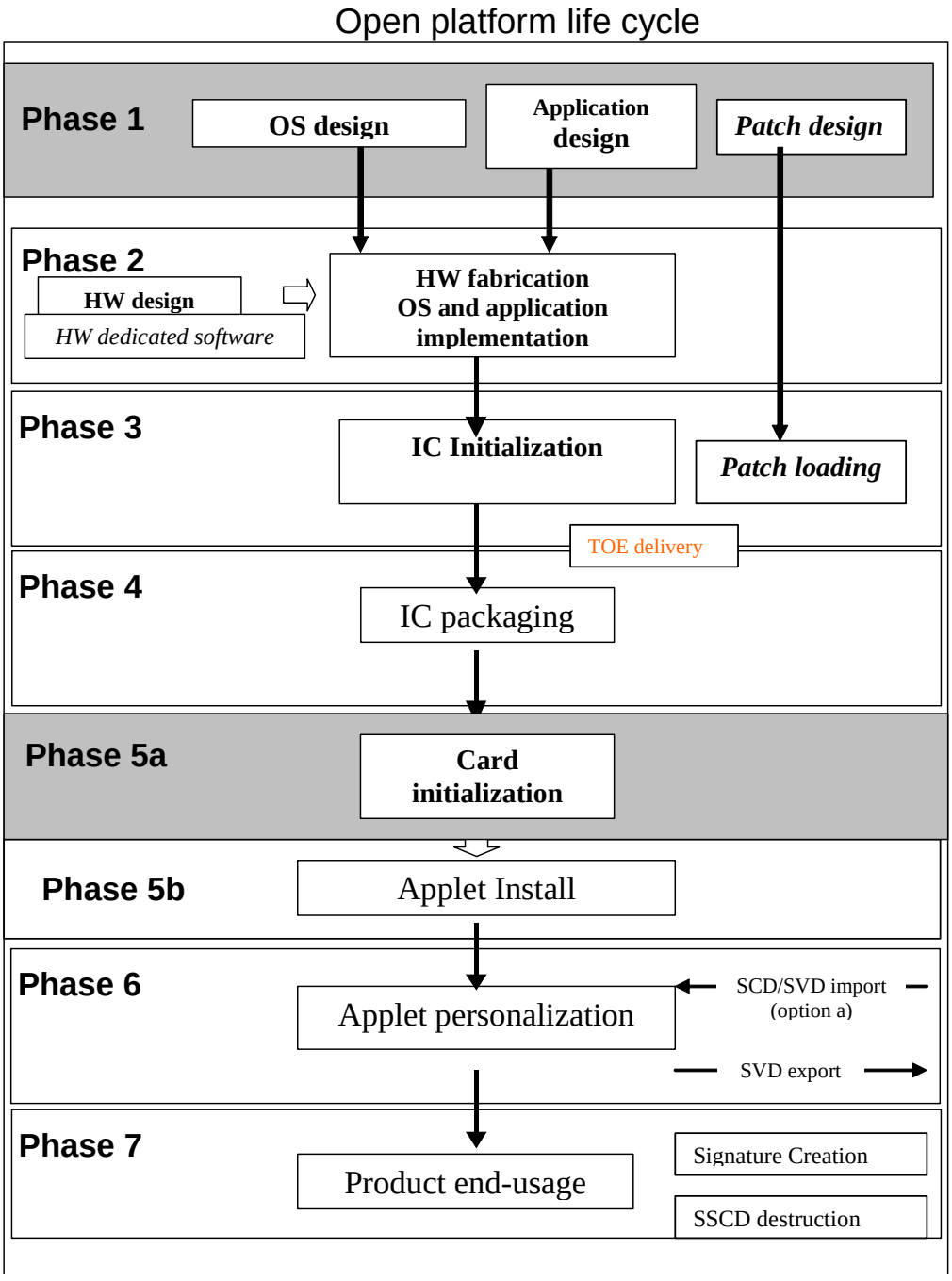

Figure 3 – Open Platform Life Cycle

In Figure 3 phase 3 to 5b correspond to the 'loading of general application data' phase of [PP SSCD2] and [PP SSCD2] Fig 3. (SSCD Life-cycle)
In this ST the TOE is delivered at the end of phase 3.(IC Initialization)

2.3.1 TOE actors

2.3.1.1 Administrators of the TOE

The administrators of the TOE are the developers, the manufacturers, the personalizer and the card issuers.

- The Product Developer designs the Embedded Software that includes Platform and Digital signature application software, during phase 1. For this product, the developer is **GEMPLUS** in La Ciotat site.

- The IC Manufacturer or founder- designs the IC during phase 2 and manufactures the Smart Card IC with the Embedded Software during phase 3. For this product, the silicon manufacturer is **INFINEON**

- The Card Manufacturer is responsible for:
  - Manufacturing the Smart Cards with the masked IC, packaging and testing during phase 4,
  - Smart Card product finishing process and testing during phase 4,
  - Card initialization (loading of data and setting Open platform to OP-READY state) during phase 5a,
  - Applet installation during phase 5b.

  For this product the card manufacturer is **GEMPLUS**

- The Platform Personalizer personalizes the card by loading the Card issuer and End user data as well as Application secrets such as cryptographic keys and PIN, during phase 6. For this product, the Personalizer is **GEMPLUS** or other Card-Issuer sites**.**

- The Applet Personalizer will
  - Generate instance of the installed application,
  - Load secret data as keys and PIN.
  - Imports SCD (option a)
  - Export SVD

  This occurs also during phase 6. For this product, the Platform Personalizer and Applet Personalizer is **GEMPLUS** or other Card-Issuer sites**.**

- The Card Issuer The Card issuer -short named « issuer » issues cards to its customers that are the « End users ». The card belongs to the Card issuer. Therefore, the Card Issuer is responsible during card usage phase (phase 7) for:
  - Distribution of the cards.
  - Maintenance of the cards (i.e. unblocking the PIN)
  - Invalidation of the cards.

  Depending on the product end usage, the Card issuers are Banks, Private companies or governmental organizations.

2.3.1.2 Users of the TOE

Usage of the TOE corresponds to phase 7, when the card has been fully personalized and delivered by the Card Issuer to the End User.

- The End User (or cardholder) is a customer of the Card issuer. The card is personalized with the End user identification and secrets (as SCD/SVD pairs for the digital signature application) and the End User PIN code.

- Terminals according to TOE end usage are Automatic Teller Machine (ATM), Point-Of-Sales terminal (POS), vending machines, SCA and CGA type for digital signature application

2.3.2 Limits of the TOE

Table 2 presents the TOE product type life-cycle with the logical phases and related Carrd and application state.

Phase	Limit of the TOE	Limits of the TOE Industrial Step	Industrial Deliverables	Logical Phase	TOE Administrators	Card State	Application state
1	Platform fabrication	Development	Platform ES	ES design	*Product developer*	None	None
			Application	Applet design	*Application developer*	None	None
2	Platform fabrication	Development	Hard mask set	IC design	*IC manufacturer*	None	None
3	Platform fabrication	Production	Wafers with Chips	IC Initialization	*IC manufacturer*	OS_NATIF	OS_NATIF
4	Platform fabrication	Production	Modules	IC Packaging	*Card manufacturer*	OS_NATIF	OS_NATIF
5	Platform fabrication	Production	Card with platform ES	Card Initialization	*Card manufacturer*	OP_READY INITIALIZED (SECURED)	
			And Applications	Applet Installed and selectable	Card manufacturer		INSTALLED SELECTABLE
6	Platform usage	Personalization	Card personalized	Card Personalization	*Platform Personalizer*	SECURED	PERSONALIZED
			Applet personalized	Applet personalized	*Applet personalizer*		PERSONALIZED
7	Platform usage	User – Use		Card Distribution Card Termination	*Card issuer End User*	SECURED LOCKED TERMINATED	PERSONALIZED BLOCKED LOCKED LOGICALLY-DELETED

Table 2 – Open Platform product type Life Cycle

The TOE limits correspond to the development phase (phase 1 to phase 2) and the production phase 3.
These limits are imposed by the fact that the Card manufacturing, initialization, applet installation are not always performed by the software developer at the same site.

The TOE provides security mechanisms to allow only authorized administrator to securely initialize and install and personalize the platform and applets.
Secure configuration and set up of the TOE are specified in Administrator and User Guidance documents.
Furthermore if the GP platform once in a SECURED state cannot go back to previous state, the application may be LOGICALLY-DELETED and new instances re-installed and personalized after post-issuance.

Logical phases of the platform and the applets are described in section 2.5.

2.4 TOE ENVIRONMENT

The TOE environment is defined as follow:

- Development environment corresponding to the Product developer environment (phase1), and the IC Photo mask Fabrication environment (phase 2);
- Production environment corresponding to the generation of the masked the IC (phase 3), the manufacturing of the card (phase 4), the initialization of the platform (phase 5a) and the installation of the applet (phase 5b), the test operations, and initialization of the ES;
- Personalization environment corresponding to phase 6 including personalization and testing of the Open platform Smart Card with the user data, the personalization of the Applet with the import of SCD (option a).
- User environment corresponding to phase 7.

2.4.1 Development environment

2.4.1.1 Software development ((Phase 1)

This environment is limited to GEMPLUS La Ciotat site.
To ensure security, access to development tools and products elements (PC, emulator, card reader, documentation, source code, etc…) is protected. The protection is based on measures for prevention and detection of unauthorized access. Two levels of protection are applied:

- Access control to GEMPLUS La Ciotat office and sensitive areas.
- Access to development data through the use of a secure computer system to design, implement and test software.

2.4.1.2 Hardware development (Phase 2)

This environment is limited to INFINEON sites.
The IC development environment is described in SLE66CX642P security target SLE66CX642P/m1485b16 With RSA 2048 V1.30.
The IC is certified EAL5+ and the IC certificate reference is BSI-DSZ-CC-0315-2005.

2.4.2 Production environment

2.4.2.1 IC initialization (Phases 3)

This environment is limited to INFINEON Dresden.
The IC development environment is described in SLE66CX642P security target SLE66CX642P/m1485b16 With RSA 2048 V1.30.

2.4.2.2 IC Packaging (phase 4)

This environment is limited to GEMPLUS La Ciotat site.
Access to IC packaging is physically protected. The protection is based on measures for prevention and detection of unauthorized access.

2.4.2.3 Card Initialization and applet installation (phase 5)

This environment is limited to GEMPLUS Gemenos site.
Access to production is physically protected. The protection is based on measures for prevention and detection of unauthorized access.

2.4.3 Personalization environment (phase 6)

This environment can be GEMPLUS Gemenos site, other Card Issuer preferred Site
Access to personalization site is physically protected. The protection is based on measures for prevention and detection of unauthorized access.

2.4.4 User environment (Phase 7)

At the end of phase 6, the Card Issuer delivers the Smart Card to the Card Holder.
The Card Holder as the signatory will use his Card for electronic signature purpose with dedicated terminals.

Terminals initiate an asymmetric mutual authentication and a Secure Channel is needed to ensure authenticity, integrity and confidentiality of the exchange.
The signatory will have to present his PIN (VAD) before being allowed to create signature.

2.5 LOGICAL PHASES

All along its life cycle, the TOE is under several logical phases as shown in Table 2.
Two life cycles have to be considered here: The open platform life cycle and the application life cycle

These phases are stored under a logical controlled sequence. The change from one phase to the next is under the TOE control.

2.5.1 Chip initialization:

Chip initialization logical phase is set by the IC manufacturer and allows the use of the IC_ key. This key is used for transportation protection between silicon manufacturer and card manufacturers in phase 4.

2.5.2 Card initialization:

The card initialization state is set at the end of phase 4. This state will allow the initialization of the platform, the loading of pre-personalization data including the Card Manager Keys
This occurs during phase 5. The platform and applet life-cycle states are changed with the following steps:

2.5.2.1 Platform states

- **OP-READY.**
  The state OP_READY indicates that the runtime environment shall be available and the Issuer Security Domain, acting as the selected Application, shall be ready to receive, execute and respond to APDU commands
  The following functionality shall be present when the card is in the state OP_READY:
  - The runtime environment shall be ready for execution,
  - The OPEN shall be ready for execution,
  - The Issuer Security Domain shall be the Default Selected Application,
  - Executable Load Files that were included in Immutable Persistent Memory shall be registered in the

- GlobalPlatform Registry,
- An initial key shall be available within the Issuer Security Domain.

The installation, from Executable Load Files, of any Application may occur.

- **INITIALIZED**
  The state INITIALIZED is an administrative card production state. The state transition from OP_READY to INITIALIZED is irreversible. This state may be used to indicate that some initial data has been populated (e.g. Issuer Security Domain keys and/or data) but that the card is not yet ready to be issued to the Cardholder.
  The card shall be capable of Card Content changes.

- **SECURED**
  The state SECURED is the intended operating card Life Cycle State in Post-Issuance. This state is used to enforce the Card Issuer's security policies related to Post-Issuance card behavior such as application loading, installation and activation. The state transition from INITIALIZED to SECURED is irreversible.
  The card is capable of Card Content and Application content changes.
  The SECURED state is used to indicate to off-card entities that the Issuer Security Domain contains all necessary keys and security elements for full functionality.

2.5.2.2 Applet states

- **INSTALLED**
  The state INSTALLED means that the Application executable code has been properly linked and that any necessary memory allocation has taken place. The Application becomes an entry in the GlobalPlatform Registry and this entry is accessible to authenticated off-card entities. The Application is not yet selectable. The installation process is not intended to incorporate personalization of the Application, which may occur as a separate step.
  The applet is installed after the platform is set at least to OP-READY state.
- **SELECTABLE**
  The state SELECTABLE means that the Application is able to receive commands from off-card entities. The state transition from INSTALLED to SELECTABLE is irreversible. The Application shall be properly installed and functional before it may be set to the state SELECTABLE. The transition to SELECTABLE may be combined with the Application installation process.

2.5.3 Card personalization

During this phase, the Card manage is fully operational. This phase is used by the Card Issuer to load additional personalization data.

During this phase, the applet personalization is completed. For the GemSAFE V2 application the SCD is imported (option a)

At the end of the applet personalization the applet state is set to **PERSONALIZED.** The transition from SELECTABLE to PERSONALIZED is irreversible.
Only Applet personalizer is allowed to execute this transition

2.5.4 Usage

2.5.4.1 Platform logical states

During usage phase the Platform can be set to the following states

- **LOCKED**
  The Card Life Cycle state LOCKED is present to provide the Card Issuer with the capability to disable Security Domain and Applications functionality. The Card Life Cycle state transition from SECURED to LOCKED is reversible.
  Setting the card to this state means that the card shall no longer function except via the Issuer Security Domain.
  Either the Card manager, or an off-card entity authenticated by the Issuer Security Domain may initiate the transition from the state SECURED to the state LOCKED.

- **TERMINATED**
  The state TERMINATED signals the end of the card Life Cycle and the card. The state transition from any other state to TERMINATED is irreversible. When in the state TERMINATED, all APDU commands shall be routed to the Issuer Security Domain and the Issuer Security Domain shall only respond to the GET DATA command.
  Either the Card manager, or an off-card entity authenticated by the Issuer Security Domain may initiate the transition to the state TERMINATED.

2.5.4.2 Applet logical states

- **BLOCKED**
  After an Integrity Problem or authentication locked due to ratification counter 0 caused by bad External Authentications, the applet is blocked. When the current state of of the Applet is BLOCKED, only the Get Data command is allowed.

- **LOCKED**
  The Card Manager or the off-card entity authenticated by the Issuer Security Domain uses the state LOCKED as a security management control to prevent the selection, and therefore the execution, of the Application.
  Once the state is LOCKED, only the Issuer Security Domain is allowed to unlock the Application. The Card Manager shall ensure that the Application Life Cycle returns to its previous state.

- **LOGICALLY-DELETED**
  At any point in the Application Life Cycle, the Card Manager may receive a request to delete an Application.
  The space previously used to store a physically deleted Application is reclaimed and may be reused. The entry within the GlobalPlatform Registry is also removed, and the Card Manager is not required to maintain a record of the deleted Application's previous existence.

2.6 TOE INTENDED USAGE

The TOE is dedicated to generate digital signature and complies to CEN/ISSS WS/E-Sign specifications see reference [E-Sign 1] and [E-Sign 2] in section 10

3. TOE SECURITY ENVIRONMENT

This section describes the security aspects of the TOE environment and addresses the description of the assets to be protected, the threats, the organizational security policies and the assumptions.

As this Security Target addresses the Digital Signature application and the Open Platform on which the application is installed, the following chapters will distinguish between the security elements related to the GemSAFE V2 and those related to the Open Platform.

Parts directly copied from the [PP SSCD2] or [PP SSCD3] are in black characters. Parts that have been added or modified are in blue characters.
(Option a) indicates that the security aspect element is specific to SSCD Type 2.
(Option b) indicates that the security aspect element is specific to SSCD Type 3.

3.1 ASSETS

3.1.1 Digital Signature assets

D.SCD	SCD : private key used to perform an electronic signature operation(confidentiality of the SCD must be maintained).
D.SVD	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).
D.DTBS	DTBS and DTBS-representation: set of data or its representation which is intended to be signed (their integrity must be maintained)
D.VAD	VAD: PIN code data entered by the End User to perform a signature operation (confidentiality and authenticity of the VAD as needed by the authentication method employed)
D.RAD	RAD: Reference PIN code authentication reference used to identify and authenticate the End User (Integrity and confidentiality of RAD must be maintained)
D.SIGN_APPLI	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)
D.SIGNATURE	Electronic signature : (unforgeability of electronic signatures must be assured).

3.1.2 Platform assets

All these assets have been added to the [PP SSCD2] and [PP SSCD3]

D. CODE	Executable code ROMed on the platform or patch loaded in EEPROM, including ROMed applet code.
D.GP_KEYS	FAB_KEY loaded by the IC manufacturer to authenticate the Card Manufacturer during phase 4 and 5 b
D.GP_REGISTRY	GP registry that contains Card Manager data for Card management operations this includes the following : [Card Life cycle State], [Application Life Cycle], [SD Life Cycle State], [ISD AID], [SD AID]
D.ISD_DATA	Issuer Security Domain Data that includes the following: [Card Image Number], [Issuer Identification Number], [Key Information Template], [SCP information template], [Available Command], [SCP Retry Counter]
D.ISD_KEYS	Issuer Security Domain Keys: Card Manager keys used during Applet initialization and card personalization. Includes keys for Authentication, Encryption and integrity (MAC)
D.SD_DATA	Application Security Domain Data includes [Key Information Template], [SCP information template]
D.SD_KEYS	Application Security domain keys includes, - Static Keys for secure channel operation (authentication), - Keys for cryptographic operations (cipher, MAC) during a session .
D.USER_PIN	Application User Pin. For the application GemSAFE V2 this data is the D.VAD
D.JAVA_OBJECT	Data Object belonging to an application identified with its SD[AID]

3.2 SUBJECTS

3.2.1 Digital signature subjects

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.
S.OFFCARD	**Attacker**. A human or 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.**

3.2.2 Platform subjects

All these assets have been added to the [PP SSCD2] and [PP SSCD3]

S.Card_Manufacturer	**Administrator** of the TOE, which can be identified as the Card Manufacturer. This entity is in charge of Platform initialization, installation of the Issuer Security domain (ISD) and set the platform to OP_READY state.
S.Card_Manager	This entity represent the Open Platform Card Issuer, manages the card

	content and controls application privileges. This entity will - Install/delete application instances - Manage the card life-cycle
S. Applet	Any application ROMed on the platform and using platform services.
S.OFFCARD	**Attacker**. A human or 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.**

3.3 THREATS

3.3.1 Digital Signature threats

T.Hack_Phys	Physical attacks through the TOE interfaces. An attacker **S.OFFCARD** interacts with the TOE interfaces to exploit vulnerabilities to gain fraudulent access to the **Assets**.
T.SCD_Divulg	Storing, copying, and releasing of signature-creation **D.SCD.** An attacker **S.OFFCARD** can store, copy the SCD**D.SCD** outside the TOE. An attacker **S.OFFCARD** can release the SCD **D.SCD** during generation, storage and use for signature-creation in the TOE.
T.SCD_Derive	Derive the signature-creation data **D.SCD.** An attacker **S.OFFCARD** derives the SCD **D.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 electronic signature **D.SIGNATURE.** An attacker **S.OFFCARD** 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 **D.SIGNATURE.** If an attacker **S.OFFCARD** 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 **D.SVD.** An attacker **S.OFFCARD** forges the SVD **D.SVD** presented by the TOE. This result in loss of SVD integrity in the certificate of the signatory.
T.DTBS_Forgery	Forgery of the DTBS-representation **D.DTBS.** An attacker **S.OFFCARD** modifies the DTBS-representation **D.DTBS.** 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 **D.SIGN_APPLI** . An attacker **S.OFFCARD** 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.

3.3.2 Platform threats

All these threats have been added to the [PP SSCD2] and[PP SSCD3]

T.Plt_Integrity	Integrity of Platform Data and code **S.OFFCARD** tries to alter Platform stored sensitive Data (assets) or Code to gain access to unauthorized data or operations This threat concerns **D.GP_KEYS**, **D.ISD_KEYS**, **D.SD_KEYS** and **D.CODE**
T.Plt_Confidentiality	Confidentiality of Platform Data **S.OFFCARD** tries to disclose Platform stored Data to gain access to unauthorized operations This threat concerns **D.GP_KEYS**, **D.ISD_KEYS**, **D.SD_KEYS**
T.Plt_Install	**S.OFFCARD** fraudulently install an applet on the card . This concerns either the installation of an unauthorized applet or an attempt to induce a malfunction in the TOE through the installation process. This threat concerns applets installation and mainly **D.GP_REGISTRY, D.SD_DATA and D.SD_KEYS**
T.Plt_Execution	**S.OFFCARD** or **S.APPLET** executes code in order to gain illegal access to platform or applet resources . This threat deals with **D.CODE** access
T.Plt_Operate	**S.OFFCARD** or **S.APPLET** tries to modify Platform behavior by unauthorized or incorrect use of commands, or by producing malfunction conditions This includes bad command, authentication bypass, insecure state by insertion or interruption of session. This threat concerns all platform assets

3.4 ASSUMPTIONS

This section defines assumptions related to the Digital Signature application as stated in PP SSCD, and assumptions related to the Smart Card platform.

3.4.1 Digital Signature assumptions

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 (option a)	Trustworthy SCD/SVD generation If a party other than the signatory generates the SCD/SVD-pair of a signatory, then (a) this party will use a SSCD for SCD/SVD-generation, (b) confidentiality of the SCD will be guaranteed until the SCD is under the sole control of the signatory and (c) the SCD will not be used for signature-creation until the SCD is under the sole control of the signatory. (d) The generation of the SCD/SVD is invoked by authorized users only (e) The SSCD Type 1 ensures the authenticity of the SVD it has created and exported

3.4.2 Platform assumptions

This assumption has been added to the [PP SSCD2] and [PP SSCD3]

A.No_Loading	It is assumed that there is no loading of applets after the TOE delivery at the end of phase 3.

A.Plt_Process	It is assumed that, after TOE delivery, Security Procedures are used by Card Manufacturer and Card Issuer (phase 4 to 6) during delivery and storage for protection of the TOE material/information. It is assumed that security procedures are used during all manufacturing and test operations through phase 4 to 6, to maintain confidentiality and integrity of the TOE and of its manufacturing and test data, to prevent any possible copy, modification, retention, theft or unauthorized used. It is assumed that appropriate functionality testing of the TOE is used in phases 4,5 and 6.

3.5 ORGANIZATIONAL SECURITY POLICIES

This section defines OSPs related to the Digital Signature application as stated in [PP SSCD2] and [PP SSCD2], and OSPs related to the Smart Card platform.

3.5.1 Digital Signature OSPs

P.CSP_Qcert	Qualified certificate. 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 [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.
P.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.
P.Sigy_SSCD	TOE as secure signature-creation device. The TOE stores the SCD used for signature creation under sole control of the signatory . The SCD used for signature generation can practically occur only once.

3.5.2 Platform OSPs

These OSPs has been added to the [PP SSCD2] [PP SSCD3].

P.Plt_Support	The platform is built with [JavaCard 2.1.1] and [GP 2.0.1] and allows the Digital Signature application to operate in a secure environment. The platform will support: - Secure Digital Signature application installation and extradition, - Secure deletion of Digital Signature instantiation. - Secure operating environment with detection of environmental trouble shooting - Secure execution environment and data sharing The Platform shall provide cryptographic services for the applet as RSA and DES
P.IC_Support	This IC is the Infineon SLE66CX642P, used by the platform shall be CC certified at a level comparable to the level of the current TOE evaluation: EAL4+ The IC shall support the security of the TOE operating environment and provide protection against - Physical manipulation of the IC - Physical Probing of the IC - Malfunction due to environment stress - Inherent or forced information leakage - Deficiency of Random Numbers

P.Applet_conformity	Other instanciable Applets, ROMed on the Platform but not part of the TOE shall comply with Java Card 2.1.1 and GP 2.0.1'. Appropriate instruction on the install of these applications shall be supplied with the TOE

4. TOE SECURITY OBJECTIVES

Parts directly copied from the [PP SSCD2]/ [PP SSCD3] are in black characters. Parts that have been added or modified are in blue characters.
(Option a) indicates that the security aspect element is specific to SSCD Type 2.
(Option b) indicates that the security aspect element is specific to SSCD Type 3.

4.1 SECURITY OBJECTIVES FOR THE TOE

4.1.1 Security objectives for the Digital Signature

OT.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.
OT.Lifecycle_Security (option a)	Lifecycle 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
OT.Lifecycle_Security (option b)	Lifecycle 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 re-generation (option b)
OT.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 . *Refinement:* The **TOE** shall ensure that the confidentiality of its temporally stored or persistently stored secrets is reasonably assured against attacks with a high attack level: • **D.VAD**: temporally stored data, used for signatory authentication. • **D.RAD**: persistently stored data, used for signatory authentication. • **D.SCD**: imported or generated and persistently stored data, used for signature generation.
OT.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.
OT.SVD_Auth_TOE	TOE ensures authenticity of SVD. The *TOE* provides means to enable the CGA to verify the authenticity SVD that has been exported by that TOE.
OT.Tamper_ID	Tamper detection. The TOE shall provide system features that detect physical tampering of a system component, and use those features to limit security breaches.

OT.Tamper_Resistance	Tamper resistance. The **TOE** shall prevent or resist physical tampering with specified system devices and components.
OT.SCD_Transfer (Option a)	Secure transfer of SCD between SSCD The TOE shall ensure the confidentiality of SCD transferred between SSCDs.
OT.Init (Option b)	Secure SCD SVD generation. The **TOE** provides security features to ensure that the generation of the SCD and the SVD is invoked by authorized users only.
OT.SCD_Unique (option b)	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.
OT.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.
OT.Sigy_SigF	Signature generation function for the legitimate signatory only. The TOE provides the signature generation function for the legitimate signatory only and protects SCD against the use of others. The TOE shall resist attacks with high attack potential.
OT.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.

4.1.2 Security objectives for the Platform

These security objectives have been added to the [PP SSCD2]/[PP SSCD3]

OT.Plt_Integrity	The platform shall ensure that sensitive data (assets) stored in its memory is protected against corruption or unauthorized modification. The platform shall provide means verify the integrity of its code
OT.Plt_Confidentiality	The platform shall ensure that sensitive information are protected against disclosure, when stored, transferred or used. The platform shall provide mechanisms to securely manage keys to avoid unauthorized access, disclosure or snooping
OT.Plt_Reallocation	The TOE shall ensure that the re-allocation of a memory block does not

	disclose sensitive information that was previously stored in that block.
OT.Plt_Install	The platform shall ensure that only authorized administrator is allowed to install /delete platform applets instantiation. The platform must ensure that initialization of applet is performed under secure conditions.
OT.Plt_Execution	The platform shall ensure that only authorized administrator is allowed to manage Card content through dedicated commands and after authentication
OT.Plt_Firewall	The platform shall ensure controlled sharing of data containers owned by applets, and between applets and the TSFs.
OT.Plt_Operate	The platform shall ensure correct operation of its security function and guaranty that the environment in which the application operates, is safe. The platform shall provide appropriate feedback information upon detection of potential violation.
OT.Plt_Support	The platform is built with [JavaCard 2.1.1] and [GP 2.0.1] and allows the Digital Signature application to operate in a secure environment. The platform will support: - Secure Digital Signature application installation and extradition, - Secure deletion of Digital Signature instantiation. - Secure operating environment with detection of environmental trouble shooting - Secure execution environment and data sharing The Platform shall provide cryptographic services for the applet as RSA and DES
OT.IC_Support	The IC, Infineon SLE66CX642P, used by TOE shall provide mechanisms to support the secure operation of the TOE. In particular: - Physical manipulation of the IC - Physical Probing of the IC - Malfunction due to environment stress - Inherent or forced information leakage - Deficiency of Random Numbers

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

4.2.1 Security Objectives for Digital Signature environment

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 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 shall 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: (a) 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, (b) sends the DTBS-representation to the TOE and shall enable verification of the integrity of the DTBS-representation by the TOE (c) attaches the signature produced by the TOE to the data or shall provide it separately.
OE.SCD_SVD_Corresp (option a)	Correspondence between SVD and SCD The SSCD Type1 shall ensure the correspondence between the SVD and the SCD. The SSVD Type1 shall verify the correspondence between the SCD sent to the TOE and the SVD sent to the CGA or TOE.
OE.SCD_Transfer (option a)	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 Type 2. The SCD shall be deleted from the SSCD Type1 whenever it is exported into the TOE.
OE.SCD_Unique (option a)	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.

4.2.2 Security objectives for the Platform environment

This security objective for the platform environment has been added to the [PP SSCD2]/[PP SSCD3]

OE.No_Loading	Loading of applet is not allowed after TOE delivery at the end of phase 3. Appropriate instruction shall be given in the Card manufacturer and administrator guidance to prohibit the loading of applets .

OE.Applet_conformity	Procedures shall ensure that for the other instanciable Applets ROMed on

	the Platform but not part of the TOE: - Appropriate conformity test to Java Card 2.1.1 and GP 2.0.1' have been performed. - Guidance for the generation of the TOE provides appropriate instruction on the install of these applications.

OE.Plt_Process	Procedures shall ensure the protection the material/information when TOE is delivered to Card Manufacturer and Card Issuer (phase 4 to 6), including the following objectives - Non-disclosure of any security relevant information, - Physical protection to prevent external damage, -Verification procedure to ensure the maintain of integrity and confidentiality of TOE sensitive data. Appropriate functionality testing of the TOE shall be used in phases 4,5 and 6.

5. IT SECURITY REQUIREMENTS

The TOE Security functional requirements define the functional requirements for the TOE using functional requirement components drawn from CCPART2 extended.
This section has been split in two sub-sections, one for the Digital Signature application for clear [PP SSCD2]/[PP SSCD3] conformance check, and one for the specific additional security requirements for the supporting platform.

Parts copied from the [PP SSCD2]/[PP SSCD3] are in black characters, with underline as when operation is performed in the PP.
Operation performed in the ST are in **bold blue** characters.
Iteration performed in the ST are in blue characters.

The minimum strength level for the TOE security functions is **SOF-high**.

5.1 DIGITAL SIGNATURE SECURITY FUNCTIONAL REQUIREMENTS

5.1.1 Digital signature security functional requirements list

Identification	Description
FCS	**Cryptographic support**
FCS_CKM.1 (option b)	Cryptographic key generation
FCS_CKM.4 (option a)	Cryptographic key destruction
FCS_CKM.4 (option b)	Cryptographic key destruction
FCS_COP.1/CORRESP	Cryptographic operation/Correspondence verification
FCS_COP.1/SIGNING	Cryptographic operation /Digital signature verification
FCS_COP.1/DES	Cryptographic operation/DES
FDP	**User data protection**
FDP_ACC.1 (option a) SVD Transfer SFP	Subset access control /SVD Transfer SFP
FDP_ACC.1 (option b) SVD Transfer SFP	Subset access control/ SVD Transfer SFP
FDP_ACC.1 (option a) SCD Import SFP	Subset access control/ SCD Import SFP
FDP_ACC.1 (option b) Initialization SFP	Subset access control/ Initialization SFP
FDP_ACC.1 Personalization SFP	Subset access control/ Personalization SFP
FDP_ACC.1 Signature-creation SFP	Subset access control/ Signature-creation SFP
FDP_ACF.1 (option b) Initialization SFP	Security attribute based access control/ Initialization SFP
FDP_ACF.1 (option a, b) SVD Transfer SFP	Security attribute based access control/ SVD Transfer SFP
FDP_ACF.1 (option a)	Security attribute based access control/ SCD Import SFP

SCD Import SFP	
FDP_ACF.1 Personalization SFP	Security attribute based access control/ Personalization SFP
FDP_ACF.1 Signature-creation SFP	Security attribute based access control/ Signature-creation SFP
FDP_ETC.1/SVD Transfer	Export of user data without security attributes/SVD Transfer
FDP_ITC.1 /SCD(option a)	Import of user data without security attributes/SCD
FDP_ITC.1 /DTBS	Import of user data without security attributes/DTBS
FDP_RIP.1	Subset residual information protection
FDP_SDI.2/persistent	Stored data integrity monitoring and action/persistent
FDP_SDI.2/DTBS	Stored data integrity monitoring and action/DTBS
FDP_UCT.1/Receiver (Option a)	Basic data exchange confidentiality
FDP_UIT.1/SVD Transfer	Data exchange integrity/ SVD Transfer
FDP_UIT.1/TOE DTBS	Data exchange integrity/TOE DTBS
FIA	**Identification and authentication**
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1 (option a)	Timing of authentication (option a)
FIA_UAU.1 (option b)	Timing of authentication (option b)
FIA_UID.1 (option a)	Timing of identification (option a)
FIA_UID.1 (option b)	Timing of identification (option b)
FMT	**Security management**
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1(option a) Administrator	Management of security attributes/ Administrator (option a)
FMT_MSA.1(option b) Administrator	Management of security attributes /Administrator (option b)
FMT_MSA.1/Signatory	Management of security attributes/Signatory
FMT_MSA.2	Secure security attributes
FMT_MSA.3 (option a)	Static attribute initialization (option a)
FMT_MSA.3 (option b)	Static attribute initialization (option b)
FMT_MTD.1	Management of TSF data
FMT_SMR.1	Security roles
FPT	**Protection of the TSF**
FPT_AMT.1	Abstract machine testing
FPT_EMSEC.1 (1)	TOE Emanation
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.1	Passive detection of physical attack
FPT_PHP.3	Resistance to physical attack
FPT_TST.1	TSF testing
FTP	**Trusted path/channels**
FTP_ITC.1(option a) SCD Import	Inter-TSF trusted channel / SCD Import (option a)
FTP_ITC.1(option a)	Inter-TSF trusted channel /SVD Transfer (option a)

SVD Transfer	
FTP_ITC.1(option b) SVD Transfer	Inter-TSF trusted channel /SVD Transfer (option b)
FTP_ITC.1/DTBS Import	Inter-TSF trusted channel /DTBS Import
FTP_TRP.1/TOE	Trusted path

Table 3 – Digital signature Security Functional Requirements list

(1) This requirement is CCPART2 extend.

5.1.2 FCS – Cryptographic support

Note: The minimum key size for Digital Signature is 1024 bit. The keys with a length smaller than 1024 are only used for other applications like authentication, enciphering and deciphering, etc. The maximum key size for the TOE is 2048 bit.

5.1.2.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 (option b)	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA with/without CRT key generation** and specified cryptographic key sizes **1024 to 2048 modulo 8 bytes** that meet the following: List of approved algorithms and parameters**.[JC2.1.1]**

5.1.2.2 FCS_CKM.4

FCS_CKM.4.1 (option a)	The TSF shall destroy cryptographic keys, in case of re-importation of the SCD in accordance with a specified cryptographic key destruction method **overwrite the key** that meets the following: **none.**

FCS_CKM.4.1 (option b)	The TSF shall destroy cryptographic keys, in case of regeneration in accordance with a specified cryptographic key destruction method **overwrite the key** that meets the following: **none**

5.1.2.3 FCS_COP.1

FCS_COP.1.1/ CORRESP	The TSF shall perform SCD/SVD correspondence verification in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **between 1024 and 2048 bit** that meet the following: List of approved algorithms and parameters. **[JC2.1.1].**
FCS_COP.1.1/	The TSF shall perform digital signature generation in accordance with

SIGNING	a specified cryptographic algorithm **RSA** and cryptographic key sizes **between 1024 and 2048 bit** that meet the following: List of approved algorithms and parameters **[JC2.1.1].**
FCS_COP.1.1/ DES	- The TSF shall perform **the following operations MAC computation for Signature CBC mode, Decryption, Encryption, session key computation in CBC mode** in accordance with a specified cryptographic algorithm **3DES** and cryptographic key sizes **16 bytes** that meet the following: **[ANSI 2]**

5.1.3 FDP – User data protection

5.1.3.1 FDP_ACC.1

FDP_ACC.1.1/ SVD Transfer SFP (option a)	The TSF shall enforce the SVD Transfer SFP on import and on export of SVD by User

FDP_ACC.1.1/ SVD Transfer SFP (option b)	The TSF shall enforce the SVD Transfer SFP on export of SVD by User

FDP_ACC.1.1/ SCD Import SFP (option a)	The TSF shall enforce the SCD Import SFP on import of SCD by User

FDP_ACC.1.1/ Initialization SFP (option b)	The TSF shall enforce the Initialization SFP on Generation of SCD/ SVD pair by User

FDP_ACC.1.1/ Personalization SFP	The TSF shall enforce the Personalization SFP on Creation of RAD by Administrator

FDP_ACC.1.1/ Signature-creation SFP	The TSF shall enforce the Signature-creation SFP on: 1. Sending of DTBS-representation by the SCA 2. Signing of DTBS-representation by S.Signatory

5.1.3.2 FDP_ACF.1

The security attributes for the subjects, Digital Signature components and related status are:

User, subject or object the attribute is associated with	Attribute	Status
General attribute		
User	Role	Administrator, Signatory
Initialization attribute group		
User	SCD / SVD management	Authorized, not authorized
SCD (option a)	Secure SCD import allowed	No, Yes
Signature-creation attribute group		
SCD	SCD operational	No, yes
DTBS	Sent by an authorized SCA	No, yes

Initialization SFP (option b)

FDP_ACF.1.1 / Initialization SFP (Option b)	The TSF shall enforce the initialization SFP to objects based on General attribute and Initialization attribute**.**
FDP_ACF.1.2 / Initialization SFP (Option b)	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. **Refinement:** **The user with the security attribute "role" set to "Administrator" and with the security attribute "SCD/SVD management" set to "authorized" is allowed to generate SCD/ SVD pair.** **Or** **The user with the security attribute "role" set to "Administrator" and user with the security attribute "role" set to Signatory and with the security attribute "SCD/SVD management" set to "authorized" is allowed to generate SCD/ SVD pair.**
FDP_ACF.1.3/ Initialization SFP (Option b)	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ Initialization SFP (Option b)	The TSF shall explicitly deny access of subjects to objects based on the rule: 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. **Refinement:** **The user with the security attribute "role" set to "Administrator" and with the security attribute "SCD/SVD management" set to "not authorized" is not allowed to generate D.SCD/D.SVD pair.** **Or**

	The user with the security attribute "role" set to "Administrator" and the User with the security attribute "role" set to "Signatory" and with the security attribute "SCD/SVD management" set to "not authorized" is not allowed to generate SCD/ SVD pair.

SVD Transfer SFP

FDP_ACF.1.1 / SVD Transfer SFP	The TSF shall enforce the SVD Transfer SFP to objects based on General attribute**.**
FDP_ACF.1.2 / SVD Transfer SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The user with security attribute "role" set to "Administrator" or to "Signatory" is allowed to export SVD.
FDP_ACF.1.3/ SVD Transfer SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none**.**
FDP_ACF.1.4/ SVD Transfer SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: none**.**

SCD Import SFP (Option a)

FDP_ACF.1.1 / SCD IMPORT SFP (Option a)	The TSF shall enforce the SCD import SFP to objects based on General attribute and Initialization attribute group**.**
FDP_ACF.1.2 / SCD IMPORT SFP (Option a)	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". **Refinement:** **The User with the security attribute "role" set to "Administrator" and with the security attribute "SCD/SVD management" set to "authorized" is allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes".** **Or** **The user with the security attribute "role" set to "Administrator" and the User with the security attribute "role" set to "Signatory" and with the security attribute "SCD/SVD management" set to "authorized" is allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes".**
FDP_ACF.1.3/ SCD IMPORT SFP (Option a)	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none

FDP_ACF.1.4/ SCD IMPORT SFP (Option a)	The TSF shall explicitly deny access of subjects to objects based on the rule: (a) The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "not authorized" is not allowed to import D.SCD if the security attribute "secure SCD import allowed" is set to "yes". (b) The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "authorized" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "no".

Personalization SFP

FDP_ACF.1.1 / Personalization SFP	The TSF shall enforce the Personalization SFP to objects based on 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: The 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 authorize 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 rule: none.

Signature-creation SFP

FDP_ACF.1.1 / Signature-creation SFP	The TSF shall enforce the Signature-creation SFP to objects based on 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 authorized 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 authorize 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 rule: (a) User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS which is not sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes". (b) User with the security attribute "role" set to "Signatory" is not

	allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "no".

5.1.3.3 FDP_ETC.1

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

5.1.3.4 FDP_ITC.1

FDP_ITC.1.1/ SCD (Option a)	The TSF shall enforce the SCD Import SFP when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.1.2/SCD (Option a)	The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3/SCD (Option a)	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: SCD shall be sent by an authorized SSCD.

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 TSC.
FDP_ITC.1.2/DTBS	The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3/DTBS	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: DTBS-representation shall be sent by an authorized SCA.

5.1.3.5 FDP_RIP.1

FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of resource from the following objects: SCD,VAD,RAD **Refinement** : De-allocation of resources on SCD, VAD and RAD is managed by the Platform

5.1.3.6 FDP_SDI.2

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

1. D.SCD
2. D.RAD
3. D.SVD (if persistent stored by TOE)

FDP_SDI.2.1/ Persistent	The TSF shall monitor user data stored within the TSC for integrity errors 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: 1. Prohibit the use of the altered data 2. Inform the S.Signatory about integrity error. **Refinement** : Integrity errors on SCD, VAD and RAD is managed by the Platform.

The DTBS-representation temporarily stored by TOE have the user data attribute “integrity checked stored data”:

FDP_SDI.2.1/DTBS	The TSF shall monitor user data stored within the TSC for integrity errors 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: 1. Prohibit the use of the altered data 2. Inform the S.Signatory about integrity error.

5.1.3.7 FDP_UCT.1

FDP_UCT.1.1 / Receiver (Option a)	The TSF shall enforce the SCD Import SFP to be able to receive SCD objects in a manner protected from unauthorized disclosure.

5.1.3.8 FDP_UIT.1

FDP_UIT.1.1/ SVD Transfer	The TSF shall enforce the SVD Transfer SFP to be able to transmit user data SVD 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.1.1/ TOE DTBS	The TSF shall enforce the Signature creation SFP to be able to receive user data DTBS-representation 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.

5.1.4 FIA – Identification and Authentication

5.1.4.1 FIA_AFL.1

FIA_AFL.1.1	The TSF shall detect when **Predefined number** unsuccessful authentication attempts occur related to consecutive failed authentication attempts **using RAD**. **Refinement:** **The predefined number of unsuccessful authentication is initially**

	defined by the applet when the D.RAD object is created. This predefined number must be set between [3] and [15];
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall block RAD**.**

5.1.4.2 FIA_ATD.1

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

5.1.4.3 FIA_UAU.1

FIA_UAU.1.1 (option a)	The TSF shall allow] 1. Identification of the user by means of TSF required FIA_UID.1 2. Establishing a trusted channel between the TOE and a SSCD by means of TSF required by FTP_ITC.1/SCD import (option a) 3. Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE 4. 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 (option a)	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1.1 (option b)	The TSF shall allow[1. Identification of the user by means of TSF required FIA_UID.1 2. Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE 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 authenticated.
FIA_UAU.1.2 (option b)	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.4.4 FIA_UID.1

FIA_UID.1.1 (Option a)	The TSF shall allow[1. Establishing a trusted channel between the TOE and a SSCD by means of TSF required by FTP_ITC.1/SCD import 2. Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE

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

FIA_UID.1.1 (Option b)	The TSF shall allow[1. Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE. 2. 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 (Option b)	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.5 FMT – Security management

5.1.5.1 FMT_MOF.1

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

5.1.5.2 FMT_MSA.1

FMT_MSA.1.1 / Administrator (Option a)	The TSF shall enforce the SCD Import SFP to restrict the ability to modify **[no other operation]** the security attributes SCD/SVD management and secure SCD import allowed to Administrator . **Refinement:** This occurs during phase 6

FMT_MSA.1.1 / Administrator (Option b)	The TSF shall enforce the Initialization SFP to restrict the ability to modify **[no other operation]** the security attributes SCD/SVD management to Administrator . **Refinement:** This occurs during phase 5b

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.

5.1.5.3 FMT_MSA.2

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

5.1.5.4 FMT_MSA.3

FMT_MSA.3.1 (Option a)	The TSF shall enforce the SCD Import 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 operational" is set to "no" after import of SCD
FMT_MSA.3.2 (Option a)	The TSF shall allow the Administrator to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3.1 (Option b)	The TSF shall enforce 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 operational" is set to "no" after import of SCD
FMT_MSA.3.2 (Option b)	The TSF shall allow the Administrator to specify alternative initial values to override the default values when an object or information is created.

5.1.5.5 FMT_MTD.1

FMT_MTD.1.1/	The TSF shall restrict the ability to modify **[no other operation]** the RAD to Signatory.

5.1.5.6 FMT_SMR.1

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.

5.1.6 FPT – Protection of the TSF

5.1.6.1 FPT_AMT.1

FPT_AMT.1.1	The TSF shall run a suite of tests **during initial start-up, periodically during normal operation** to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.1.6.2 FPT_EMSEC.1.1

FPT_EMSEC.1.1	The TOE shall not emit **electromagnetic radiation** in excess of **unintelligible emission** enabling access to RAD and SCD.

5.1.6.3 FPT_EMSEC.1.2

FPT_EMSEC.1.2	The TOE shall ensure **attacker S.OFFCARD** are unable to use the following interface **I/O, VCC, Ground** to gain access to RAD and SCD

5.1.6.4 FPT_FLS.1

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: • **Unexpected abortion of the execution of the TSF due to external events** • **Unexpected errors during execution of the TSF**

5.1.6.5 FPT_PHP.1

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.

5.1.6.6 FPT_PHP.3

FPT_PHP.3.1	The TSF shall resist the **following physical tampering scenarios** to the **following TSF devices/elements** by responding automatically such that the TSP is not violated. **Devices/Elements** / **Physical tampering scenarios** **Active shield** / **Attack over the surface** **Clock** / **Reduction/increase of frequency** **Voltage supply** / **Voltage out of range**

5.1.6.7 FPT_TST.1

FPT_TST.1.1	The TSF shall run a suite of self-tests at **the following period** and **conditions** to demonstrate the correct operation of the TSF. **Period** / **Self-test/Condition** **startup** / **Integrity verification of the TSF Filter table at startup** **startup** / **Test of random numbers at the request of the operating system** **startup** / **Card Life Cycle state consistency**
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code. **Refinement :** executable code consist of the ROM code, the EEPROM patches and filter area integrity

5.1.7 FTP – Trusted path/channels

5.1.7.1 FTP_ITC.1

FTP_ITC.1.1 / SCD IMPORT (Option a)	The TSF shall provide a communication channel between itself and a remote 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 (Option a)	The TSF shall permit **the remote trusted IT product SSCD** to initiate communication via the trusted channel.
FTP_ITC.1.3 / SCD IMPORT (Option a)	The TSF or the remote trusted IT shall initiate communication via the trusted channel for SCD Import**.**

Refinement: The mentioned remote trusted IT product is a SSCD of type 1 (option a)

FTP_ITC.1.1 / SVD Transfer Option a)	The TSF shall provide a communication channel between itself and a remote 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 Transfer Option a)	The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.
FTP_ITC.1.3 / SVD Transfer Option a)	The TSF or the remote trusted IT product shall initiate communication via the trusted channel for transfer of SVD

Refinement: The mentioned remote trusted IT product is a SSCD of type 1 for SVD import and the CGA for the SVD export (option a)

FTP_ITC.1.1 / SVD Transfer (Option b)	The TSF shall provide a communication channel between itself and a remote trusted IT product **CGA** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2 / SVD Transfer (Option b)	The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.
FTP_ITC.1.3 / SVD Transfer (Option b)	The TSF **or the CGA** shall initiate communication via the trusted channel for export SVD

FTP_ITC.1.1 / DTBS Import	The TSF shall provide a communication channel between itself and a remote 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	The TSF shall permit **SCA** to initiate communication via the trusted

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

5.1.7.2 FTP_TRP.1

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 or 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.**

5.2 PLATFORM SECURITY FUNCTIONAL REQUIREMENTS

5.2.1 Platform security functional requirements list

All following SFRS have been added to [PP SSCD2]/[PP SSCD3]

Identification	Description
FAU	Security audit
FAU_ARP.1	Security alarms
FAU_SAA.1	Potential violation analysis
FCS	Cryptographic support
FCS_CKM.1	Cryptographic key generation
FCS_CKM.3	Cryptographic key access
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operations
FDP	**User data protection**
FDP_ACC.1	Subset Access control
FDP_ACF.1	Security attributes based access control
FDP_RIP.1	Subset residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
FDP_UCT.1	Basic data exchange confidentiality
FIA	**Identification and Authentication**
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding
FMT	**Security management**
FMT_MOF.1	Management of security function behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes

FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Function
FMT_SMR.1	Security roles
FPT	**Protection of the TOE Security function**
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.1	Passive detection of physical attack
FPT_PHP.3	Resistance to physical attack
FPT_RVM.1	Non bypassability of the TSP
FPT_SEP.1	TSF Domain separation
FPT_TDC.1	Inter TSF Basic TSF Data consistency
FPT_TST.1	TSF testing
FTP	**Trusted path/Channel**
FTP_TRP.1	Trusted Path

Table 4 – Platform security functional requirements list

5.2.2 FAU Security audits

5.2.2.1 FAU_ARP.1 Security alarms

FAU_ARP.1.1	The TSF shall take **one of the following disruptive actions** upon detection of a potential security violation. **List of disruptive actions:** **1. Reset the card and clear all volatile memory.** **2. Block the action that produced the security violation and throw an exception.** **3. Terminate the card (after this action, the card will stays mute forever).** **4. Mute the card.**

5.2.2.2 FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1	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 TSP.
FAU_SAA.1.2	The TSF shall enforce the following rules for monitoring audited events: a) Accumulation or combination of **the following auditable events** known to indicate a potential security violation: **1. Card Manager life cycle state inconsistency (D.ISD_DATA)** **2. Integrity errors on D.GP_KEYS, D.ISD_KEYS and D.SD_KEYS, D.USER_PIN.** **3. Illegal Access to Java object** **4. Unavailability of resources audited through the object allocation mechanism** b) Any other rules: **none.**

5.2.3 FCS – Cryptographic support

5.2.3.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1/ RSA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **(RSA) for the generation of public keys** and specified cryptographic key sizes **of 512 to 2048 bits** that meet the following standards: **1. JavaCard API 2.1.1**
FCS_CKM.1.1/ DES	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **DES or 3-DES for the generation of session keys** and specified cryptographic key sizes **of single (64 bits) and double (128 bits) or triple length (192 bits)** that meet the following standards: **1. [VOP] sections 5, 6 and 7.**

5.2.3.2 FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1	The TSF shall perform **the cryptographic keys decryption** in accordance with a specified cryptographic key access method **(OP/VOP command and OP/VOP Java API)** that meets the following standards: **1. [OP] sections 8 and 9.9.** **2. [VOP] section 9.3.** **3. JavaCard API 2.1.1**

5.2.3.3 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 unavailable** that meets the following: **none**

5.1.3.2 FCS_COP.1 Cryptographic operations

FCS_COP.1.1/ RSA	The TSF shall perform **the encryption and decryption operations** in accordance with a specified cryptographic algorithm **RSA (RSA)** and cryptographic key sizes **of 512 to 2048 bits** that meet the following standards: **Java Card API 2.1.1**
FCS_COP.1.1/ DES	The TSF shall perform **encryption and decryption operations** in accordance with a specified cryptographic algorithm **Data Encryption Standards (DES)** and cryptographic key sizes **of 64 bits (DES) and 128 bits, 192 bits (Triple-DES)** that meet the following standards: **Java Card API 2.1.1**

5.2.4 FDP – User data protection

5.2.4.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1/ Platform Initialization	The TSF shall enforce the **Platform Initialization SFP** on **the following list** of subjects, objects and operations	
Subjects	**Objects**	**Operations**
S.Card_Manufacturer	D.GP_KEYS D.GP_REGISTRY D.ISD_DATA D.ISD_KEYS	Make unavailable Create, Change [Card Life Status], Create Load

FDP_ACC.1.1/ Card Manager	The TSF shall enforce the **Card Manager SFP** on following list of subjects objects and operations.	
Subjects	**Objects**	**Operations**
S.Card_Manager	D.GP_REGISTRY D.SD_DATA D.SD_KEYS D.ISD_DATA	Update [SD AID] (install, delete) Change [Application Life Cycle] Create, Extradite Create, Lock Installation Lock Application Load

FDP_ACC.1.1/ Firewall	The TSF shall enforce the **Firewall SFP** on Access to D.JAVA_OBJECT and objects by S.APPLET	
Subjects	**Objects**	**Operations**
S.Applet	D.JAVA_OBJECT including D.USER_PIN	Use, Update, Delete

5.2.4.2 FDP_ACF.1 Security attributes based access control

The security attributes for the platform.

The attributes used in this section are the following:

Subject/object	Attribute	Values
S.Card_Manufacturer	Authentication[Card Manufacturer]	Yes, No
S.Card_Manager	Authentication[Card Manager]	Yes, No
S.Card_Manufacturer S.Card_Manager	Secure Channel	Open, Not Open
S.Applet	Security Context	Java Object, Current
D.ISD_DATA	Card Life Status	OP_READY, INITIALIZED,

		SECURED, CARD_BLOCKED, TERMINATED
D.ISD_DATA	Available Command	Yes, No
D.SD_DATA	Applet Life Status	INSTALL, SELETABLE, PERSONNALIZED, LOCKED, LOGICALLY-DELETED
D.JAVA_OBJECT	Security Context	Java Object, Current

FDP_ACF.1.1/ Platform Initialization	The TSF shall enforce the **Platform Initialization SFP** to objects based on **following attributes**
FDP_ACF.1.2/ Platform Initialization	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
Attributes	**Rules**
Authentication [Card Manufacturer]	- Creation of **D.ISD_DATA** is allowed if Card Manufacturer has been correctly identified and **Authentication** status is set to Yes. - Load of **D.ISD_KEY** is allowed if Card Manufacturer has been correctly identified and **Authentication** status is set to Yes, - Only Card Manufacturer with **Authentication** status set to Yes is allowed to create the **D.GP_REGISTRY** and to modify the **D.GP_REGISTRY [Card Life Status]** to OP_READY state in phase 5b - Only Card Manufacturer with Authentication status set to Yes is allowed to make **D.GP_KEYS** unavailable

FDP_ACF.1.3/ Platform Initialization	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none.**
FDP_ACF.1.4/ Platform Initialization	The TSF shall explicitly deny access of subjects to objects based on the rule: **none.**

FDP_ACF.1.1/ Card Manager	The TSF shall enforce the **Card Manager SFP** to objects based on **following attributes**
FDP_ACF.1.2/ Card Manager	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
Attributes	**Rules**
	- The **Secure Channel** is set to Open only if Card Manager has

Authentication [Card Manager] Secure Channel Card Life Status Available command	been correctly authenticated and **Authentication[Card Manager]** set to Yes - Operations on applications are allowed only if **Card life Status** is set to OP_READY, INITIALIZED or SECURED and if Card Manager has been correctly authenticated with **Authentication[Card Manager]** set to Yes - Only Card Manager correctly authenticated with **Authentication[Card Manager]** set to Yes is allowed to Update **D.GP_REGISTRY [SD AID]** during Applet Install/Delete - Only Card Manager correctly authenticated with **Authentication[Card Manager]** set to Yes is allowed to create **D.SD_DATA** - Only Card Manager correctly authenticated with **Authentication [Card Manager]** set to Yes is allowed to create **D.SD_KEY** - Only Card Manager correctly authenticated with **Authentication[Card Manager]** set to Yes is allowed to modify **D.SD_DATA** for extradition operation. - Only Card Manager correctly authenticated with **Authentication[Card Manager]** set to Yes is allowed to set the GP_REGISTRY [Applet Life Status] to INSTALL . - -Only Card Manager correctly authenticated with **Authentication[Card Manager]** set to Yes is allowed to modify D.ISD_DATA[Available Command] to Lock application installation - - Only Card Manager correctly authenticated with **Authentication[Card Manager]** set to Yes is allowed to modify D.ISD_DATA[Available Command] to Lock the Load of application during phase 5.

FDP_ACF.1.3/ Card Manager	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none.**
FDP_ACF.1.4/ Card Manager	The TSF shall explicitly deny access of subjects to objects based on the rule: **none.**

FDP_ACF.1.1/ Firewall	The TSF shall enforce the **Firewall SFP** to objects based on **following attributes**
FDP_ACF.1.2/ Firewall	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed
Attributes	**Rules**
Security Context[Java Object], Security Context [Current]	Access to **D. JAVA_OBJECT** by an **S.Applet** shall be allowed only if the **Security context [Java Object]** meets the **Security context**

	[Current] of the selected Java object _, as per the rules defined in the JavaCard 2.1.1 [JCRE], section 6.
FDP_ACF.1.3/ Firewall	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none.**
FDP_ACF.1.4/ Firewall	The TSF shall explicitly deny access of subjects to objects based on the rule: **none.**

5.2.4.3 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 resource** for the following objects: • D.GP_KEYS • D.ISD_KEYS • D.SD_KEYS • D.USER_PIN

5.2.4.4 FDP_SDI.2 Stored data integrity monitoring and action

The following data persistently stored by TOE have the user attribute “integrity checked persistent stored data”:

- Keys : GP_KEYS, ISD.KEYS, SD.KEYS, D.USER_PIN
- Card Life Cycle state : D.GP_REGISTRY [Card Life Status], Applet Life Status].

FDP_SDI.2.1/ KEYS	The TSF shall monitor user data stored within the TSC for **integrity errors** on all objects, based on the following attributes: **integrity checked persistent stored data.**
FDP_SDI.2.2/ KEYS	Upon detection of a data integrity error, the TSF shall: • **Prohibit the use of the altered data** • **Inform the S.Card_Manufacturer/S.Card_Manager about integrity error.** • **Mute the card**

FDP_SDI.2.1/ Card_life_cycle	The TSF shall monitor user data stored within the TSC for **integrity errors** on all objects, based on the following attributes: **integrity checked persistent stored data.**
FDP_SDI.2.2/ Card_life_cycle	Upon detection of a data integrity error, the TSF shall: • **Prohibit the use of the altered data** • **Inform the S.Card_Manufacturer/S.Card_Manager about integrity error.** • **Terminate the card**

5.2.4.5 FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1	The TSF shall enforce the **Card Manager SFP,** to be able to **transmit and receive** objects in a manner protected from unauthorized disclosure.

5.2.5 FIA – Identification and Authentication

5.2.5.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1	The TSF shall detect when **Predefined number** unsuccessful authentication attempts occur related to any **administrator authentication**
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **block the card**

5.2.5.2 FIA_ATD.1 User attribute definition

FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: **- Authentication[Card Manufacturer]** **- Authentication[Card Manager]** **- Security Context[Java Object, Current]**

5.2.5.3 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1	The TSF shall allow **the following TSF mediated actions** on behalf of the user to be performed before the user is authenticated. **S.Applet** — **Get Challenge**, **Get Data**, **Select Application.** **S.Card_Manager** — **Get Data**, **Select**, **Initialize Update**
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.

5.2.5.4 FIA_UID.1 Timing of identification

FIA_UID.1.1	The TSF shall allow the **selection of a S.APPLET** on behalf of the user to be performed before 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 **.**

5.2.5.5 FIA_USB.1 User-subject binding

FIA_USB.1.1	The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

5.2.6 FMT – Security Management

5.2.6.1 FMT_MOF.1 Management of security function behavior

FMT_MOF.1.1	The TSF shall restrict the ability to **modify the behavior of** the functions **listed below** to **the S.Card _Manager** - Load application - Install application - Update D.ISD.KEY

5.2.6.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1	The TSF shall enforce the **Platform Initialization SFP, the Card Manager SFP,** to restrict the ability to **perform the following operations on** the security attributes **defined below** to **the *Card Manufacturer,* the *Card manager.***

Object	**Security attribute**	**Operation**	**SFP**	**Role**
			See FDP_ACC.2 And FDP_ACF.1	**See FMT_SMR.1**
D.GP_REGISTRY	**ISD[AID]** **Card Life Status**	**Create** **Modify**	**Platform Initialization** **Card Manager**	**Card Manufacturer phase 5** **Card Manager phase 6**
D.ISD_DATA	**Key Information** **Available Command** **Retry Counter**	**Create** **Modify** **Modify**	**Card Manager**	**Card Manager (phase 6)**
D.GP_REGISTRY	**Application Life Cycle** **SD[AID]**	**Modify** **Create**	**Card Manager**	**Card Manager phase 6**
D.SD_DATA	**Key information**	**Create/ Modify**	**Card Manager**	**Card Manager phase 6**

5.2.6.3 FMT_MSA.2 Secure security attributes

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

5.2.6.4 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1	The TSF shall enforce the **Platform Initialization SFP, Card Manager,** to provide **restrictive** default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow **none** to specify alternative initial values to override the default values when an object or information is created.

5.2.6.5 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1	The TSF shall restrict the ability to **access or modify** the **following TSF data** to **the *Card Manager* role.** **D.ISD_KEY.**

5.2.6.6 FMT_SMF.1 Specification of Management function

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: - **Load application** - **Install application** - **Update D.ISD.KEY** - **Create / Modify D.GP_REGISTRY** - **Create/Modify D.ISD_DATA** - **Create/Modify D.SD_DATA**

5.2.6.7 FMT_SMR.1 Security roles

FMT_SMR.1.1	The TSF shall maintain the roles **defined in the following list.** **The roles list:** **1. The *Card manufacturer* role (phase 5a).** The *Card manufacturer* is in charge of initializing the secrets related to the JCP ES, and to set the Card Manager state to OP_READY, then INITIALIZED. **2. The Card Manager role (phase 5b, 6)** The *Card Manager is the personalizer of the Card and the Card Issuer as there is no post issuance loading of application.* *He is* in charge of Application INSTALL operation and of sets the application to INSTALL and SELECTABLE, then set the platform state to SECURED. The *Card Manager* is in charge of deleting an Application if it doesn't share any object

	3.The *Application User* role (phase 6 to 7). After application installation, the platform only sees application users and users . The access to platform resources is granted according to Java Object access conditions defined in Security context
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

5.2.7 FPT – Protection of the TSF

5.2.7.1 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1/Platform	The TSF shall preserve a secure state when the following types of failures occur: - **Unexpected abortion of the execution of the TSF due to external events.**

5.2.7.2 FPT_PHP.1 Passive detection of physical attacks

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.

5.2.7.3 FPT_PHP.3 Resistance to physical attacks

FPT_PHP.3.1	The TSF shall resist the **following physical tampering scenarios** to the **following TSF devices/elements** by responding automatically such that the TSP is not violated.

Devices/Elements	**Physical tampering scenarios**
Active shield	Attack over the surface
Clock	Reduction/increase of frequency
Voltage supply	Voltage out of range

5.2.7.4 FPT_RVM.1 Non-Bypassability of the TSP

FPT_RVM.1.1	The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2.7.5 FPT_SEP.1 TSF Domain separation

FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.

5.2.7.6 FPT_TDC.1 Inter-TSF data consistency

FPT_TDC.1.1	The TSF shall provide the capability to consistently interpret **data types (defined in [VOP]) and S.APPLET code** when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use **the following interpretation rules** when interpreting the TSF data from another trusted IT product. **Interpretation rules list:** **1. The ISO 7816-6 rules [ISO7816].** **2. The [JCVM].**

5.2.7.7 FPT_TST TSF testing

FPT_TST.1.1	The TSF shall run a suite of self-tests at **the following period** and **conditions** to demonstrate the correct operation of the TSF. **Period** / **Self-test/Condition** startup — Integrity verification of the TSF Filter table at startup startup — Test of random numbers at the request of the operating system startup — Card Life Cycle state consistency
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code. Refinement : executable code consist of the ROM code, the EEPROM patches and filter area integrity

5.2.8 FTP – Trusted path/channels

5.2.8.1 FTP_TRP.1 Trusted channel

FTP_TRP.1.1	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 or disclosure.
FTP_TRP.1.2	The TSF shall permit **local users** to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for **D. ISD_KEYS load** and application **Install, Extradite** operations .

5.3 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE security assurance requirements define the assurance requirements for the TOE using only assurance components drawn from [CCPART3].

The assurance level is **EAL4** augmented on:

- **AVA_MSU.3 (Misuse - Analysis and testing for insecure states)**
- **AVA_VLA.4 (Vulnerability Analysis - Highly resistant).**
- **ADV_IMP.2 (Implementation of the TSF)**

5.3.1 TOE security assurance requirements list

All requirements below are those from [PP SSCD2]/[PP SSCD3] except ADV_IMP.1 augmented to ADV_IMP.2.
ADV_IMP.2 Implementation of the TSF is from **CCPART3.**

Identification	Description
ACM	**Configuration management**
ACM_AUT.1	Partial CM automation
ACM_CAP.4	Generation support and acceptance procedures
ACM_SCP.2	Problem tracking CM coverage
ADO	**Delivery and Operation**
ADO_DEL.2	Detection of modification
ADO_IGS.1	Installation, generation and start-up procedures
ADV	**Development**
ADV_FSP.2	Fully defined external interfaces
ADV_HLD.2	Security enforcing high-level design
ADV_IMP.2	Implementation of the TSF
ADV_LLD.1	Descriptive low-level design
ADV_RCR.1	Informal correspondence demonstration
ADV_SPM.1	Informal TOE security policy model
AGD	**Guidance documents**
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC	**Life cycle support**
ALC_DVS.1	Identification of security measures
ALC_LCD.1	Developer defined life-cycle model

ALC_TAT.1	Well-defined development tools
ATE	**Tests**
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: high –level design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA	**Vulnerability assessment**
AVA_MSU.3	Analysis and testing for insecure states
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.4	Highly resistant

Table 5 – TOE security assurance requirements list

5.3.2 Refinements on TOE Assurance Requirement

The ADO_IGS component has been refined as indicated below

ADO_IGS.2.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.2.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

ADO_IGS.2.2C The installation, generation and start-up documentation shall describe procedures capable of creating a log containing the generation options used to generate the TOE in such a way that it is possible to determine exactly how and when the TOE was generated.

ADO_IGS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.2.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

Refinement:
The installation generation and start-up documentation addresses also the Java Card platform ROMed applet installation together with the TOE installation.
Developer shall provide assurance that ROMed applets installed on the platform are Java Card and GP compliant and have been tested according to their specification.
Evaluator shall confirm that such assurance is supplied.

5.4 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT

The following section is copied from the [PP SSCD2]/[PP SSCD3]

5.4.1 Signature Key generation (SSCD Type 1)

This applies only to SSCD type 2 (Option a)

5.4.1.1 FCS_CKM.1.1

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA with/without CRT key generation** and specified cryptographic key sizes **1024 to 2048 modulo 8 bytes** that meet the following: List of approved algorithms and parameters: **[JC2.1.1]**

5.4.1.2 FCS_CKM.4.1/Type 1

FCS_CKM.4.1/Type1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwrite the key** that meets the following: **none.**

5.4.1.3 FCS_COP.1.1

FCS_COP.1.1/CORRESP	The TSF shall perform SCD / SVD correspondence verification in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes between 1024 and 2048 bit that meet the following: List of approved algorithms and parameters: [JC2.1.1].

5.4.1.4 FDP_ACC.1.1/SCD Export SFP

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

5.4.1.5 FDP_UCT.1.1/Sender

FDP_UCT.1.1/Sender	The TSF shall enforce the SCD Export SFP to be able to transmit objects in a manner protected from unauthorized disclosure.

5.4.1.6 FTP_ITC.1 SCD/Export

FTP_ITC.1.1/SCD Export	The TSF shall provide a communication channel between itself and a remote 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	The TSF shall permit **the TSF**] to initiate communication via the trusted channel.
FTP_ITC.1.3/SCD Export	The TSF or the SSCD Type 2 shall initiate communication via the trusted channel for SCD export.

Refinement : The mentioned remote trusted IT product is a SSCD Type 2

5.4.2 Certification Generation application (CGA)

5.4.2.1 FCS_CKM.2

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: List of approved algorithms and parameters: [E-Sign1]

5.4.2.2 FCS_CKM.3

FCS_CKM.3.1 /CGA	The TSF shall perform import the SVD in accordance with a specified cryptographic key access method import through a secure channel that meets the following: List of Standards [E-Sign1]

5.4.2.3 FDP_UIT.1

FDP_UIT.1.1 / SVD Import	The TSF shall enforce the SVD Import SFP to be able 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.

5.4.2.4 FTP_ITC.1

FTP_ITC.1.1 / SVD Import	The TSF shall provide a communication channel between itself and a remote 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	The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.
FTP_ITC.1.3 / SVD Import (option a)	The TSF or the remote trusted IT product shall initiate communication via the trusted channel for Import SVD
FTP_ITC.1.3 / SVD Import (Option b)	The TSF **or the TOE** shall initiate communication via the trusted channel for Import SVD

5.4.3 Signature creation application (SCA)

5.4.3.1 FCS_COP.1

FCS_COP.1.1 / SCA Hash	The TSF shall perform hashing the DTBS in accordance with a specified cryptographic algorithm SHA-1 and cryptographic key sizes none that meet the following: List of approved algorithms and parameters SHA-1

5.4.3.2 FDP_UIT.1

FDP_UIT.1.1 /	The TSF shall enforce the Signature-creation SFP to be able to

SCA DTBS	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.

5.4.3.3 FTP_ITC.1

FTP_ITC.1.1 / SCA DTBS	The TSF shall provide a communication channel between itself and a remote 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 (option a)	The TSF or the remote trusted product shall initiate communication via the trusted channel for sending D.DTBS-representation by means of the SSCD**.**
FTP_ITC.1.3 / SCA DTBS (option b)	The TSF **or the TOE** shall initiate communication via the trusted channel for sending D.DTBS-representation by means of the SSCD**.**

5.4.3.4 FTP_TRP.1

FTP_TRP.1.1 / SCA (option a)	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 or disclosure.
FTP_TRP.1.2 / SCA option a	The TSF shall permit **the TSF** to initiate communication via the trusted path.
FTP_TRP.1.3 / SCA (option a)	The TSF shall require the use of the trusted path for **initial user authentication.**

FTP_TRP.1.1 / SCA (option b)	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 or disclosure.
FTP_TRP.1.2 / SCA (option b)	The TSF shall permit **the TSF or local users** to initiate communication via the trusted path.
FTP_TRP.1.3 / SCA (option b)	The TSF shall require the use of the trusted path for **initial user authentication.**

5.5 SECURITY REQUIREMENTS FOR THE NON-IT ENVIRONMENT

R.Administrator_Guide *Application of Administrator Guidance*

The implementation of the requirements of the Directive, 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 ensure the ongoing compliance.

R.Sigy_Guide *Application of User Guidance*

The SCP implementation of the requirements of the Directive, 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 [1], ANNEX II "Requirements for certification-service-providers issuing qualified certificates", literal (d). The CSP shall verify that this person holds the SSCD which implements the SCD corresponding to the SVD to be included in the qualified certificate.

6. TOE SUMMARY SPECIFICATION

6.1 TOE SECURITY FUNCTIONS

This part covers the IT security functions and specifies how these functions satisfy the TOE security functional requirement with:

- The security function supplied by the Integrated Circuit
- The security functions supplied by the platform ES
- The security function supplied by the Digital Signature GemSAFE V2

6.1.1 TOE security functions list

Identification	Name	SOF statement
IC Security functions		
SEF1	Operating State checking	See note 1
SEF3	Protection against snooping	See note 1
SEF4	Data encryption and data distinguish	See note 1
SEF5	Random number generator	See note 1
SEF6	TSF self test	See note 1
SEF7	Notification of physical attack	See note 1
SEF9	Cryptographic support	See note 1
Digital Signature Security Functions		
SF_SIG_AUTHENTICATION	Authentication management	Yes
SF_SIG_CRYPTO	Cryptography management	N/A
SF_SIG_INTEGRITY	Integrity	N/A
SF_SIG_MANAGEMENT	Management of operations & access control	N/A
SF_SIG_SECURE_MESSAGING	Secure messaging	N/A
Platform Security Functions		
SF_CARD_AUTHENTICATION	Card authentication	Yes
SF_CARD_CRYPTO	Card cryptographic algorithm & key management	Partial (RNG part)
SF_CARD_EMANATION	Emanation protection	N/A
SF_CARD_INTEGRITY	Card objects integrity	N/A
SF_CARD_MGR	Card Manager	N/A
SF_CARD_PROTECT	Card operation protection	N/A
SF_CARD_SECURE_MESSAGING	Card Secure Messaging	N/A

Table 6 – TOE security functions list

Note 1 : IC SOF claim is defined in IC security target

6.1.2 Security functions provided by the IC

The security functions listed here after are described in the IC Security Target SLE66CX642P/m1485b16 With RSA 2048 V1.30.

6.1.2.1 SEF1- Operating state checking.

Correct function of the SLE66CX642P is only given in the specified range. To prevent an attack exploiting that circumstances it is necessary to detect if the specified range is left.
All operating signals are filtered to prevent malfunction.
In addition the operating state is monitored with sensors for the operating voltage, clock signal, frequency, temperature and electro magnetic radiation. The TOE falls into the defined secure state in case of a specified range violation.

6.1.2.2 SEF2- Phase Management with test mode lock-out

This Security function deals with Chip different operating mode: test mode and User mode.
This Security function is not used by the software as chip is always delivered in User mode.

6.1.2.3 SEF3- Protection against snooping.

Several mechanisms protect the SLE66CX642P with RSA2048 against snooping the design or the user data during operation and even if it is out of operation (power down)
There are topological design measures for disguise, such as the use of the top metal layer with active signals for protecting critical data. The entire design is kept in a non standard way to prevent attacks using standard analysis methods. A smart card dedicated CPU with a non public bus protocol is used which makes analysis complicated.
This function uses probabilistic and permutational effect and has to be included in the AVA_SOF analysis with SOF HIGH.

6.1.2.4 SEF4- Data encryption and data disguising

The readout of data can be controlled with the use of encryption. Only the key owner has the possibility to read out the data. An attacker cannot use the data he has espionaged, because he must break the encryption.
The memory contents of the SLE66CX642P with RSA2048 are encrypted on chip to protect against data analysis on stored data as well as on internally transmitted data. To prevent interpretation of leaked information randomness is inserted in the information.

6.1.2.5 SEF5- Random number generating.

Random data is essential for cryptography as well as for physical security mechanisms. The SLE66CX642P with RSA2048 is equipped with a true random generator based on physical probabilistic controlled effects. The random data can be used from the user software as well as from the security enforcing functions.

6.1.2.6 SEF6- TSF self test

The TSF of the SLE66CX642P has either a hardware controlled self test which can be started from the user software or can be tested directly from the user software.

6.1.2.7 SEF7- Notification of physical attack

The entire surface of the SLE66CX642P is protected with the active shield. Attacks over the surface are detected when the shield lines are cut or get contact.

6.1.2.8 SEF8- Memory Management Unit (MMU)

The MMU in the SLE66CX642P with RSA2048 gives the user software possibility to define access rights for memory areas.
This Security feature is not used by the TOE Software.

6.1.2.9 SEF9- Cryptographic support

The TOE is equipped with several hardware accelerators to support the standard cryptographic operations. This security enforcing function is introduced to include the cryptographic operation in the scope of the evaluation as the cryptographic function itself is not used from the TOE security policy. On the other hand these functions are of special interest for the use of the hardware platform for the software. The components are a hardware DES encryption unit and a combination of software and hardware unit to support RSA cryptography and RSA key generation.

6.1.3 Security functions provided by the Digital signature application GemSAFE V2

6.1.3.1 SF_SIG_AUTHENTICATION - Authentication management

This security function manages the authentication mechanisms of the Digital Signature application including authentication operations for secure channel management.
This Security Function:

- Manages Authentication failure and detect when 3 unsuccessful authentication attempts occur related to consecutive failed authentication attempts .When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall block D.RAD.
- Maintains security attributes D.RAD belonging to individual users.

This SF allows the following operation to be performed on behalf of the user, before the user is authenticated :

- Identification the user
- Establishing a trusted path between local user and the TOE.
- Establishing a trusted channel between the SCA and the TOE for D.DTBS import.
- Establishing a trusted channel between the TOE and the SSCD (Option a) for D.SCD import.

This SF uses a permutational mechanism for the Authentication of the users (PIN code or D.RAD) and establishing Secure channel, and has to be included in the AVA_SOF analysis with SOF HIGH.

6.1.3.2 SF_SIG_CRYPTO - Cryptography management

This function manages the cryptographic operations of the Digital signature application.

- Destroys the previous cryptographic keys, in case of re-importation (option a)
- Destroys the previous cryptographic keys, in case of re-generation (option b)
- Perform Cryptographic operations for authentication and, Secure messaging: MAC computation for signature in CBS mode, Decryption, Encryption, session key computation in CBC mode

This function is supported by platform Security Function SF_CARD_CRYPTO .
SF_CARD_CRYPTO provides Cryptographic algorithms DES, RSA and Random Generator and Ensures that D. SCD information is made unavailable after use.
SF_CARD_CRYPTO provides the following for the Digital Signature

- Generates 3DES keys
- Generates RSA cryptographic keys within the range of 1024 to 2048
- Performs SCD/SVD correspondence

6.1.3.3 SF_SIG_INTEGRITY integrity

This SF will monitor the integrity of user data and integrity of the DTBS.
Integrity of user persistently stored data D.SCD, D.RAD and D.SVD is monitored using the platform Security Function SF_CARD_INTEGRITY.

In case of integrity error this SF will

- Prohibit the use of the altered data
- Inform the S.Signatory about integrity error.

This SF will also monitor integrity of access condition of created data objects.

6.1.3.4 SF_SIG_MANAGEMENT Management of operations and Access control

This SF provides application operation management and access control

Operation management
This SF manages the Digital Signature application during its initialization and operation.
This SF manages the Security Environment of the application and ensures the following:

- Maintains the roles S.Signatory, S.Admin,
- Controls if the authentication is required for a specific operation has been performed with success and manages restriction to security function access and modification of security attributes.
- only secure values are accepted for security attributes

This SF restricts the ability to enable the function Signature-creation SFP to S.Signatory
This SF will ensure that only S.Admin will be authorized to
- modify SCD Import SFP attributes,
- specify alternative default values.

This SF enforces the SCD Import SFP and Signature-creation SFP to provide **restrictive** default values.
Only S.Admin is allowed to specify alternative values.

Access control
This SF provides the digital signature access control SFP and ensures that operations on digital signature objects will be executed by authorized roles:

- import and export of D.SVD by S.User
- Generation of D.SCD/D.SVD pair by S.User (option b)
- Creation of D.RAD by S.Admin
- SCD import (option a) by S.User
- Sending of D.DTBS-representation by the SCA
- Signing of D.DTBS-representation by S.Signatory

This SF will provide access control to APDUs according to APDU format (CLA,INS) and Application life cycle
This SF will provide Access control to Data Objects according access rules related to the objects.

This SF enforces the security policy on Import and export of user data:
- SVD Transfer SFP
- SCD Import SFP: D.SCD shall be sent by an authorized SSCD.
- Signature-creation SFP: D.DTBS-representation shall be sent by an authorized SCA

6.1.3.5 SF_SIG_SECURE_MESSAGING

This SF will ensure the integrity and confidentiality of user data exchanged.
This SF ensures that the TSF is able to
- receive D.SCD objects in a manner protected from unauthorized disclosure (option a)
- Transmit user data D.SVD in a manner protected from modification and insertion errors.
- Determine on receipt of user data, whether modification and insertion has occurred
- receive user data D.DTBS-representation in a manner protected from modification, deletion and insertion errors
- determine on receipt of user data, whether modification, deletion and insertion has occurred

This SF manages four modes of Secure Channel:
- Mutual Authentication
- Mutual authentication with integrity (MAC)
- Mutual authentication with encryption
- Mutual authentication with Integrity (MAC) and encryption

This SF is supported by the Platform SF_CARD_SECURE_MESSAGING during the Application personalization phase.

6.1.4 Security function provided by the platform

6.1.4.1 SF_CARD_AUTHENTICATION card authentication

This security function ensures the management of the administrator authentication:

- The ***Terminal*** is authenticated through the administrator authentication mechanism, based on a one-time cryptographic challenge-response protocol.
- The administrator is the only card user able to open a secure channel.

As the User PIN is the application User PIN managed by the application itself, this Security Function manages administrator authentication that allows to open secure channel for communication with the Terminal. Authentication failure is managed using the SCP Retry Counter. When the predefined number of unsuccessful authentication is reached the card will be BLOCKED.
The administrator authentication is based on the one-time cryptographic challenge-response protocol. This function is SOF High and has to be included in the AVA_SOF analysis with SOF HIGH.

6.1.4.2 SF_CARD_CRYPTO : Card cryptographic algorithm and keys managements

This security function provides the cryptographic algorithm and functions used by the TSF

- DES algorithm supports 64 bits, 128 bits 192 bits long keys. The DES algorithm is the certified hardware DES.
- RSA algorithm supports 1024bits to 2048 bits long keys. The RSA algorithm is **software**.
- Random generator is software and uses the certified Hardware True Random Generator.

This security function controls all the operations relative to the card keys management:

- Key generation: The TOE provides the following:
  - RSA key generation manages 512 to 2048 bits long keys . The RSA key generation is **software**.
  - DES key generation manages 64, 128, 192 bits long keys. The 3DES key generation (for session keys) uses the certified hardware DES.
- Key decryption: the TOE provides Applications with a mean to decrypt keys which are imported using an APDU command. This service is provided by OP/VOP Java API.
- Key destruction: the TOE provides specified cryptographic key destruction methods that makes Key Unavailable.

The Random generator is needed for the generation of Keys, and Authentication challenge. The Random Generator part of this SF is SOF-High
The Random generator used the Hardware True RNG compliant with AIS31 and provides a K3-DRNG according to AIS20.

This function ensures the confidentiality of keys during manipulation and ensures the de-allocation of memory after use.
This SF is supported by IC security functions SEF5 –Random number generator and SEF9 –Cryptographic support.

6.1.4.3 SF_CARD_EMANATION : Emanation protection

This SF protects the Digital signature application data D.RAD and D.SCD against snooping:

- Ensures that TOE shall not emit electromagnetic radiation in excess of unintelligible emission enabling access to D.RAD and D.SCD.
- Ensures that the TOE shall ensure attacker S.OFFCARD are unable to use I/O, VCC or Ground interface to gain access to D.RAD and D.SCD:

This SF is supported by IC Security functions SEF3-Protection against snooping and SEF4- Data encryption and data distinguish.

6.1.4.4 SF_CARD_INTEGRITY : Card objects integrity

This security function provides a mean to check the integrity of data stored in EEPROM: the cryptographic keys, including Digital Signature persistently stored data D.SCD, D.RAD and D.SVD, and the card life cycle state.
This SF controls the manipulation of the D.USER_PIN (D.RAD and D.VAD) and will ensure that its value is unavailable during the data manipulation.
Incase of integrity error detection, this SF will prohibit the use of the altered data, and inform Administrator to take appropriate actions: Mute or terminate the card.
This SF supports SF_CARD_PROTECT by checking platform data integrity before use .

This SF also provides authorized users with the capability to verify the integrity of stored TSF executable code.

6.1.4.5 SF_CARD_MGR - Card manager

This security function ensures the administration of the card during all its life-cycle: initialization phase personalization phase, and usage phase.

This SF enforces the following access control policies

- Platform initialization access control.
- Applet installation, extradition, deletion,
- Firewall - Java Objects access control,

This SF will analyze incoming commands and check access rights, according to life-cycle and the Secure Environment required.

This SF ensures that only authorized administrator can manage card content and manages following access control policies based on security attributes.

This SF will provide access control to objects according to the security context required.

- During platform initialization, operations are performed by the authenticated Card Manufacturer, the Card Manager (Issuer) Security Domain is created and the associated Card Manager keys are loaded before the Card Life Status is set to OP-READY. Once in OP-READY state, the Card is under Card Manager control.
- Once the platform is set to OP-READY, applets can be installed by the authenticated Card Manager, through a successfully opened Secure Channel. Application Security Domains are created with associated keys loaded.
  Only an authenticated card Manager is allowed to modify the security functions, change card life Cycle, or lock the load operation, or to update the keys . Access to objects is controlled by the Firewall using the Security context attached to each Java Objects .
- During usage phase the Card Manager will control access to a Java Object through the Firewall, using the Security context associated with each object.

The Selection of an application is always allowed.

This Security function is dependent on SF_CARD_AUTHENTICATION and SF_CARD_SECURE_MESSAGING

6.1.4.6 SF_CARD_PROTECT : Card operation protection

This security function ensures the protection of the TSF and supports the following operations.

- Analyze potential violation on : Card Life Cycle inconsistency, PIN and keys integrity error, illegal access to Java objects, unavailability of resources
- Take action upon violation detection : Reset the card, block the action, terminate or mute the Card .
- Check Startup security conditions (consistency of life-cycle, specific data area integrity)
- Check operating conditions of active shield at start-up (using SEF6)

In case of error detections this functions returns an error or an exception and take appropriate shield action
If during the TSF execution an unexpected error or abortion occurs, a secure state will be preserved by resetting security attributes to secure values and if necessary recover the persistently stored data to a secure consistent state.

This security function ensures atomicity of Java objects update in EEPROM:

- The content of the data that are modified within a transaction is copied in the transaction dedicated EEPROM area.
- Commit operation: closes the transaction, and clears the dedicated transaction area.
- Rollback operation: restores the original values of the objects (modified during the transaction) and clears the dedicated transaction area.
- The TOE manages an optimistic backup: the optimistic backup mechanism includes a backup of the previous data value at first data modification, and previous value restoring at abort.
- The security function ensures that the EEPROM containing sensitive data is in a coherent state whatever the time when EEPROM programming sequence stops, either during copying, invalidating, restoring data to or from the backup dedicated EEPROM area or updating sensitive data in EEPROM.

This SF is supported by the IC SEF6 Self test.

6.1.4.7 SF_CARD_ SECURE_MESSAGING: Card secure messaging

This security function ensures the integrity and/or the confidentiality of command messages transmission in a secure channel. The integrity is achieved by adding a signature (Message Authentication Code: MAC) to the command message. The confidentiality is achieved by APDU message data field encryption. These features are used in accordance with the security mode applied to the secure channel.
This Security Function is activated after a Card Manager authentication that allows the Secure Channel opening.
Then this SF will ensure the closing of the secure channel after a Select Application command or in case of error within the session.
Communication channel is initiated by the local user.
Secure channel is required for the Applet Install or Extradite and Card Manager keys loading (ISD Keys).
This SF depends on SF_CARD_AUTHENTICATION.

6.2 ASSURANCE MEASURES

This chapter defines the list of the assurance measures required for the TOE security assurance requirements.

6.2.1 Assurance measures list

Measure	Name
AM_ACM	Configuration management, reference ACM01A10190C
AM_ADO	Delivery and Operation, reference ADO01A10190C
AM_ADV	Development, reference ADV01A10190C
AM_AGD	Guidance documents, reference AGD01A10190C
AM_ALC	Life cycle, reference ALC01A10190C
AM_ATE	Tests, reference ATE01A10190C
AM_AVA	Vulnerability assessment, reference AVA01A10190C

Table 7 – Assurance measures list

6.2.2 AM_ACM: Configuration management

This assurance measure ensures the configuration management. The CM responsible is in charge to write the CM plan, use the CM system and validate the CM system in order to confirm that ACM_XXX.Y components are completed.

6.2.3 AM_ADO: Delivery and Operation

This assurance measure ensures the delivery and operation. The delivery responsible is in charge to write delivery documentation and validate it in order to confirm that the procedure is applied.

6.2.4 AM_ADV: Development

This assurance measure ensures the development. The development responsible is in charge to design the TOE, write development documentation and validate it in order to confirm that the related security functional requirements are completed by security functions.

6.2.5 AM_AGD: Guidance documents

This assurance measure ensures the guidance documents. The guidance responsible is in charge to write administrator and user guidance. The documentation provides the rules to use and administrate the TOE in a secured manner.

6.2.6 AM_ALC: Life cycle

This assurance measure ensures the life cycle. The life cycle responsible is in charge to confirm that the life cycle process is applied.

6.2.7 AM_ATE: Tests

This assurance measure ensures the tests. The test responsible is in charge to write tests and execute it in order to confirm that the security functions are tested.

6.2.8 AM_AVA: Vulnerability assessment

This assurance measure ensures the vulnerability assessment. The security responsible is in charge to confirm that the security measures are suitable to meet the TOE security objectives conducing a vulnerability analysis.

7. PP CLAIMS

7.1 PP REFERENCE

The Protection Profiles “Secure Signature Creation Devices” Type 2 [PP SSCD2] for option a, and [PP SSCD3] for option b, are claimed.

The PP “Secure Signature-Creation device Type 2” V1.04 [PP SSCD2] is certified at the German Certification Body under the number **BSI-PP-0005-2002**T- 03-04-2002

The PP “Secure Signature-Creation device Type 3” V1.05 [PP SSCD3] is certified at the German Certification Body under the number **BSI-PP-0006-2002**T- 03-04-2002

7.2 PP REFINEMENT

The following functional requirements found in the claimed PP are refined.

Component	Iteration	Assignment	Selection	Refinement
TOE				
FCS_CKM.1 (option b)	–	X	–	–
FCS_CKM.4 (option a)	–	X	–	–
FCS_CKM.4 (option b)	–	X	–	–
FCS_COP.1 /CORRESP	X	X	–	–
FCS_COP.1 /SIGNING	X	X	–	–
FCS_COP.1 /DES	X	X	–	–
FDP_ACC.1/SVD Transfer SFP (option a)	X	–	–	–
FDP_ACC.1 /SVD Transfer SFP (option b)	X	–	–	–
FDP_ACC.1 /SCD Import SFP (option a)	X	–	–	–
FDP_ACC.1 /Initialization SFP (option b)	– X	–	–	–
FDP_ACC.1 /Personalization SFP	X	–	–	–
FDP_ACC.1 /Signature-creation SFP	X –	–	–	–
FDP_ACF.1 Initialization SFP (option b)	X	–	–	X
FDP_ACF.1 SVD Transfer SFP	X	–	–	–
FDP_ACF.1 SCD Import (option a)	X	–	–	X
FDP_ACF.1 Personalization SFP	X	–	–	–
FDP_ACF.1 Signature-creation SFP	X	–	–	–
FDP_ETC.1 SVD Transfer identical	X	–	–	–
FDP_ITC.1 /SCD (option a)	X	–	–	–
FDP_ITC.1 DTBS	X	–	–	–

Component	Iteration	Assignment	Selection	Refinement
FDP_RIP.1	–	–	–	X
FDP_SDI.2 /persistent	X	–	–	X
FDP_SDI.2 /DTBS	X	–	–	–
FDP_UCT.1 Receiver (option a) identical	X	–	–	–
FDP_UIT.1 SVD Transfer identical	X	–	–	–
FDP_UIT.1 DTBS identical	X	–	–	–
FIA_AFL.1	–	X	–	X
FIA_ATD.1 identical	–	–	–	–
FIA_UAU.1 (option a) identical	X	–	–	–
FIA_UAU.1 (option b) identical	X	–	–	–
FIA_UID.1 (option a) identical	X	–	–	–
FIA_UID.1 (option b) identical	X	–	–	–
FMT_MOF.1 identical	–	–	–	–
FMT_MSA.1 Administrator (option a)	X	X	–	X
FMT_MSA.1 Administrator (option b)	X	X	–	X
FMT_MSA.1 Signatory	X	X	–	–
FMT_MSA.2 identical	–	–	–	–
FMT_MSA.3 (option a) identical	X	–	–	x
FMT_MSA.3 (option b) identical	X	–	–	x
FMT_MTD.1		X	–	–
FMT_SMR.1 identical	–	–	–	–
FPT_AMT.1	–	–	X	–
FPT_EMSEC.1	–	X	–	–
FPT_FLS.1 l	–	X	–	–
FPT_PHP.1 identical	–	–	–	–
FPT_PHP.3	–	X	–	–
FPT_TST.1	–	X	X	X
FTP_ITC.1 SCD Import (option a)	X	–	X	–
FTP_ITC.1 SCD Transfer (option a)	X	X	X	–
FTP_ITC.1 SVD Transfer (option b)	X	X	X	–
FTP_ITC.1 DTBS Import		X	X	–
FTP_TRP.1 TOE	–	X	X	–
IT Environment Signature Key Generation SSCD type 1				
FCS_CKM.1 (option a)	–	x	–	–
FCS_CKM.4 (option a)	–	x	–	–
FCS_COP.1 Correspondence (option a)	–	X	–	–
FDP_ACC.1 SCD Export SFP (option a)	–	X	–	–
FDP_UCT.1 Sender (option a)	–	X	–	–
FTP_ITC.1 SCD Export (option a)	–	–	X	–
IT Environment CGA				
FCS_CKM.2 /CGA	–	X	–	–

Component	Iteration	Assignment	Selection	Refinement
FCS_CKM.3 /CGA	–	X		–
FDP_UIT.1 SVD Import	–	X	X	–
FTP_ITC.1 SVD Import (option a)	–	X	X	–
FTP_ITC.1 SVD Import (option b)	–	X	X	–
IT Environnement SCA				
FCS_COP.1 SCA Hash	–	X	–	–
FDP_UIT.1 SCA DTBS	–	X	–	–
FTP_ITC.1 SCA DTBS (option a)	X	X	X	–
FTP_ITC.1 SCA DTBS (option b)	X	X	X	–
FTP_TRP.1 (option a) identical	X	–	X	–
FTP_TRP.1 (option b) identical	x	–	X	–

Table 8 – Mapping of the performed operations and the IT security functional requirements

7.3 PP ADDITIONS

As this Security Target includes the Embedded Software of the platform that supports the GemSAFE V2 security requirements for the platform in have been added order to ensure the secure operation of the SSCD. Section 8 demonstrates that the platform Security Requirements, the related Security Functional requirements and security functions, do not lead to conflict or misleading statements with the Security requirements of the [PP SSCD2] and [PP SSCD3].

7.3.1 Assets refinement

Assets have been refined with the following names: D.SCD, D.DTBS, D.VAD, D.RAD, D.SIGN_APPLI, D.SIGNATURE.

Following assets have been added for the platform :
D.CODE, D.GP_KEYS, D.GP_REGISTRY, D.ISD_DATA, D.ISD_KEYS, D.SD_DATA, D.SD_KEYS, D.USER_PIN, D.JAVA_OBJECT .

7.3.2 Additional assumptions

Following assumption has been added to the [PP SSCD2]/[PP SSCD3]
A.Plt_Process, A.No_Loading.

7.3.3 Additional Organizational Security Policy

Following [PP SSCD2]/[PP SSCD3] OSP has been refined
P.CSP_Qcert.

Following OSP has been added to the [PP SSCD2]/[PP SSCD3]
P.Plt_Support, P.IC_Support, P.Applet_Conformity

7.3.4 Additional threats

All threats from [PP SSCD2]/[PP SSCD3] have been refined with the assets refined names.

.Following threats have been added for the platform : T.Plt_Integrity, T.Plt_Confidentiality, T.Plt_Install T.Plt_Execution, T.Plt_Operate

7.3.5 Additional security objectives

The following [PP SSCD2]/[PP SSCD3] security objective have been refined:
OT.SCD_Secrecy (Secrecy of the SCD) is refined with D.VAD, D.RAD and D.SCD

Following objectives have been added for the platform
OT.Plt_Integrity, OT.Plt_Confidentiality, OT.Plt_Reallocation, OT.Plt_Install, OT.Plt_Execution, OT.Plt_Firewall, OT.Plt_Operate, OT.Plt_Support, OT.IC_Support.

Following Objectives for the platform environment have been added
OE.No_Loading, OE.Applet_Conformity, OE.Plt_Process.

7.3.6 Additional security functional requirements

Following Security Functional Requirements has been added to the claimed PP:
FCS_COP.1/DES: Cryptographic operations (for DES operations and Mac computation).

Following Security Functional Requirements have been added to fulfill the platform objectives.
FAU_ARP.1, FAU_SAA.1, FCS_CKM.1/RSA, FCS_CKM.1/DES FCS_CKM.3, FCS_CKM.4, FCS_COP.1/RSA, FCS_COP.1/DES FDP_ACC.1/Platform Initialization, FDP_ACC.1/Card Manager, FDP_ACC.1/Firewall,FDP_ACF.1/Platform Initialization, FDP_ACF.1/ Card Manager, FDP_ACF.1/Firewall FDP_RIP.1, FDP_SDI.2/KEYS, FDP_SDI.2/Card_Life_Cycle FDP_UCT.1, FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UID.1, FIA_USB.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FPT_FLS.1/Platform, FPT_PHP.1, FPT_PHP.3, FPT_RVM.1, FPT_SEP.1, FPT_TDC.1, FPT_TST.1, FTP_TRP.1

7.3.7 Additional security assurance requirements

Assurance requirement component ADV_IMP.1 has been augmented to ADV_IMP.2
The TOE being composed of Digital Signature application supported by a Java Card Type Platform, the whole TSF can be represented .

8. RATIONALE

This section presents the evidence to be used for the ST evaluation. This evidence supports the claim that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment.

This rational is built in two parts. One part addresses the Digital Signature application, GemSAFE V2 and the other part addresses the supporting GP platform ES.

As this ST claims compliance to [PP SSCD2] and [PP SSCD3] for the Digital Signature application GemSAFE V2, the following section will not repeat the entire PP SSCD rational but will refer to the PPSSCD rational parts in Appendix 1.

8.1 DIGITAL SIGNATURE PPSSCD RATIONAL

8.1.1 Assets coverage

The following table shows how the threats address the SSCD assets.

Threats / Assets	D.SCD	D.SVD	D.DTBS	D.VAD	D.RAD	D.SIGN_APPLI	D.SIGNATURE
T.Hack_Phys	x	x		x	x	x	
T.SCD_Divulg	x						
T.SCD_Derive	x						
T.Sig_Forgery							x
T.Sig_Repud							x
T.SVD_Forgery		x					
T.DTBS_Forgery			x				
T.SigF_Misuse				x		x	

Table 9 – SSCD Threats / Assets correspondence analysis

The next table shows that Platform threats address the Platform identified assets.

	D.CODE	D.GP_KEYS	D.GP_REGISTRY	D.ISD_DATA	D.ISD_KEYS	D.SD_DATA	D.SD_KEYS	D.USER_PIN	D.JAVA_OBJECT
T.Plt_Integrity	X	X	X	X	X	X	X	X	
T.Plt_Data_confidentiality		X			X		X	X	
T.Plt_Install			X			X	X		
T.Plt_Execution	X								X
T.Plt_Operate	X	X	X	X	X	X	X	X	X

8.1.2 Security objectives rational

8.1.2.1 Digital Signature Security objectives rational

The following table shows how the security objectives appropriately cover threats, assumptions and Organizational Security policies for the digital signature application.

Threats - Assumptions - Policies / Security objectives	**OT.EMSEC_Design**	**OT.Lifecycle_Security**	**OT.SCD_Transfer (option a)**	**OT.SCD_Secrecy**	**OT.SCD_SVD_Corresp**	**OT.SVD_Auth_TOE**	**OT.Tamper_ID**	**OT.Tamper_Resistance**	**OT.DTBS_Integrity_TOE**	**OT.Sigy_SigF**	**OT.Sig_Secure**	**OE.SCD_SVD_Corresp(option a)**	**OE.SCD_Transfer (option a)**	**OE.SCD_Unique (option a)**	**OE.CGA_Qcert**	**OE.SVD_Auth_CGA**	**OE.HI_VAD**	**OE.SCA_Data_Intend**
T.Hack_Phys	x			x			x	x										
T.SCD_Divulg			x	x									x					
T.SCD_Derive											x			x				
T.SVD_Forgery						x										x		
T.DTBS_Forgery									x									x
T.SigF_Misuse									x	x							x	x
T.Sig_Forgery	x	x	x	x	x	x	x	x			x	x	x		x	x		x
T.Sig_Repud	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x

A.CGA															x	x		
A.SCA																		x
A.SCD_Generate												x	x	x				
P.CSP_Qcert					x							x			x			
P.Qsign										x	x				x			x
P.Sigy_SSCD										x				x				

Table 10 – Security objectives correspondence analysis (option a)

Threats - Assumptions - Policies / Security objectives	**OT.EMSEC_Design**	**OT.Lifecycle_Security**	**OT.SCD_Secrecy**	**OT.SCD_SVD_Corresp**	**OT.SVD_Auth_TOE**	**OT.Tamper_ID**	**OT.Tamper_Resistance**	**OT.DTBS_Integrity_TOE**	**OT.Sigy_SigF**	**OT.Sig_Secure**	**OT.Init (option b)**	**OT.SCD_Unique (option b)**	**OE.CGA_Qcert**	**OE.SVD_Auth_CGA**	**OE.HI_VAD**	**OE.SCA_Data_Intend**
T.Hack_Phys	x		x			x	x									
T.SCD_Divulg			x													
T.SCD_Derive										x		x				
T.SVD_Forgery					x									x		
T.DTBS_Forgery								x								x
T.SigF_Misuse								x	x						x	x
T.Sig_Forgery	x	x	x	x	x	x	x			x			x	x		x
T.Sig_Repud	x	x	x	x	x	x	x	x	x	x		x	x	x		x
A.CGA													x	x		
A.SCA																x
P.CSP_Qcert				x									x			
P.Qsign									x	x			x			x
P.Sigy_SSCD									x		x	x				

Table 11– Security objectives correspondence analysis (option b)

Refer to Appendix 1 - Security Objective sufficiency ([PP SSCD2]/PP SSCD 3 section 6.2.2) which contains [PP SSCD2]/[PP SSCD3] rational section 6.2.2 for Security objective Sufficiency argumentation

8.1.2.2 Platform security objective rational

Threats - Assumptions - Policies / Security objectives	**OT.Plt_Integrity**	**OT.Plt_Confidentiality**	**OT.Plt_reallocation**	**OT.Plt_Install**	**OT.Plt_Execution**	**OT.Plt_Firewall**	**OT.Plt_Operate**	**OT.Plt_Support**	**OT.IC_Support**	**OE.Applet_Conformity**	**OE.No_Loading**	**OE.Plt_Process**
T.Plt_Integrity	X											
T.Plt_Confidentiality		X	X									
T.Plt_Install				X								
T.Plt_Execution					X	X						
T.Plt_Operate							X					
P.Plt_Support	X	X	X	X	X	X	X	X				
P.Ic_Support									X			
P.Applet_Conformity										X		
A.No_Loading											X	
A.Plt_Process												X

OT. Plt_Integrity addresses the protection of data stored in the memory, against corruption or unauthorized modification and the code integrity check . It covers **T.Plt_Integrity**

OT.Plt_Confidentiality addresses protection of data against disclosure when stored transferred or used. This objective covers **T.Plt_Confidentiality**.

OT.Plt_Reallocation addresses specifically disclosure of sensitive information during re-allocation. This objective covers also **T.Plt_Confidentiality**.

OT.Plt_Install addresses the control of applet installation /deletion instances by an authorized administrator . This objective covers **T.Plt_Install**.

O.Plt_Execution addresses Card Content management control and covers **T.Plt_Execution**.

O.Plt_Firewall addresses specifically the control of data sharing between applets and addresses also **T.Plt_Execution**

O.Plt_Operate addresses the correctness of operating condition for the platform and covers **T. Plt_Operate**

All these objectives contributes to the satisfaction of the Platform OSP **P.Plt_Support.**
OT.Plt_Support covers directly **P.Plt_Support**

OT.IC_Support covers the IC OSPs P.IC_Support.

.

OE.Applet_Conformity addresses the **P.Applet_Conformity** policies by requiring appropriate testing according to Java Card 2.1.1 and GP 2.0.1' testing and guidance for secure TOE installation.

OE.No_Loading addresses the prohibition of applet loading after TOE delivery at the end of phase 3 and covers **A.No_Loading assumption**.

OE.PLt_Process addresses the Security procedures to be implemented by Card Manufacturer and Card Issuer during phase 4 to 6 and covers **A.Plt_Process** .

8.1.3 Digital Signature Security Functional Requirements rationale

The following table shows how the security functional requirements appropriately cover Digital signature application objectives .

Security Functional Requirements / Security objectives (option a)	OT.EMSEC_Design	OT.Lifecycle_Security	OT.SCD_Transfer (option a)	OT.Datas_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure
FCS_CKM.4		x	x	x							
FCS_COP.1/CORRESP					x						
FCS_COP.1/SIGNING											x
FCS_COP.1/DES		x							x		
FDP_ACC.1/SVD TRANSFER SFP						x					
FDP_ACC.1/PERSONALISATION SFP										x	
FDP_ACC.1/SCD IMPORT SFP (option a)			x								
FDP_ACC.1/SIGNATURE-CREATION SFP									x	x	
FDP_ACF.1/SVD TRANSFER SFP						x					
FDP_ACF.1/PERSONALISATION SFP										x	
FDP_ACF.1/SCD IMPORT SFP (option a)			x								
FDP_ACF.1/SIGNATURE-CREATION SFP									x	x	
FDP_ETC.1/SVD TRANSFER						x					
FDP_ITC.1/SCD (option a)			x								
FDP_ITC.1/DTBS									x		
FDP_RIP.1				x						x	
FDP_SDI.2/DTBS									x		
FDP_SDI.2/Persistent				x	x					x	x
FDP_UCT.1/Receiver SCD (option a)			x								
FDP_UIT.1/SVD TRANSFER						x					

Security Functional Requirements / Security objectives (option a)	OT.EMSEC_Design	OT.Lifecycle_Security	OT.SCD_Transfer (option a)	OT.Datas_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure
FDP_UIT.1/TOE DTBS									**x**		
FIA_AFL.1										**x**	
FIA_AFL.1										**x**	
FIA_ATD.1										**x**	
FIA_UAU.1(option a)										**x**	
FIA_UID.1 (option a)										**x**	
FMT_MOF.1				**x**						**x**	
FMT_MSA.1/ADMINISTRATOR (option a)				**x**							
FMT_MSA.1/SIGNATORY				**x**						**x**	
FMT_MSA.2			**x**							**x**	
FMT_MSA.3/(option a)			**x**	**x**						**x**	
FMT_MTD.1										**x**	
FMT_SMR.1			**x**	**x**						**x**	
FPT_AMT.1		**x**		**x**							**x**
FPT_EMSEC.1	**x**										
FPT_FLS.1				**x**							
FPT-PHP.1							**x**				
FPT_PHP.3								**x**			
FPT_TST.1		x									x
FTP_ITC.1/SCD IMPORT (option a)			x								
FTP_ITC.1/SVD TRANSFER						x					
FTP_ITC.1/DTBS IMPORT									x		
FTP_TRP.1/TOE										x	

Table 12 – Functional requirements to TOE type 2 Security objective Mapping

Security Functional Requirements / Security objectives (Option b)	OT.EMSEC_Design	OT.Lifecycle_Security	OT.INIT	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_UNIQUE	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure

Security Functional Requirements / Security objectives (Option b)	OT.EMSEC_Design	OT.Lifecycle_Security	OT.INIT	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_UNIQUE	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure
FCS_CKM.1(option b)				x	x				x			
FCS_CKM.4 (option b)		x		x								
FCS_COP.1/CORRESP					x							
FCS_COP.1/SIGNING												x
FCS_COP.1/DES		x								x		
FDP_ACC.1/SVD TRANSFER SFP						x						
FDP_ACC.1/INITIALIZATION SFP (option b)			x	x								
FDP_ACC.1/PERSONALISATION SFP											x	
FDP_ACC.1/SIGNATURE-CREATION SFP										x	x	
FDP_ACF.1/INITIALIZATION SFP(option b)			x	x								
FDP_ACF.1/SVD TRANSFER SFP						x						
FDP_ACF.1/PERSONALISATION SFP											x	
FDP_ACF.1/SIGNATURE-CREATION SFP										x	x	
FDP_ETC.1/SVD TRANSFER						x						
FDP_ITC.1/DTBS										x		
FDP_RIP.1				x							x	
FDP_SDI.2/Persistent				x	x						x	x
FDP_SDI.2/DTBS										x		
FDP_UIT.1/SVD TRANSFER						x						
FDP_UIT.1/TOE DTBS										x		
FIA_AFL.1			x								x	
FIA_ATD.1			x								x	
FIA_UAU.1 (option b)			x								x	
FIA_UID.1 (option b)			x								x	
FMT_MOF.1				x							x	
FMT_MSA.1/ADMINISTRATOR (option b)			x	x								
FMT_MSA.1/SIGNATORY				x							x	
FMT_MSA.1/USER				x								
FMT_MSA.2											x	
FMT_MSA.3/(option b)			x	x							x	
FMT_MTD.1											x	
FMT_SMR.1				x							x	
FPT_AMT.1		x		x								x
FPT_EMSEC.1	x											
FPT_FLS.1				x								
FTP_PHP.1							x					
FTP_PHP.3								x				
FPT_TST.1		x										x
FTP_ITC.1/SVD TRANSFER						x						
FTP_ITC.1/DTBS IMPORT										x		
FTP_TRP.1/TOE											x	

Table 13– Functional requirements to TOE type 3 Security objective Mapping

Environment security Requirements/ Environment Security Objectives Type 2 (option a)	OE.SCD_SVD_Corresp	OE.SCD_TRansfer	OE.SCD_Unique	OE.CGA_QCert	OE_HI_VAD	OE .SCA_Data_Intend	OE.SVD_Auth_CGA
FCS_CKM.1	X		X				
FCS_CKM.4/Type1		X					
FCS_COP.1/CORRESP	X						
FDP_ACC.1/SCD Export SFP		X					
FDP_UCT.1/SEnder		X					
FDP_ITC.1/SCD Export		X					
FCS_CKM.2/CGA				X			
FCS_CKM.3/CGA				X			
FDP_UIT.1/SVD Import							X
FDP_ITC.1/SVD Import							X
FCS_COP.1/SCAHASH						X	
FDP_UIT.1/SCA DTBS						X	
FTP_ITC.1/SCA DTBS						X	
FTP_TRP.1/SCA					X		
R.Sigy_Name				X			

Table 14- IT Environment Functional Requirement to Environment Security Objective Mapping (type 2)

Environment security Requirements/ Environment Security Objectives Type 3 (option b)	OE.CGA_QCert	OE_HI_VAD	OE .SCA_Data_Intend	OE.SVD_Auth_CGA
FCS_CKM.2/CGA	X			
FCS_CKM.3/CGA	X			
FCS_COP.1/SCA HASH			X	
FDP_UIT.1/SVD Import				X
FDP_ITC.1/SVD Import				X
FDP_UIT.1/SCA DTBS			X	
FTP_ITC.1/SCA DTBS			X	
FTP_TRP.1/SCA		X		
R.Sigy_Name	X			

Table 15 - IT Environment Functional Requirement to Environment Security Objective Mapping (type 3)

Objectives	Requirements
Security Assurance Requirements (option a)	
OT.Life-Cycle_Security	ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ADO_DEL.2, ADO_IGS.1
OT.SCD_Secrecy	ADV_IMP.2, AVA_SOF.1, AVA_VLA.4
OT.Sigy_SigF	AVA_VLA.4
OT.Sig_Secure	AVA_MSU.3, AVA_SOF.1, AVA_VLA.4
Security Objectives	ACM_AUT.1, ACM_CAP.4, ACM_SCP.2, ADO_DEL.2, ADO_ISG.1, ADV_FSP.2, ADV_HLD.2, ADV_IMP.2, ADV_LLD.1, ADV_RCR.1, ADV_SPM.1, AGD_ADM.1, AGD_USR.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2

Table 16- Assurance requirements to security objectives mapping (type 2)

Objectives	Requirements
Security Assurance Requirements (option b)	
OT.Life-Cycle_Security	ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ADO_DEL.2, ADO_IGS.1
OT.SCD_Secrecy	AVA_SOF.1, AVA_VLA.4
OT.Sigy_SigF	AVA_MSU.3, AVA_SOF.1
OT.Sig_Secure	AVA_VLA.4
Security Objectives	ACM_AUT.1, ACM_CAP.4, ACM_SCP.2, ADO_DEL.2, ADO_ISG.1, ADV_FSP.2, ADV_HLD.2, ADV_IMP.2, ADV_LLD.1, ADV_RCR.1, ADV_SPM.1, AGD_ADM.1, AGD_USR.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2

Table 17- Assurance requirements to security objectives mapping (type 3)

Refer to Appendix 1 - Security requirement sufficiency ([PP SSCD2]/PP SSCD 3 section 6.3.2)which contains [PP SSCD2]/[PP SSCD3] rational section 6.3.2 for Security objective Sufficiency argumentation

8.1.3.1 Security functional Requirements dependency rational

Refer to Appendix 1 - Functional and assurance requirement dependencies which contains [PP SSCD2] rational in section 6.4 for functional and assurance requirements dependencies argumentation.

8.1.3.2 Rational for extension

Refer to Appendix 1 Rational for extension (PP SSCD 6.6) which contains [PP SSCD2] rational in section 6.6 for additional family FPT_EMSEC rational.

8.1.3.3 Security assurance requirements rationale

Strength of function rational (see [PP SSCD2]/[PP SSCD3] section 6.7)

The TOE shall demonstrate to be highly resistant against penetration attacks in order to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. The protection against attacks with a high attack potential dictates a strength of function high rating for functions in the TOE that are realized by probabilistic or permutational mechanisms.

Assurance level rational (see [PP SSCD2] [PP SSCD3] section 6.7)

The assurance level for this protection profile is EAL4 augmented.EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. The TOE described in this protection profile is just such a product. Augmentation results from the selection of:
AVA_MSU.3 Vulnerability Assessment - Misuse - Analysis and testing for insecure states
AVA_VLA.4 Vulnerability Assessment - Vulnerability Analysis – Highly resistant
The TOE is intended to function in a variety of signature generation systems for qualified electronic signatures. Due to the nature of its intended application, i.e., the TOE may be issued
to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.
In **AVA_MSU.**3, an analysis of the guidance documentation by the developer is required to provide additional assurance that the objective has been met, and this analysis is validated and confirmed through testing by the evaluator. AVA_MSU.3 has the following dependencies:
ADO_IGS.1 Installation, generation, and start-up procedures
ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance
All of these are met or exceeded in the EAL4 assurance package.
AVA_VLA.4 Vulnerability Assessment - Vulnerability Analysis – Highly resistant
The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. AVA_VLA.4 has the following dependencies:
ADV_FSP.1 Informal functional specification
ADV_HLD.2 Security enforcing high-level design
ADV_IMP.2 Implementation of the TSF augmentation from ADV_IMP.1- Subset Implementation of TSF, is needed as it is important for a Smart Card that the evaluation includes the representation of the entire TSF and determines whether the functional requirements in the Security target are addressed by the representation of the TSF to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure.
ADV_IMP.2 has dependencies with ADV_LLD.1 ADV_RCR.1 and ALC_TAT.1 . These assurance components are included in EAL4, then these dependencies are satisfied.
ADV_LLD.1 Descriptive low-level design

The assurance level of the Hardware platform included in the TOE, is EAL5 augmented with components ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4. The Hardware platform assurance level required is therefore appropriate for the Digital signature Smart Card assurance level.

8.1.4 Platform Security Functional Requirements rationale

The following section shows how the security functional requirements appropriately cover Platform objectives.

OT.Plt_Integrity
This objective requires that the data and code stored in the platform memories be protected against corruption or unauthorized modification. This objective is ensured by Access control to objects defined in by **FD_ACC .1** and **FDP_ACF.1. FIA_UAU.1 and FIA_UID** ensures that no operation can be performed on objects before authentication. **FMT_MSA.1**, **FMT_MSA.2**, **FMT_MSA.3**, **FMT_MTD.1** and **FMT_SMF.1** enforce the access control policies and contribute to satisfy this objective as well as **FPT_SEP.1** that ensure protection from interference and tampering by untrusted subjects.
The verification of code integrity is covered is covered by **FPT_TST.1**

OT.Plt_Confidentiality
This objective requires data to be protected against disclosure during storage, usage or transfer.
Confidentiality of data is supported by **FDP_RIP.1** during usage, and **FDP_UCT.1** and **FTP_TRP.1** during transfer
FCS_CKM.4 prevent access to cryptographic unused keys .
FIA_UAU.1 and **FIA_UID.1** prevent access to stored data when user is not authenticated.
FPT_SEP.1 protect data from interference by untrusted subjects.
Confidentiality during data exchange is supported by cryptography, **FCS_CKM.1**, **FCS_CKM.3** and **FCS_COP.1**

OT.Plt_Reallocation
This objective is directly mapped to **FDP_RIP.1** that specifically requires deallocation of resources

OT.Plt_Install
This objective requires a specific control on applet management.
Access control policy **FDP_ACC.1/Card Manager** with **FCP_ACF.1/Card Manager** fulfill the objectives for a secure installation, deletion and personalization of the applet.
This objective is also supported by **FMT_MOF.1**, **FMT_MSA.1**, **FMT_MSA.2**, **FMT_MSA.3** with **FMT_SMF.1,** which restrict ability to install or delete the application by authorized user with the controlled management of attributes related to these operations.

OT.Plt_Execution

This objective requires that only authorized administrator is allowed to manage Card content.
Access control policy defined in **FDP_ACC.1** and **FDP_ACF.1** fulfills this objective. **FIA_ATD.1** maintains attributes belonging to users while **FIA_USB.1** associate user attributes with subjects, **FMT_SMR.1** allows to associate user with roles . These SFRs support authentication mechanisms required by this objective.
Management of security function and attributes through **FMT_MOF.1**, **FMT.MSA.1**, **FMT_MSA.2** **FMT_MSA.3** as well as **FMT_MTD.1** and **FMT_SMF.1** enforce this Access control policy.

OT.Plt_Firewall
This objectives requires explicitly that the platform controls the sharing of data.

FDP_ACC.1 Firewall, **FDP_ACF.1/Firewall** meet this objectives

OT.Plt_Operate
This objective requires that the platform ensure correct operation of its security function.
This is achieved by:

- **FAU_ARP.1** and **FAU_SAR.1** which provide security alarms and potential violation analysis.
- **FDP_SDI.2** which monitors data integrity
- **FIA_AFL.1** which monitors authentication failures
- **FPT_FLS.1** which monitors failure states preserving secure state.
- **FPT_PHP.1** and **FPT_PHP.3** which provide physical detection
- **FPT_TST.1** which monitors operating conditions

FPT_TDC.1 support this objective, by ensuring Inter-TSF data consistency.

OT.Plt_Support
This objectives requires the platform to support specifically Digital Signature operations.
All SFR contribute to meet this objective

OT.IC_Support
This objectives requires the IC to provide mechanisms to support the secure operation of the TSF when attacks path are hardware oriented.
FPT_PHP.1 and **FPT_PHP.3** security function address specifically hardware parts of the TOE.

Security Functional Requirements / Security objectives	OT.Plt_Integrity	OT.Plt_Confidentiality	OT.Plt_reallocation	OT.Plt_Install	OT.Plt_Execution	OT.Plt_Firewall	OT.Plt_Operate	OT.Plt_Support	OT.IC_Support
FAU_ARP.1							X		
FAU_SAA.1							X		
FCS_CKM.1/RSA								X	
FCS_CKM.1/DES		X							
FCS_CKM.3		X							
FCS_CKM.4		X							
FCS_COP.1/RSA							X		
FCS_COP.1/DES		X					X		
FDP_ACC.1/Initialization	X				X				
FDP_ACC.1/Card_Manager	X			X	X				
FDP_ACC.1/Firewall	X				X	X			
FDP_ACF.1/Initialization	X				X				
FDP_ACF.1/Card_Manager	X			X	X				
FDP_ACF.1/Firewall	X				X	X			
FDP_RIP.1		X							
FDP_SDI.2/ Keys			X				X		

Security Functional Requirements / Security objectives	OT.Plt_Integrity	OT.Plt_Confidentiality	OT.Plt_reallocation	OT.Plt_Install	OT.Plt_Execution	OT.Plt_Firewall	OT.Plt_Operate	OT.Plt_Support	OT.IC_Support
FDP_SDI.2/Card_Life_Cycle							X		
FDP_UCT.1		X							
FIA_AFL.1							X		
FIA_ATD.1					X				
FIA_UAU.1		X							
FIA_UID.1		X							
FIA_USB.1					X				
FMT_MOF				X	X				
FMT_MSA.1	X			X	X				
FMT_MSA.2	X			X	X				
FMT_MSA.3	X			X	X				
FMT_MTD.1	X				X				
FMT.SMF.1	X			X	X				
FMT_SMR.1					X				
FPT_FLS.1							X		
FPT_PHP.1							X		X
FPT_PHP.3							X		X
FPT_RVM.1	X	X	X	X	X	X	X		
FPT_SEP.1	X	X				X			
FPT_TDC.1							X		
FPT_TST.1	X						X		
FTP_TRP.1		X							

Table 18 : Platform Security objectives / Security Requirements cross table

8.1.4.1 Security functional Requirements dependency rationale

This section demonstrates that all dependencies between components of security functional requirements included in this ST for the Platform part of the TOE, are satisfied.

Security Functional Requirements	Dependencies	Included
FAU_ARP.1 Security Alarms	FAU_SAA.1	Yes
FAU_SAA.1 Potential violation analysis	**FIA_GEN.1**	**No**
FCS_CKM.1 Cryptographic key generation	FCS_COP.1 FCS_CKM.4 FMT_MSA.2	Yes Yes Yes
FCS_CKM.3 Cryptographic key access	FCS_COP.1 FCS_CKM.4 FMT_MSA.2	Yes Yes Yes
FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1	Yes

		FMT_MSA.2	Yes
FCS_COP.1	Cryptographic operations	FCS_CKM.1 FMT_MSA.2	Yes Yes
FDP_ACC.1	Subset Access control	FDP_ACF.1	Yes
FDP_ACF.1	Security attributes based access control	FDP_ACC.1 FMT_MSA.3	Yes (Partial)
FDP_RIP.1	Subset residual information protection	None	_
FDP_SDI.2	Stored data integrity monitoring and action	None	_
FDP_UCT.1	Basic data exchange confidentiality	FTP_ITC.1 or FTP_TRP.1 FDP_ACC.1 or FDP_IFC.1	No Yes Yes No
FIA_AFL.1	Authentication failure handling	FIA_UAU.1	Yes
FIA_ATD.1	User attribute definition	None	_
FIA_UAU.1	Timing of authentication	FIA_UID.1	Yes
FIA_UID.1	Timing of identification	None	_
FIA_USB.1	User-subject binding	FIA_ATD.1	**Yes**
FMT_MOF.1	Management of security function behavior	FMT_SMR.1	Yes
FMT_MSA.1	Management of security attributes	FDP_ACC.1 FMT_SMR.1	Yes Yes
FMT_MSA.2	Secure security attributes	ADV_SPM.1 FDP_ACC.1 FMT_MSA.1 FMT_SMR.1	Yes Yes Yes Yes
FMT_MSA.3	Static attribute initialization	FMT_MSA.1 FMT_SMR.1	Yes Yes
FMT_MTD.1	Management of TSF data	FMT_SMR.1	Yes
FMT_SMF.1	Specification of Management function	None	_
FMT_SMR.1	Security roles	FIA_UID.1	Yes
FPT_FLS.1	Failure with preservation of secure state	ADV_SPM.1	Yes
FPT_PHP.1	Passive detection of physical attack	FMT_MOF.1	Yes
FPT_PHP.3	Resistance to physical attack	None	_
FPT_RVM.1	No-Bypassability of the TSF	None	_
FPT_SEP.1	TSF Domain separation	None	_
FPT_TDC.1	Inter TSF Basic TSF Data consistency	None	_
FPT_TST.1	TSF testing	**FPT_AMT.1**	**No**
FTP_TRP.1	Trusted Path	None	_

The dependency of FAU_SAA.1 with FAU_GEN.1 is not applicable to the TOE; the FAU_GEN.1 component forces many security relevant events to be recorded (due to dependencies with other functional security components) and this is not achievable in a Smart Card since many of these events result in card being in an insecure state where recording of the event itself could cause a security breach. It is then assumed that the function FAU_SAA.1 may still be used and the specific audited events will have to be defined in the ST independently with FAU_GEN.1.

The dependency of FPT_TST.1 with FPT_AMT.1 is not clearly relevant for a Smart Card; FPT_TST.1 is self-consistent for the platform (hardware and software) and does not require the FPT_AMT.1 function (Abstract Machine Testing). The TOE software is not tested inside the scope of FPT_TST.1. In its relations with external devices, typically the card reader, the TOE is always the slave. This is why FPT_TST.1 is self-consistent, and FPT_AMT.1 is not applicable.
The dependency of FDP_ACF.1 on FMT_MSA.3 is fulfilled for the 'Platform Initialization' and 'Card Manager' policies.
The FDP_ACF.1/Firewall dependency on FMT_MSA.3 is not applicable here as the Firewall operation is inherent to Java Card structure and attributes initialization is not relevant for this operation.

8.1.4.2 Security assurance requirements rationale

The Platform supports the Digital signature application that requires a high resistance to attacks as stated in section 8.1.3.3. The platform security function must have the same SOF as the Digital signature .

Assurance level EAL4 augmented required for the digital signature applies to the platform part of the TOE. Refer to Assurance level rational in section 8.1.3.3.

Security objectives for the environment that address the platform part of the TOE, and which are not covered by a Security Function Requirement, are covered by assurance measures:

OE.Applet_Conformity addresses other applets ROMed and installed on the platform. Appropriate recommendation in AGD and ADO class document will require that ROMed applets fulfill they specification and operate as per GP and Java specifications and will provide instructions for applets installation operation.

OE.No_Loading addresses prohibition of applets loading after TOE delivery**.** Appropriate recommendation in AGD an ADO class document will require Card Manufacturer to lock the possibility of loading application.

OE.Plt_Process addresses the production, delivery and pre-issuance environment of the TOE . Assurance classes as ADV,ACM, ATE, ADO ensures during development, test phases and delivery that the product is protected from Disclosure and physical damage.
Recommendation on AGD, will require the Card Manufacturer and Issuer to take appropriate protection measures to maintain integrity and confidentiality of the TOE and apply appropriate testing to the TOE before issuance.

8.2 TOE SUMMARY SPECIFICATION RATIONALE

8.2.1 Security functions rationale for the Digital Signature application

The following section demonstrates that the Security Functions supplied by the Digital Signature part of the TOE fulfill the [PP SSCD2] and the [PP SSCD3] Security Functional Requirements.

Table 19 shows which SF covers each Security Functional Requirements . Supporting SF from platform including IC appear in gray color.

8.2.1.1 Security functions coverage

FCS-CKM.1 - Cryptographic key generation. (Option b)
This SFR requires the generation of digital signature keys SCD/SVD pair within a specified the key length range.
This requirement is fulfilled by **SF_SIG_CRYPTO** that manages the cryptographic operations of the Digital Signature part of the TOE with the support of the platform Security Function **SF_CARD_CRYPTO.**

FCS-CKM.4 - Cryptographic key destruction. (option a, b)
This SFR requires the destruction of the previous SCD/SVD pair in case of re-generation (option b) or the destruction of the SCD in case of re-importation (option a) . This requirement is fulfilled by **SF_SIG_CRYPTO** that manages the cryptographic operations of the Digital Signature part of the TOE.

FCS_COP.1 - Cryptographic operation.
This SFR requires the availability of cryptographic operations to support the digital signature application.
This requirement is fulfilled by **SF_SIG_CRYPTO** that supply cryptographic algorithm using specified key length for FCS_COP.1/Signing and FCS_COP.1/DES and FCS_COP.1/CORRESP This function uses the platform Security Function **SF_CARD_CRYPTO**

FDP_ACC.1 - **Access control policy**
This SFR requires that each identified access control SFP cover all operations on subjects and objects covered by that SFP. It further requires that all objects and operations with the TSC be covered by at least one identified access control SFP.

SF_SIG_MANAGEMENT fulfill this SFR requirements by ensuring the following access control:
- Import and export of D.SVD fulfill FDP_ACC.1/SVD Transfer SFP (option a and b)
- Generation of D.SCD/D.SVD pair fulfill FDP_ACC.1/ Initialization SFP (Option b)
- Import of D.SCD fulfill FDP_ACC.1/SCD Import SFP (Option a)
- Generation of D.RAD fulfill FDP_ACC.1/ Personalization SFP
- Sending of D.DTBS-representation and Signing of D.DTBS-representation fulfill FDP_ACC.1/Signature-Creation SFP

Security Function/ SFRs	SF_SIG_AUTHENTICATION	SF_SIG_CRYPTO	SF_SIG_INTEGRITY	SF_SIG_MANAGEMENT	SF_SIG_SECURE_MESSAGING	SF_CARD_CRYPTO	SF_CARD_EMANATION	SF_CARD_INTEGRITY	SF_CARD_PROTECT	SF_CARD_SECURE_MESSAGING	SEF1 Operating statee checking	SEF3 Protection against snooping	SEF4 Data encryption & data disguising	SEF6 Self Test	SEF7 Notification of physical attack
FCS_CKM.1(option b)		X				X									

Security Function/ SFRs	SF_SIG_AUTHENTICATION	SF_SIG_CRYPTO	SF_SIG_INTEGRITY	SF_SIG_MANAGEMENT	SF_SIG_SECURE_MESSAGING	SF_CARD_CRYPTO	SF_CARD_EMANATION	SF_CARD_INTEGRITY	SF_CARD_PROTECT	SF_CARD_SECURE_MESSAGING	SEF1 Operating statee checking	SEF3 Protection against snooping	SEF4 Data encryption & data disguising	SEF6 Self Test	SEF7 Notification of physical attack
FCS_CKM.4 (option a)		X													
FCS_CKM.4 (option b)		X													
FCS_COP.1/CORRESP		X				X									
FCS_COP.1/SIGNING		X				X									
FCS_COP.1/DES		X				X									
FDP_ACC.1 (option a) SVD Transfer SFP				X											
FDP_ACC.1 (option b)SVD Transfer SFP				X											
FDP_ACC.1 (option a) SCD Import SFP				X											
FDP_ACC.1 (option b) Initialization SFP				X											
FDP_ACC.1 Personalization SFP				X											
FDP_ACC.1 Signature-creation SFP				X											
FDP_ACF.1 (option b) Initialization SFP				X											
FDP_ACF.1 (option a, b) SVD Transfer SFP				X											
FDP_ACF.1 (option a) SCD Import SFP				X											
FDP_ACF.1 Personalization SFP				X											
FDP_ACF.1 Signature-creation SFP				X											
FDP_ETC.1/ SVD Transfer				X											
FDP_ITC.1/ SCD (option a)				X											
FDP_ITC.1/ DTBS				X											
FDP_RIP.1	X	X													
FDP_SDI.2/Persistent			X					X							
FDP_SDI.2/DTBS			X												
FDP_UCT.1 Receiver (option a)					X										
FDP_UIT.1/SVD Transfer					X										
FDP_UIT.1/TOE DTBS					X										
FIA_AFL.1	X														
FIA_ATD.1	X														
FIA_UAU.1(option a)	X														
FIA_UAU.1(option b)	X														
FIA_UID.1(option a)	X														
FIA_UID.1(option b)	X														
FMT_MOF.1				X											
FMT_MSA.1/				X											

Security Function/ SFRs	SF_SIG_AUTHENTICATION	SF_SIG_CRYPTO	SF_SIG_INTEGRITY	SF_SIG_MANAGEMENT	SF_SIG_SECURE_MESSAGING	SF_CARD_CRYPTO	SF_CARD_EMANATION	SF_CARD_INTEGRITY	SF_CARD_PROTECT	SF_CARD_SECURE_MESSAGING	SEF1 Operating statee checking	SEF3 Protection against snooping	SEF4 Data encryption & data disguising	SEF6 Self Test	SEF7 Notification of physical attack
Administrator (option a)															
FMT_MSA.1/ Administrator (option b)				X											
FMT_MSA.1/ Signatory				X											
FMT_MSA.2	X			X											
FMT_MSA.3 (option a)				X											
FMT_MSA.3 (option b)				X											
FMT_MTD.1				X											
FMT_SMR.1	X			X											
FPT_AMT.1									X					X	
FPT_EMSEC.1							X					X	X		
FPT_FLS.1									X						
FPT_PHP.1											X				X
FPT_PHP.3											X			X	
FPT_TST.1									X						
FTP_ITC.1 (option a) SCD Import					X										
FTP_ITC.1 (option a) SVD Transfer					X										
FTP_ITC.1 (option b) SVD Transfer					X										
FTP_ITC.1/DTBS Import					X										
FTP_TRP.1/TOE					X										

Table 19 – Coverage of PPSSCD SFRs by Digital Signature Security Functions (options a and b)

FDP_ACF Access control functions

This SFR defines the rules for the functions that implement the SFPs identified in FDP_ACC.1.

- Import and export of D.SVD fulfill FDP_ACF.1/SVD Transfer SFP (option a and b)
- Generation of D.SCD/D.SVD pair fulfill FDP_ACF.1/ Initialization SFP (Option b)
- Import of D.SCD fulfill FDP_ACF.1/SCD Import SFP (Option a)
- Generation of D.RAD fulfill FDP_ACF.1/ Personalization SFP
- Sending of D.DTBS-representation and Signing of D.DTBS-representation fulfill FDP_ACF.1/Signature-Creation SFP

SF_SIG_MANAGEMENT supports also this SFR as it allows to control if authorized roles have been correctly identified before access is granted.

FDP_ETC Export to outside TSF control
This SFR requires the appropriate SFPs are enforced during export of user data without its associated security attributes.
SF_SIG_MANAGEMENT ensures that the SVD is exported without its security attributes and enforces **FDP_ETC/SVD Transfer** SFP.

FDP_ITC Import from outside TSF control
This SFR requires that the security attributes are supplied separately and correctly represent the user data imported without security attributes.
SF_SIG_MANAGEMENT manages the import of the SCD without any security attributes **(FDP_ITC/SCD)** and the import of DTBS for Signature creation operation (**FDP_ITC/DTBS)**.

FDP_RIP Residual information protection
This SFR requires that the TSF ensure that any residual information content of a resource is made unavailable to objects upon de-allocation of this resource to the objects.
All temporarily copies of the SCD are destroyed after usage by SF_SIG_CRYPTO. For the VAD and RAD the temporarily copies are deleted by SF_SIG_AUTHENTICATION.

FDP_SDI Stored data integrity
This SFR requires that the TSF monitors user data stored within the TSC for identified integrity errors.
SF_CARD_INTEGRITY monitors SCD, RAD, SVD integrity and fulfills **FDP_SDI.2/Persistent**.
SF_SIG_INTEGRITY monitors the DTBS integrity and fulfills **FDP_SDI.2/DTBS.**

FDP_UCT Inter-TSF user data confidentiality transfer protection Receiver **(Option a)**
This SFR requires the TSF ensures the confidentiality of user data when it is transferred using an external channel between distinct TOEs.
SF_SIG_SECURE_MESSAGING fulfill this requirement by ensuring confidentiality of the D. SCD when it is imported

FDP_UIT Inter-TSF user data integrity transfer protection
This SFR requires the TSF ensures the detection of modification, insertion and/or deletion of the user data during a transfer.
SF_SIG_SECURE_MESSAGING fulfill this requirement by ensuring protection against insertion or modification during the D. SVD transfer **(FDP_UIT.1/SVD Transfer)**, and protection against modification, deletion and insertion of D.DTBS during reception. (**FDP_UIT.1.2/TOE DTBS)**

FIA Identification and authentication
These SFRs require authentication management. FIA_UAU.1 (option a), FIA_UAU.1 (option b) FIA_UID.1 (option a), FIA_UID.1 (option b) requirements are fulfilled by SF_SIG_AUTHENTICATION that will ensure the following

- Identification of the user
- Establishing trusted path between local user and TOE
- Establishing a trusted channel between the SCA and the TOE
- Establishing a trusted channel between the TOE and the SSCD (Option a)

FMT_MOF.1 Management of functions in the TSF
This SFR requires to restrict the ability to enable the signature creation function by the signatory. SF_SIG_MANAGEMENT ensures that only S.Signatory will be authorized to enable the Signature-Creation .

FMT_MSA. 1 Management of security attributes
This SFR requires restricting the ability to manage security attributes to S.Admin.
SF_SIG_MANAGEMENT restrict the ability to manage security Attributes for the SCD Import SFP **(FMT_MSA.1/Administrator-option a),**and for Initialization SFP to S.Admin **(FMT_MSA.1/Administrator-option b)**
SF_SIG_ACCESS restrict Signature- creation by S.Signatory **(FMT_MSA.1/Signatory)**

FMT_MSA. 2 Secure Security attributes
This SFR requires that values assigned to security attributes are valid with respect to the secure state.
SF_SIG_AUTHENTICATION ensures that secure values are accepted for D.RAD.
SF_SIG_MANAGEMENT ensures that secure values are accepted for SCD import (option a) SCD/SVD management and SCD operational attributes.

FMT_MSA.3 Static attribute initialization
This SFR ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.
SF_SIG_MANAGEMEMENT ensures that:
- restrictive default values is provided after import of D.SCD (FMT_MSA.3 (option a). SCD operational" is set to "no".
- restrictive default values is provided after generation of the D.SCD (FMT_MSA.3 option b). SCD operational" is set to "no".
- only S.Admin is allowed to specify alternative values

FMT_MTD Management of TSF data
This SFR allows authorized users to manage TSF data.
The access to commands allowing the signatory to modify D.RAD is controlled by SF_SIG_MANAGEMENT.

FMT_SMR.1 Security management roles
This SFR specifies the roles with respect to security that the TSF recognizes.
SF_SIG_AUTHENTICATION and SF_SIG_MANAGEMENT maintains the roles S.Admin and S.Signatory.

FPT_AMT Abstract machine testing
This SFR provides testing of the underlying abstract machine.
The hardware security functionalities are tested during initial start-up and periodically by SF_CARD_PROTECT, and the IC security function SEF6 (TSF self test) that manages the IC security features.

FPT_EMSEC TOE Emanation
This SFR provides counter-measures to avoid access via emanations using TOE interfaces.
These countermeasures are implemented by the platform by SF_CARD_EMANATION and supported by the IC security function SEF3 (protection against snooping) and SEF4 (Data Protection and data disguidsing)

FPT_FLS Fail secure
This SFR requires that the TSF preserve a secure state in the face of the following identified failures:

- Authentication data integrity failure: SF_CARD_PROTECT prevents the use of RAD and informs the user.
- Unexpected abortion of the execution of the TSF due to external events and unexpected errors during execution of the TSF: SF_CARD_PROTECT preserves a secure state by resetting security attributes to secure values and if necessary recovers the persistently stored data to a secure state.

FPT_PHP TSF Physical Protection
FPT_PHP.1 Passive detection of physical attack is supported by security functions provided by the IC, which are SEF1 (Operating state checking), , and SEF7 (Notification of physical attack).

FPT_PHP.3 Notification of physical attack is supported by by security functions provided by the IC, which are SEF1 (Operating state checking) and SEF6 (TSF Self Test)

FPT_TST.1 TSF self test
This SFR requires for self testing of the TSF and verifying the integrity of the executable code.
This SF is provided by the platform Security Function SF_CARD_PROTECT which supports this requirement with testing during initial start-up, and periodically during operation.
FTP_ITC.1 Inter-TSF trusted channel
This SFR requires that the TSF provide a trusted communication channel between itself and another trusted IT product.
SF_SIG_SECURE_MESSAGING manages the trusted channel during initialization and personalization phase for the SCD import (option a) **(FTP_ITC.1/SCD IMPORT),** the SVD export **(FTP_ITC.1/SVD TRANSFER)**, and the DTBS import **FTP_ITC.1/DTBS)**.

FTP_TRP.1 Trusted path
This SFR **FTP_TRP.1/TOE,** requires that a trusted path between the TSF and a user be provided for user authentication. SF_SIG_SECURE_MESSAGING support this requirement

8.2.1.2 Security functions dependencies

This section shows that the Digital signature Security Functions are complete and internally consistent by showing that they are mutually supportive and provide and 'integrated effective whole' also with the platform, including the IC, on which it is built . For Platform Security function rational see section 8.2.2

#	Digital Signature Security Functions	Dependencies	#
1	SF_SIG_CRYPTO	SF_CARD_CRYPTO,	13

2	SF_SIG_INTEGRITY	SF_CARD_INTEGRITY	9
3	SF_SIG_SECURE_MESSAGING	SF_SIG_AUTHENTICATION, SF_SIG_CRYPTO, SF_CARD_SECURE_MESSAGING	4, 1 16
4	SF_SIG_AUTHENTICATION	SF_SIG_CRYPTO	1
5	SF_SIG_MANAGEMENT	SF_SIG_AUTHENTICATION	5
	Platform Security Functions	**See section 8.2.2**	
8	SF_CARD_PROTECT	SF_CARD_INTEGRITY ,SEF6	9, 21
9	SF_CARD_INTEGRITY	None	_
10	SF_CARD_EMANATION	SEF3 Protection against snooping SEF4- Data encryption and data distinguish.	18 19
11	SF_CARD_MGR	SF_CARD_AUTHENTICATION SF_CARD_SECURE_MESSAGING	14 16
13	SF_CARD_CRYPTO	SEF9 Cryptographic support	23
14	SF_CARD_AUTHENTICATION	SF_CARD_CRYPTO	13
16	SF_CARD_SECURE_MESSAGING	SF_CARD_AUTHENTICATION	14
	IC Security Functions		
17	SEF1: operating state check	_	_
18	SEF3: protection against snooping	_	_
19	SEF4: Data encryption	_	_
20	SEF5: Random number generating	_	_
21	SEF6: Self Test	_	_
22	SEF7: Notification of physical attack	_	_
23	SEF9: Cryptographic support	_	_

Table 20 – Digital Signature Security function dependencies

8.2.1.3 SOF level rationale

The strength level for the TOE security functions is **SOF-high**. According to [CEM] part 2 section 424, the strength of cryptographic algorithms is outside the scope of the CC evaluation.

SF_SIG_CRYPTO provides cryptographic algorithm and is therefore outside the scope of SOF for CC evaluation.
The security functions SF_SIG_INTEGRITY, SF_SIG_MANAGEMENT SF_SIG_PROTECTION do not use probalistic or permutational effects.

SF_SIG_AUTHENTICATION, uses a permutational mechanism for the Authentication of the users (PIN code or D.RAD) and establishing Secure channel.
The strength of the functions is SOF-high.

The SOF-High for the authentication of the users (at least 6 digits PIN with retry counter of 3) is achieved with the combination of the following SFRs: FIA_ATD.1, FMT_MSA.2 FIA_AFL.1.
The SOF High for establishing Trusted Path is achieved with the combination of the following SFRS: FIA_UAU.1, FIA_UID.1,FIA_ITC.1, FIA_TRP.1.

SF_SIG_SECURE_MESSAGING, is not directly involved by the SOF as it is based on SF_SIG_AUTHENTICATION.

8.2.2 Security functions rationale for the platform

FAU_ARP.1 Security Alarm
This SFR requires the TOE to take action upon detection of a potential violation.
This requirement is fulfilled by SF_CARD_PROTECT.

FAU_SAA.1 Potential violation Analysis
This SFR requires the TOE to monitor events in order to detect potential violation.
This requirement is fulfilled by SF_CARD_PROTECT.

FCS_CKM.1 Cryptographic key generation
This SFR deals with the generation of cryptographic Keys.
This requirement is fulfilled by SF_CARD_CRYPTO which manages the keys generation according to the required key length and standards

- DES/3-DES key generation fulfills FCS_CKM.1/DES,
- RSA key generation fulfills FCS_CKM.1/RSA

FCS_CKM.3 Cryptographic key access
This SFR deals with cryptographic Keys access.
This requirement is fulfilled by SF_CARD_CRYPTO which manages the keys decryption and session key generation according to OP/VOP and Java Card API standards.

FCS_CKM.4 Cryptographic key destruction
This SFR deals with cryptographic Keys destruction.
This requirement is fulfilled by SF_CARD_CRYPTO which manages the keys destruction methods

FCS_COP.1 Cryptographic operations
This SFR deals with the cryptographic operations.
This requirement is fulfilled by SF_CARD_CRYPTO that provides encryption and description operations with RSA or DES algorithms.

- DES algorithm fulfills FCS_COP.1/DES
- RSA algorithm fulfills FCS_COP.1/RSA

This SFR is supported also by the IC cryptographic features : SEF5 –Random number generator and SEF9 – Cryptographic support.

FDP_ACC.1 Subset access control
This SFR require to enforce the access control policies to subjects and objects of the TOE
This requirement is fulfilled by SF_CARD_MGR that manages the Card access security policies according to Card Life Cycle, authenticated administrator and security context attributes

- Access control during platform Initialization enforces the SFP required by FDP_ACC.1/Initialization
- Access control ensured by the card manager enforces the SFP required by FDP_ACC.1/Card Manager
- The firewall access control enforces the SFP required by FDP_ACC.1/Firewall

FDP_ACF.1 Security attributes based access control
This SFR require to enforce the access control policies to subjects and objects based on security attributes .
This requirement is fulfilled by SF_CARD_MGR that manages the Card access security policies according to Card Life Cycle, authenticated administrator and security context attributes

- Access control during platform Initialization enforces the SFP required by FDP_ACF.1/Initialization
- Access control ensured by the card manager enforces the SFP required by FDP_ACF.1/Card Manager
- The firewall access control enforces the SFP required by FDP_ACF.1/Firewall

FDP_RIP.1 Subset residual information protection
This SFR requires the de-allocation of memory in order to ensure that previous information is unavailable.
This requirement is fulfilled by SF_CARD_CRYPTO for the Keys manipulation and SF_CARD_INTEGRITY during User PIN manipulation.

FDP_SDI.2 Stored data integrity monitoring and action
This requirement is fulfilled by SF_CARD_INTEGRITY that provides means to check the integrity of stored data as keys (FDP_SDI.2/Keys), User Pin, life cycle state (FDP_SDI.2/Life Cycle).
In case of integrity error this SF will throw an exception to inform Administrator to take appropriate action.

FDP_UCT.1 Basic data exchange confidentiality
This SFR requires the TSF to be able to transmit and receive objects in a protected manner.
This requirement is fulfilled by SF_CARD_SECURE_MESSAGING .

FIA_AFL.1 Authentication failure handling
This SFR requires authentication failure handling
This requirement is fulfilled by SF_CARD_AUTHENTICATION which manages Administrator authentication through Retry Counter. When the predefined number of unsuccessful authentication is reached the card will be BLOCKED.

FIA_ATD.1 User attribute definition
This SFR requires the TSF to maintain Security attributes.
This requirement is fulfilled by several security functions:

- SF_CARD_MGR creates the Card Manager Secure environment with the associated authentication data, and manages access to objects through the Firewall,
- SF_CARD_AUTHENTICATION manages Administrator authentication counters
- SF_CARD_SECURE_MESSAGING maintains the Administrator authentication attributes while the Secure channel is open.

FIA_UAU.1 Timing of authentication
This SFR requires the TSF to allows actions before user is authenticated.
This requirement is fulfilled by SF_CARD_MGR that allows actions to be performed if no specific Security environment is required

FIA_UID.1 Timing of identification

This SFR requires the TSF to allows actions before user is identified.
This requirement is fulfilled by SF_CARD_MGR that allows to perform Selection of an application.

FIA_USB.1 User-subject binding
This SFR requires to associate security attributes with subjects acting on behalf of the user.
This requirement is fulfilled by SF_CARD_MGR, SF_CARD_AUTHENTICATION and SF_CARD_SECURE_MESSAGING as defined for FIA_ATD.1

FMT_MOF.1 Management of security function behavior
This SFR requires TSF to restrict ability to modify the behavior of applet Load or install to Card Manager.
This requirement is fulfilled by SF_CARD_MGR.

FMT_MSA.1 Management of security attributes
This SFR requires TSF to enforce the management of Security Attributes.
This requirement is fulfilled by SF_CARD_MGR that allow authenticated administrator to create, modify security attributes according to TOE life cycle.

FMT_MSA.2 Secure security attributes
This SF requires that only secure values are accepted for security attributes.
This requirement is fulfilled by SF_CARD_MGR that allow authenticated administrator to create, modify security attributes and SF_CARD_AUTHENTICATION that controls Retry counter value.

FMT_MSA.3 Static attribute initialization
This SFR requires to enforce access control SFP by providing restrictive default values.
This requirement is fulfilled by SF_CARD_MGR during the creation of the Security Environment of the TOE, Issuer Security Domains, Application Security Domains and related access condition to the commands and Objects created.

FMT_MTD.1 Management of TSF data
This SFR requires to restrict ability to access or modify the Security domain Key (D.SD_KEY)
This requirement is fulfilled by SF_CARD_MGR which restricts the ability to modify keys to Card Manager

FMT_SMF.1 Specification of Management function
This SFR requires to list the security management functions of the TOE.
This requirement is fulfilled as per FMT_MOF.1, FMT_MSA.1, FMT_MTD.1 by SF_CARD_MGR

FMT_SMR.1 Security roles
This SFR requires to maintain security roles
This requirement is fulfilled by SF_CARD_MGR, SF_CARD_AUTHENTICATION and SF_CARD_SECURE_MESSAGING .

FPT_FLS.1 Failure with preservation of secure state
This SFR requires the TOE to preserve a secure state in case of failure.
SF_CARD_PROTECT fulfill the requirement and ensures that TOE will return to a secure state after an Unexpected abortion of the execution of the TSF due to external events.

FPT_PHP.1 Passive detection of physical attacks
This SFR requires attack detection. This requirement is fulfilled by IC security functions SEF1-Operating State Checking and SEF7- Notification of physical.

FPT_PHP.3 Resistance to physical attacks
This SFRS requires physical attack resistance.
This requirements are fulfilled by the IC security functions SEF1-Operating State Checking and SEF6- TSF self Test.

FPT_RVM.1 Non-Bypassability of the TSF
Almost all Security Functions of the platform (including the IC) contributes to the non bypassability of the TSF, except the following:
SF_CARD_EMANATION, SEF3 and SEF4. These SF concern emanation protection using encryption. and are set by construction and has no action on the TSC proceeding
SEF5 random generator and SEF9 Cryptographic support, provide supports but have no action on the TSC proceeding (it does not provide testing or control)
SEF2 and SEF8 are not used by the software.

FPT_SEP TSF Domain separation
This SFR requires the TSF to maintain a security domain for its execution.
This requirement is fulfilled by SF_CARD_MGR that creates the Issuer Security Domain (ISD), specific Security Domain for each application, and manages Objects related these Security Domains.

FPT_TDC.1 Inter-TSF data consistency
This SFR requires the TOE to provide capability to consistently interpret Data Type and Applet code.
This requirement is achieved by the use of Standards ad OP/VPO and JavaCard.
This requirement is fulfilled by the means of SF_CARD_MGR and SF_CARD_PROTECT
Both SFRS deal with data interpretation by Card manager
FPT_TST TSF testing
This SFR requires the TOE to run test to demonstrate its correct operation.
SF_CARD_PROTECT fulfill this requirement by performing security conditions at startup and periodically. The SF_CARD_PROTECT is support ed by the IC SEF6-Selt Test as indicated in Table 22

SF_CARD_INTEGRITY provides capability to authorized users to check TSF data and TSF executable code integrity.

FTP_TRP.1 Trusted channel
This SFR requires the TSF to use Trusted Path for performing some operations.
This requirement is fulfilled by SF_CARD_SECURE_MESSAGING which manages operations that occur under secure messaging conditions.

	SF_CARD_AUTHENTICATION	SF_CARD_CRYPTO	SF_CARD_EMANATION	SF_CARD_INTEGRITY	SF_CARD_MGR	SF_CARD_PROTECT	SF_CARD_SECURE_MESSAGING	SEF1 Operating statee checking	SEF3 protection against snooping	SEF4 Data encryption	SFF5 Random number generating	SEF6 Self Test	SEF7 Notification of physical attack	SEF9 Cryptographic support
FAU_ARP.1						X								
FAU_SAA.1						X								
FCS_CKM.1/RSA		X												
FCS_CKM.1/DES		X												
FCS_CKM.3		X												
FCS_CKM.4		X												
FCS_COP.1/RSA		X												x
FCS_COP.1/DES		X									X			X
FDP_ACC.1/Initilization					X									
FDP_ACC.1/Card Manager					X									
FDP_ACC.1/Firewall					X									
FDP_ACF.1/Initialization					X									
FDP_ACF.1/Card Manager					X									
FDP_ACF.1/Firewall					X									
FDP_RIP.1		X		X										
FDP_SDI.2/Keys				X										
FDP_SDI.2/ CardLifeCycle				X										
FDP_UCT.1							X							
FIA_AFL.1	X													
FIA_ATD.1	X				X		X							
FIA_UAU.1					X									
FIA_UID.1					X									
FIA_USB.1	X				X		X							
FMT_MOF.1					X									
FMT_MSA.1					X									
FMT_MSA.2	X				X									
FMT_MSA.3					X									
FMT_MTD.1					X									
FMT_SMF.1					X									
FMT_SMR.1	X				X		X							
FPT_FLS.1						X								
FPT_PHP.1								X					X	
FPT_PHP.3								X				X		
FPT_RVM.1	X	X		X	X	X	X	X				X	X	
FPT_SEP.1					X									
FPT_TDC.1					X	X								
FPT_TST.1				X		X								
FTP_TRP.1							X							

Table 21 - Coverage of Platform SFR by Security Functions

Note:
SF_CARD_EMANATION is a Security Function provided by the platform but required by the digital Signature application. See Rational in section 8.2.1
SEF3 and SEF4 concern also emanation protection and are necessitated by digital Signature application. See Rational in section 8.2.1
SEF2 and SEF8 are not used by the software.

8.2.2.1 Security functions dependencies

This section shows that the Platform Security Functions are complete and internally consistent by showing that they are mutually supportive and provide and 'integrated effective whole' also with the platform, including the IC, on which it is built.

#	**Platform Security Functions**	**Dependencies**	#
8	SF_CARD_PROTECT	SF_CARD_INTEGRITY,SEF6	9, 21
9	SF_CARD_INTEGRITY	None	_
10	SF_CARD_EMANATION	SEF3 Protection against snooping SEF4- Data encryption and data distinguish.	18 19
11	SF_CARD_MGR	SF_CARD_AUTHENTICATION SF_CARD_SECURE_MESSAGING	14 16
13	SF_CARD_CRYPTO	SEF9 Cryptographic support	23
14	SF_CARD_AUTHENTICATION	SF_CARD_CRYPTO	13
16	SF_CARD_SECURE_MESSAGING	SF_CARD_AUTHENTICATION	14
	IC Security Functions		
17	SEF1: operating state check	_	_
18	SEF3: protection against snooping	_	_
19	SEF4: Data encryption	_	_
20	SEF5: Random number generating	_	_
21	SEF6: Self Test	_	_
22	SEF7: Notification of physical attack	_	_
23	SEF9: Cryptographic support	_	_

Table 22- Platform Security function dependencies

8.2.2.2 SOF level rationale for the platform

The strength level for the TOE security functions is **SOF-high**. According to [CEM] part 2 section 424, the strength of cryptographic algorithms is outside the scope of the CC evaluation.

For platform security functions listed in section 6.1.4, only the functions realized by a probabilistic or permutational mechanism (e.g. a password or hash function), has been identified in the following to have a SOF.

SF_CARD_AUTHENTICATION

The administrator authentication is based on the one-time cryptographic challenge-response protocol. This function is SOF High.

SF_SECURE_MESSAGING
The secure messaging uses a MAC signature to achieve confidentiality.
For this security function, the strength was not evaluated as it is a cryptographic algorithm suitable for encryption and decryption

8.2.3 Security measures rationale

8.2.3.1 Security measures coverage

The following table shows how the assurance measures are appropriated to complete each security assurance requirements.

Security assurance requirement	Assurance measure	Rationale
ACM_AUT.1	AM_ACM	The assurance measure AM_ACM is about configuration management.
ACM_CAP.4	AM_ACM	The assurance measure AM_ACM is about configuration management, and confirms that the ACM_CAP.4 component is completed.
ACM_SCP.2	AM_ACM	The assurance measure AM_ACM is about configuration management, and confirms that the ACM_SCP.2 component is completed.
ADO_DEL.2	AM_ADO	The assurance measure AM_ADO gives the delivery procedures and confirms that the ADO_DEL.2 component is completed.
ADO_IGS.1	AM_ADO	The assurance measure AM_ADO gives the installation, generation and start-up procedures and confirms that the ADO_IGS.1 component is completed.
ADV_FSP.2	AM_ADV	The assurance measure AM_ADV gives the functional specification by describing the internal and external interfaces and confirms that the ADV_FSP.2 component is completed.
ADV_HLD.2	AM_ADV	The assurance measure AM_ADV gives the architectural design by system decomposition and confirms that the ADV_HLD.2 component is completed
ADV_IMP.2	AM_ADV	The assurance measure AM_ADV gives the implementation and confirms that the ADV_IMP.2 component is completed
ADV_LLD.1	AM_ADV	The assurance measure AM_ADV gives the architectural design by subsystem decomposition and confirms that the ADV_LLD.1 component is

		completed
ADV_RCR.1	AM_ADV	The assurance measure AM_ADV gives the correspondence demonstration and confirms that the ADV_RCR.1 component is completed
ADV_SPM.1	AM_ADV	The assurance measure AM_ADV gives the security policy model and confirms that the ADV_SPM.1 component is completed
AGD_ADM.1	AM_AGD	The assurance measure AM_AGD gives the administration documentation and confirms that the AGD_ADM.1 component is completed
AGD_USR.1	AM_AGD	The assurance measure AM_AGD gives the user documentation and confirms that the AGD_USR.1 component is completed
ALC_DVS.1	AM_ALC	The assurance measure AM_ALC gives the security measures and confirms that the ALC_DVS.1 component is completed
ALC_LCD.1	AM_ALC	The assurance measure AM_ALC gives the development process and confirms that the ALC_LCD.1 component is completed
ALC_TAT.1	AM_ALC	The assurance measure AM_ALC gives the development tools and confirms that the ALC_TAT.1 component is completed
ATE_COV.2	AM_ATE	The assurance measure AM_ATE gives the test documentation and confirms that the ATE_COV.2 component is completed
ATE_DPT.1	AM_ATE	The assurance measure AM_ATE gives the test documentation and confirms that the ATE_DPT.1 component is completed
ATE_FUN.1	AM_ATE	The assurance measure AM_ATE gives the test documentation and confirms that the ATE_FUN.1 component is completed
ATE_IND.2	AM_ATE	The assurance measure AM_ATE gives the test documentation and confirms that the ATE_IND.2 component is completed
AVA_MSU.3	AM_AVA	The assurance measure AM_AVA gives the validation of analysis and confirms that the AVA_MSU.3 component is completed
AVA_SOF.1	AM_AVA	The assurance measure AM_AVA gives the SOF evaluation and confirms that the AVA_SOF.1 component is completed
AVA_VLA.4	AM_AVA	The assurance measure AM_VLA gives the covert channel analysis and confirms that the AVA_VLA.1 component is completed

Table 23 – Assurance measures coverage

8.2.3.2 Security measures dependencies

The following table gives the dependencies of the assurance measures.

AM	Dependency	Which is
AM_ACM	AM_ACM	Included
AM_ADO	AM_ACM AM_AGD	Included Included
AM_ADV	AM_ADV AM_ALC	Included Included
AM_AGD	AM_ADV	Included
AM_ALC	AM_ADV	Included
AM_ATE	AM_ADV AM_AGD	Included Included
AM_AVA	AM_ADV AM_AGD	Included Included

Table 24 – Assurance measure dependencies

8.2.4 Mutually supportive and internally consistent rationale

This part shows that the IT security functions are complete and internally consistent by demonstrating that they are mutually supportive and provide an 'integrated effective whole'.
The interactions between security functions are limited to the dependencies between these security functions.

The Platform Part of the TOE provides Security functions to ensure a secure environment for the installation an personalization of the Digital Signature and for the usage phase .
All SF are mutually supportive and built an 'integrated effective whole'.

Assurance measures are those defined in EAL4 with appropriate augmentation due to the high level of security required for the Digital Signature.
Assurance measures also provide an 'integrated effective whole' .

8.3 PP CLAIMS RATIONALE

This security target presents all [PP SSCD2] and [PP SSCD3] threats, assumptions, objectives, assurance measures and functional requirements.

As stated in the [PP SSCD2] and [PP SSCD3] , SSCD Type 2 and Type 3 “are not necessarily to be considered mutually exclusive”.
One product may fulfill both type.
SSCD Type 2 (option a) does not generate SCD /SVD pair so has to import SCD/SVD. The SSCD Type 2 objectives for the TOE (OT.SCD_Transfer, OT_LifeCycle_Security) and for the TOE environment (OE.SCD_Transfer, OE.SCD_Unique, OE.SCD_SVD_Corresp are for the security of SCD/SVD generation outside the TOE and transfer into the TOE.
SSCD Type 3 (option b) TOE objectives for the TOE (OT_LifeCycle_Security OT.Init , OT.SCD_Unique) address the internal generation of the SCD/SVD pair.

In both type, the OT_LifeCycle_Security objective requires that a previous SCD/SVD pair be safely destroyed before a new importation or generation of key pair.
In SSCD Type 2 , OT.SCD_Transfer and OE_SCD_Transfer require that both TOE and environment ansure confidentiality when SCD is imported inside the TOE. This objective does not apply when the SCD is generated inside the TOE. The OT.Init requires only that this generation is performes by authorized person, which is implicit when the SCD is imported.
OE.SCD_Unique and OT.SCD_Unique address same objective for a unique of key pair imported or generated.
OE.SCD_SVD_Corresp requires to the environment to check the correspondence of the key pair before it is imported. This correspondence operation is implicit when the key pair is generated by the TOE and inside the TOE

The SFRs selected to fulfill these objectives are compatible with the services required by both SSCD Type 2 (option a) and SSCD Type 3 (option b) Digital Signature application.

- FCS_CKM.1 applies to option b for the key generation
- FCS_CKM.4 addresses key destruction that applies to either imported (option a) either generated (option b) keys
- FDP_ACC.1 , FDP_ACF.1 address SCD Import and SVD Transfer when Key pair is generated outside the TOE (option a)
- FDP_ACC.1 , FDP_ACF.1 address initialization of Key pair when generated inside the TOE (option b)
- FDP_ETC.1/SVD_Transfer addresses export of SVD which applies to both option a and option b
- FDP_ITC.1/SCD addresses specifically import of SCD for option a
- FDP_UCT.1/Receiver addresses specifically case of SCD import from the environment for option a
- FIA_UAU.1 and FIA_UID.1 requires to establish additional trusted channel in the case of SCD import for option a
- FMT_MSA.1 /Administrator and FMT_MSA.3 addresses Initialisation SFP for option b, while FMT_MSA.1/Administrator and FMT_MSA.3 addresses SCD Import for option a
- FDP_ITC.1/SVD_Transfer addresses the export of the SVD in case of option b , while FDP_ITC.1/SVD_Transfer addresses the transfer of SVD (import and export) in case of option a
- FDP_ITC.1/SCD_Import addresses the import of SCD from the environment in case of option a

This shows that objectives and related SFRS are complementary and allow the TOE to behave either as a SSCD Type 2 (option a) or SSCD Type 3 (option b) as both cases are covered by a functional requirement.

The iterated or added SFRs addresses the specific security objectives related to the transfer of the SCD/SVD pair in case of Type 2, and the specific security objectives of SCD/SVD generation in case of Type3.
Functional iteration of FCS_COP.1/DES does not introduce contradiction.
RSA and DES cryptographic algorithm used for the signature are supplied by the platform .
FCS_COP.1 is hierarchical to no other component and has a dependency with FCS_CKM.1, which is part of the PP and this ST. The FCS_COP.1/DES dependency on FCS_CKM.1 is fulfilled in this ST by the platform SFRs (see 5.2.3.1)

The additional security aspects of this Security Target address the platform that supports the SSCD before or during its installation and during its usage.

- Platform assets to be protected include application user PIN (D.USER_PIN_ , application keys (D.SD_KEYS) and application security domain data (D.SD_DATA) which are stored on the platform.
- Threats address assets that are stored or manipulated by the platform and used by the ROMed applets.
- Assumption (A.No_Loading ,A.Plt_Process) address the product personalisation environment
- OSPs addresses Java Card type product functional specification the platform has to comply to (P.Plt_Support, P.Applet_conformity and the security level required for the IC use (P.IC_Support)
- Platform objectives addresses the platform identified threats, assumptions and OSPs
- The SRF are selected to fulfil the platform security objectives and are compatible with the services required by the Digital Signature application.
    - FAU_ARP.1 and FAU_SAA.1 address the security audit
    - FCS_CKM.1, FCS_CKM.3, FCS_CKM.4 and FCS_COP.1 provide the algorithm and Keys length (RSA,DES) to support the Digital Signature cryptographic requirements,
    - FDP_ACC.1 and FDP_ACF.1 address the Car manager access control policy
    - FDP_RIP.1 and FDP_SDI.2 support also the Digital signature requirements regarding information protection and data integrity.
    - FDP_UCT.1 addresses card manager capability to be able to transmit and receive protected data
    - FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UID.1 and FIA_USB.1 address authentication and identification of the Card Manager users
    - FMT_MOF.1, FMT_MSA.1 , FMT_MSA.2 , FMT_MSA.3, FMT_MTD.1, FMT_SMF.1 , FMT_SMR.1 provides the management of security attributes as platform and application life cycle , platform keys updates . It provides the support for the application installation .
    - FPT_FLS.1, FPT_PHP.1 , FPT_PHP.3, ensure the protection of the smart Card platform product against physical attacks
    - FPT_SEP.1 , FPT_TDC.1 ensures Java Card product type correct operation
    - FPT_TST.1 ensure the correct operation of the platform
    - FTP_TRP.1 provides the trusted channel communication needed for the install of application by the Card manager.

This shows that there is no contradiction between SSCD and platform security.
The platform security supports the SSCD security requirement and complements the Java Card product type required security.

The augmentation of assurance measures component from ADV_IMP.1 to ADV_IMP.2 is compatible with [PP SSCD2] and [PP SSCD3] .
The strength of function claimed is high, and the claimed level is EAL4 + as required by the claimed PP. The IC security functions used by the platform also claim high level and the used IC is compliant to level EAL4+.
Therefore, no inconsistency is introduced. [PP SSCD2] claim is fulfilled and [PP SSCD3] is fulfilled.

9. GLOSSARY & ABBREVIATIONS

CEN workshop agreement (CWA) is a consensus-based specification, drawn up in an open workshop environment of the European Committee for Standardization (CEN). This Protection Profile (PP) represents Annex A to the CWA that has been developed by the European Electronic Signature Standardization Initiative (EESSI) CEN/ISSS electronic signature (E-SIGN) workshop, Area F on secure signature-creation devices (SSCD).
Certificate means an electronic attestation which links the SVD to a person and confirms the identity of that person. (defined in the Directive [1], article 2.9)
Certification generation application (CGA) means a collection of application elements which requests the SVD from the SSCD for generation of the qualified certificate. The CGA stipulates the generation of a correspondent SCD / SVD pair by the SSCD, if the requested SVD has not been generated by the SSCD yet. The CGA verifies the authenticity of the SVD by means of (a) the SSCD proof of correspondence between SCD and SVD and (b) checking the sender and integrity of the received SVD.
Certification-service-provider (CSP) means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures. (defined in the Directive [1], article 2.11)
Data to be signed (DTBS) means the complete electronic data to be signed (including both user message and signature attributes).
Data to be signed representation (DTBS-representation) means the data sent by the SCA to the TOE for signing and is a hash-value of the DTBS or an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS or the DTBS. The SCA indicates to the TOE the case of DTBS-representation, unless implicitly indicated. The hash-value in case (a) or the intermediate hash-value in case (b) is calculated by the SCA. The final hash-value in case (b) or the hash-value in case (c) is calculated by the TOE.
Qualified certificate means a certificate which meets the requirements laid down in Annex I of the Directive [1] and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive [1]. (defined in the Directive [1], article 2.10)
Qualified electronic signature means an advanced signature which is based on a qualified certificate and which is created by a SSCD according to the Directive [1], article 5, paragraph 1.
Reference authentication data (RAD) means data persistently stored by the TOE for verification of the authentication attempt as authorised user.
Secure signature-creation device (SSCD) means configured software or hardware which is used to implement the SCD and which meets the requirements laid down in Annex III of the Directive [1]. (SSCD is defined in the Directive [1], article 2.5 and 2.6).
Signatory means a person who holds a SSCD and acts either on his own behalf or on behalf of the natural or legal person or entity he represents. (defined in the Directive [1], article 2.3)
Signature attributes means additional information that is signed together with the user message.

Signature-creation application (SCA) means the application used to create an electronic signature, excluding the SSCD. I.e., the SCA is a collection of application elements 1. to perform the presentation of the DTBS to the signatory prior to the signature process according to the signatory's decision, 2. to send a DTBS-representation to the TOE, if the signatory indicates by specific non-misinterpretable input or action the intend to sign, 3. to attach the qualified electronic signature generated by the TOE to the data or provides the qualified electronic signature as separate data.
Signature-creation data (SCD) means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature. (defined in the Directive [1], article 2.4)
Signature-creation system (SCS) means the overall system that creates an electronic signature. The signature-creation system consists of the SCA and the SSCD.
Signature-verification data (SVD) means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature. (defined in the Directive [1], article 2.7)
Signed data object (SDO) means the electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.
Sub-Referential. Consistent set of software components (Example: test scripts, specification documents,). A Sub-referential belongs to a Referential.
SSCD provision service means a service that prepares and provides a SSCD to subscribers.
Tip Revision. The latest revision of a line of development (the trunk or a branch)
User means any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Verification authentication data (VAD) means authentication data provided as input by knowledge or authentication data derived from user's biometric characteristics.

10. REFERENCES

Short Reference	Title - Reference
CCPART1	Common Criteria for Information Technology Security Evaluation. Part 1: Introduction & general model,. Version 2.1. August, 1999. CCIMB-99-031/ Incorporated with interpretation as of 2002-02-28
CCPART2	Common Criteria for Information Technology Security Evaluation. Part 2: Functional security requirements, Version 2.1. August, 1999. CCIMB-99-032/ Incorporated with interpretation as of 2002-02-28
CCPART3	Common Criteria for Information Technology Security Evaluation. Part 3: Assurance security requirements, Version 2.1. August, 1999. CCIMB-99-033/ Incorporated with interpretation as of 2002-02-28
CEM	Common Methodology for Information Technology Evaluation, CEM-99/045. Part 2 Evaluation Methodology Incorporated with interpretation as of 2002-02-28

PP SSCD1	Protection Profile Creation Device Type 1 Version 1.05 BSI-PP-0004-2002T- 03-04-2002
[PP SSCD2]	Protection Profile Creation Device Type 2 Version 1.04 BSI-PP-0005-2002T-03-04-2002
[PP SSCD3]	Protection Profile Creation Device Type 3 Version 1.05 BSI-PP-0006-2002T-03-04-2002
DIRECTIVE	DIRECTIVE 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures" DIRECTIVE 1999/93/EC
[E-Sign 1]	Application Interface for Smart Cards used as secure Signature Creation Device CEN/ISSS WS/E-Sign Draft CWA Group K part 1 – Basic requirements. Version 1 Release 9 (17th September 2003)
[E-Sign 2]	Application Interface for Smart Cards used as secure Signature Creation Device CEN/ISSS WS/E-Sign Draft CWA Group K part 2 – Additional services. Version 0 Release:19 (12th December 2003)
[GemXpresso PRO R3]	**GemXpresso PRO R3 Card Reference Manual** Document Reference: DOC106957B Document Version: 2.0 November 24, 2003
[Java Card 2.1.1]	*Java Card 2.1.1 Virtual Machine Specification* from Sun Microsystems, Revision 1.0, May 18, 2000. *Java Card 2.1.1 Virtual Machine Specification*, Revision 1.0, May 18, 2000.
	Java Card 2.1.1 Runtime Environment Specification from Sun Microsystems, *Java Card 2.1.1 Runtime Environment Specification* Revision 1.0, May 18, 2000

	Java Card 2.1.1 Application Programming Interface from Sun Microsystems, *Java Card 2.1.1 Application Programming Interface.* Revision 1.0, May 18, 2000.
[GP2.0.1]	*GlobalPlatform Card Specification 2.0.'1* from GlobalPlatform, *GlobalPlatform Card Specification 2.0.'1* April 7th, 2000.
	GlobalPlatform Card Specification 2.1 from GlobalPlatform *GlobalPlatform Card Specification 2.1* June, 2001.
	Open Platform 2.0.1' Visa Card Implementation Requirements, Configuration 2 compact with PK, from Visa, *Open Platform 2.0.1' Visa Card Implementation Requirements, Configuration 2 - compact with PK*, June 2001.
[AIS32]	*CCIMB All Final Interpretation*
[AIS36]	*Composite evaluation activities* ETR-lite for Composition Reference : Version 1.1, July 2002
	ETR-lite for composition: Annex A Composite smartcard evaluation : Recommended best practice Reference : Version 1.2, March 2002
AIS31	Functionality classes and evaluation methodology for physical Random Number Generator. Version 1 September 2001
AIS20	Functionality classes and evaluation methodology for deterministic Random Number Generator. Version 1 December 1999

Appendix 1- PPSSCD Rationale

1. Security Objective sufficiency ([PP SSCD2]/PP SSCD 3 section 6.2.2)

Policies and security objective sufficiency

P.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. P.CSP_QCert is addressed by the TOE by OT.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.

P.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 [1], article 5, paragraph 1. Directive [1], 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. OT.Sig_Secure and OT.Sigy_SigF address the generation of advanced signatures by the TOE.

P.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 OT.Sigy_SigF ensuring that the SCD is under sole control of the signatory and OT.SCD_Unique **(option b)** ensuring the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. OT.Init **(option b)** and provide that generation of the SCD/SVD pair is restricted to authorised users.

Threats and Security Objective sufficiency

T.Hack_Phys (Exploitation of vulnerabilities in the physical environment), which is a generic threat, deals with physical attacks exploiting vulnerabilities in the environment of the TOE. OT.Datas_Secrecy preserves the secrecy of the datas including D.SCD. Physical attacks through the TOE interfaces are countered by OT.EMSEC_Design. OT.Tamper_ID and OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tamper attacks on the IC.

T.SCD_Divulg (Storing, copying, and releasing of the signature-creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the Directive [1], recital (18). This threat is countered by OT.Datas_Secrecy which assures the secrecy of the datas including the SCD used for signature generation.

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 OT.SCD_Unique **(option b)** and OE.SCD_Unique **(option a)** that provides cryptographic secure generation of the SCD/SVD-pair. OT.Sig_Secure ensures cryptographic secure electronic signatures.

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 than 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 OT.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_Indent.

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 for data the signatory has not decided to sign as required by the Directive [1], Annex III, paragraph 1, literal (c). This threat is addressed by the OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OE.SCA_Data_Intend (Data intended to be signed), OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity), and OE.HI_VAD (Protection of the VAD) as follows: OT.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 OT.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.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 **(option b)**, OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.Datas_Secrecy (Secrecy of datas), 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 **(option b)**,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.Datas_Secrecy, 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 (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, OE.SCD_Unique **(option a)**, OT.SCD_Transfer, OT.datas_Secrecy (Secrecy of datas), 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.Datas_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 (Forgery of the signature-verification data) deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate. T.SVD_Forgery is addressed by OT.SVD_Auth_TOE which ensures that the TOE provides means to enable CGA to verify the authenticity SVD exported by the TOE, as well as by OE.SVD_Auth_CGA which provides verification of SVD authenticity by the CGA.

Assumption and Security objective sufficiency

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 (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 (Secure generation of SCD/SVD) addresses the requirement of confidentiality of the signatory's SCD during the generation process. This 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.

2. Security requirement sufficiency ([PP SSCD2]/PP SSCD 3 section 6.3.2)

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

OT.Init (SCD/SVD generation – option b) addresses that generation of a SCD/SVD pair requires proper user authentication. FIA_ATD.1 define RAD as the corresponding user attribute. The TSF specified by FIA_UID.1 and FIA_UAU.1 provide user identification and user authentication prior to enabling access to authorised functions. The attributes of the authenticated user are provided by FMT_MSA.1/ADMINISTRATOR (option b) and FMT_MSA.3 for static attribute initialisation. Access control is provided by FDP_ACC.1/INITIALISATION SFP (option b) and FDP_ACF.1/INITIALISATION SFP (option b). Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA_AFL.1.

OT.Lifecycle_Security (Lifecycle security) is provided by the security assurance requirements ALC_DVS.1, ALC_LCD.1, ALC_TAT.1,ADO_DEL.2, and ADO_IGS.1 that ensure the lifecycle security during the development, configuration and delivery phases of the TOE. The test functions FPT_TST.1 and FPT_AMT.1 provide failure detection throughout the lifecycle. FCS_CKM.4 provides secure destruction of the SCD. Authenticity and integrity failure detection is ensured by FCS_COP.1/DES.

OT.Datas_Secrecy (Secrecy of data) counters that storage or copying of secrets including the SCD causes a threat to the legal validity of electronic signatures. OT.Datas_Secrecy is provided by the security functions specified by FDP_ACC.1/INITIALISATION SFP (option b) and FDP_ACF.1/INITIALISATION SFP (option b) that ensure that only authorised user can initialise the TOE and create the SCD. The authentication and access management functions specified by FMT_MOF.1, FMT_MSA.1 (option a and b), FMT_MSA.3 (option a and b), and FMT_SMR.1 ensure that only the signatory or administrator can use (signatory) or manage (administrator) the SCD and thus avoid that an attacker may gain information on it. The security functions specified by FDP_RIP.1 and FCS_CKM.4 (option b) ensure that residual information on SCD, VAD, RAD is destroyed after usage and that destruction of SCD leaves no residual information. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD (FCS_CKM.1-option b). The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD, VAD, and RAD. FPT_AMT.1 and FPT_FLS.1 test the working conditions of the TOE and guarantee a secure state when integrity is violated and thus assure that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS is differential fault analysis (DFA).
The assurance requirements ADV_IMP.2 by requesting evaluation of the TOE implementation, AVA_SOF HIGH by requesting strength of function high for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

OT.SCD_SVD_Corresp (Correspondence between SVD and SCD) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1 (option b) to generate corresponding SVD/SCD pairs. The security functions specified by FDP_SDI.2/Persistent ensure that the keys are not modified, so to retain the correspondence. Cryptographic correspondence is provided by FCS_COP.1/CORRESP.

OT.SCD_Transfer (Secure transfer of SCD between SSCD – option a) is provided by FDP_ITC.1/SCD(option a), FTP_ITC.1/SCD IMPORT(option a) and FDP_UCT.1/RECEIVER (option a) that ensure that a trusted channel is provided and that confidentiality is maintained.
Security functions specified by FDP_ACC.1/SCD IMPORT SFP (option a), FMT_MSA.2; FMT_MSA.3(option a), FMT_SMR.1, FDP_ACF.1/SCD IMPORT SFP (option a), ensure that transfer of SCDs is restricted to administrators. This supports the confidentiality-oriented functions.
Security function FCS_CKM.4 destroys the SCD before the SCD is re-imported into the TOE.

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

OT.DTBS_Integrity_TOE (Verification of DTBS-representation integrity) covers that integrity of the DTBS-representation to be signed is to be verified, as well as the DTBS-representation is not altered by the TOE. This is provided by integrity failure detection (FCS_COP.1/DES) and the trusted channel integrity verification mechanisms of FDP_ITC.1/DTBS, FTP_ITC.1/DTBS IMPORT, and by FDP_UIT.1/TOE DTBS. The verification that the DTBS-representation has not been altered by the TOE is done by integrity functions specified by FDP_SDI.2/DTBS. The access control requirements of FDP_ACC.1/SIGNATURE-CREATION SFP and FDP_ACF.1/ SIGNATURE CREATION SFP keeps unauthorised parties off from manipulating the TOE to alter the DTBS-representation. Authenticity

OT.Sigy_SigF (Signature generation function for the legitimate signatory only) is provided by FIA_UAU.1 (option a and b) and FIA_UID.1(option a and b) that ensure that no signature generation function can be invoked before the signatory is identified and authenticated. The security functions specified by FDP_ACC.1/PERSONALISATION SFP, FDP_ACC.1/SIGNATURE-CREATION SFP, FDP_ACF.1/PERSONALISATION SFP, FDP_ACF.1/SIGNATURE-CREATION SFP, FMT_MTD.1 and FMT_SMR.1 ensure that the signature process is restricted to the signatory. The security functions specified by FIA_ATD.1, FMT_MOF.1, FMT_MSA.2, FMT_MSA.3 (option a and b) ensure that the access to the signature generation functions for usage remain under the sole control of the signatory, as well as FMT_MSA.1/SIGNATORY provides that the control of corresponding security attributes is under signatory's control.
The security functions specified by FDP_SDI.2/Persistent and FPT_TRP.1/TOE ensure the integrity of stored data both during communication and while stored. The security functions specified by FDP_RIP.1 and FIA_AFL.1 provide protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication.
The assurance measures specified by AVA_MSU.3 by requesting analysis of misuse of the TOE implementation, AVA_SOF.1 by requesting high strength level for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

OT.Sig_Secure (Cryptographic security of the electronic signature) is provided by the cryptographic algorithms specified by FCS_COP.1/SIGNING which ensures the cryptographic robustness of the signature algorithms. The security functions specified by FPT_AMT.1 and FPT_TST.1 ensure that the security functions are performing correctly. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE.

OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD) is provided by a trusted channel guaranteeing SVD origin and integrity by means of FTP_ITC.1/SVD TRANSFER and FDP_UIT.1/SVD TRANSFER. The cryptographic algorithms specified by FDP_ACC.1/SVD TRANSFER SFP, FDP_ACF.1/SVD TRANSFER SFP and FDP_ETC.1/SVD TRANSFER ensure that only authorized user can export the SVD to the CGA.

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

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

Environment security requirements rationale

OE.CGA_QCert (Generation of qualified certificates) addresses the requirement of qualified certificates. The functions specified by FCS_CKM.2/CGA provide the cryptographic key distribution method. The functions specified by FCS_CKM.3/CGA ensure that the CGA imports the SVD using a secure channel and a secure key access method. R.Sigy_Name ensures that the identity of the person is verified in the corresponding qualified certificate according Annex 2 of [DIRECTIVE].

OE.HI_VAD (Protection of the VAD) covers confidentiality and integrity of the VAD which is provided by the trusted path FTP_TRP.1/SCA.

OE.SCA_Data_Intend (Data intended to be signed) is provided by the functions specified by FDP_UIT.1/SCA DTBS that ensures that the DTBS can be checked, by FTP_ITC.1/SCA DTBS that protects the DTBS by using a trusted channel to transmit the DTBS to the TOE, and FCS_COP.1/SCA HASH that provides that the hashing function corresponds to the approved algorithms.

OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD) is provided by FTP_ITC.1/SVD IMPORT which assures identification of the sender and by FDP_UIT.1/SVD IMPORT wich guarentees it's integrity.

OE.SCD_SVD_Corresp (Correspondence between SVD and SCD) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1 to generate corresponding SVD/SCD pairs. Cryptographic correspondence is provided by FCS_COP.1/SSCD CORRESP.

OE.SCD_Transfer (Secure transfer of SCD between SSCD) is provided by FDP_UCT.1/Sender, that ensure that a trusted channel is provided and that confidentiality is maintained.
Security functions complying with FDP_ACC.1/Export SFP and FTP_ITC.1/ SCD Export ensure that only TOE may export the SCD. Security function specified by FCS_CKM.4/SCCD destroy the SCD, once exported from the TOE.

OE.SCD_Unique (Uniqueness of the signature-creation data) stores the requirement of practically unique SCD as laid down in the Directive [1], Annex III, article 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1.

3. Functional and assurance requirement dependencies (PPSSCD 6.4)

SFR	Dependency	Which is
CGA		
FCS.CKM.2/CGA	[FDP_ITC.1 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	Not included Not included Not included Not included
FCS.CKM.3/CGA	[FDP_ITC.1/SVD IMPORT or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	Included - Not included Not included
FDP_UIT.1/ CGA SVD IMPORT	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1/SVD IMPORT or FTP_TRP.1]	Not included - Included -
FTP_ITC.1/CGA SVD IMPORT	None	-
SCA		
FCS_COP.1/SCA HASH	[FDP_ITC.1 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	Not included Not included Not included Not included
FDP_UIT.1/SCA DTBS	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	Not Included - Included Included
FTP_ITC.1/SCA DTBS	None	
FTP_TRP.1/SCA	None	-
SSCD (option a)		
FCS_CKM.1/SSCD	[FCS_CKM.2 or FCS_COP.1/CORRESP SSCD] FCS_CKM.4/SSCD FMT_MSA.2	Not Included Included Included Not Included
FCS_CKM.4/SSCD	[FDP_ITC.1/ or FCS_CKM.1/SSCD] FMT_MSA.2	- Included Not included
FCS_COP.1/SSCD CORRESP	[FDP_ITC.1/SCD or FCS_CKM.1/SSCD] FCS_CKM.4/SSCD FMT_MSA.2	- included included Not included
FDP_ACC.1/SSCD SCD EXPORT SFP	FDP_ACF.1	Not Included
FDP_UCT.1/SSCD SENDER	[FTP_ITC.1/SSCD SCD EXPORT or	 Included

	FTP_TRP.1] [FDP_ACC.1/SSCD SCD EXPORT SFP or FDP_IFC.1]	- Included -
FTP_ITC.1/SSCD SCD EXPORT	none	-

Justification of unsupported IT environment security functional requirements dependencies

FCS_CKM.2/CGA	The CGA generates qualified electronic signatures including the SVD imported from the TOE. The dependency for the import is supported by FTP_ITC.1/SVD IMPORT. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this ST.
FCS_CKM.3/CGA	The CGA imports SVD via trusted cannel implemented by FTP_ITC.1/ SVD import. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this ST.
FDP_UIT.1/SVD IMPORT (CGA)	The Access control policy (FDP_ACC.1.1) for the CGA are outside of the scope of this ST.
FCS_COP.1/SCA HASH	The hash algorithm implemented by FCS_COP.1/SCA HASH does not require any key or security management. Therefore FDP_ITC.1, FCS_CKM.1, FCS_CKM.4 and FMT_MSA.2 are not required for FCS_COP.1/SCA HASH in the SCA.
FDP_UIT.1/SCA DTBS	The Access control policy (FDP_ACC.1.1) for the SCA are outside of the scope of this ST
FCS_CKM.1/ SSCD	The SSCD generates the SCD/SVD pair. The dependency for cryptographic secure key generation is supported by FCS_COP.1/CORRESP, verificatione of SCD/SVD correspondence, and the key destruction by FCS_CKM.4/SSCD. The Secure security attribute SFR, FMT_MSA.2 is outside the scope of this PP.
FCS_CKM.4/ SSCD	The SSCD destroys the SCD once it has been exported. The dependency for key generation is supported by FCS_CKM.1. The Secure security attribute SFR, FMT_MSA.2 is outside the scope of this PP.
FCS_COP.1/ SSCD CORRESP	The SSCD does a cryptographic operation when creating the SCD/SVD pair, FCS_CKM.1 and when destroying it, FCS_CKM.4/SSCD. The Secure security attribute SFR, FMT_MSA.2 is outside the scope of this PP.
FDP/ACC.1/SSCD SCD Export SFP	The SSCD will follow the SCD export SFP when exporting the SCD. The access control required by this SFP, FDP_ACF.1 Security attribute based access control, is outside the scope of this PP.

4. TOE security assurance requirements rationale (PPSSCD section 6.5)

Security assurance requirements / TOE security objectives correspondence analysis

Requirement	Security Objectives
Security Assurance Requirements	
ACM_AUT.1	EAL 4
ACM_CAP.4	EAL 4
ACM_SCP.2	EAL 4
ADO_DEL.2	EAL 4
ADO_IGS.1	EAL 4

Requirement	Security Objectives
ADV_FSP.2	EAL 4
ADV_HLD.2	EAL 4
ADV_IMP.2	EAL 4 augmented from IMP.1 to IMP.2 in this product ST ; OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF
ADV_LLD.1	EAL 4
ADV_RCR.1	EAL 4
ADV_SPM.1	EAL 4
AGD_ADM.1	EAL 4
AGD_USR.1	EAL 4
ALC_DVS.1	EAL4, OT.Lifecycle_Security
ALC_LCD.1	EAL4, OT.Lifecycle_Security
ALC_TAT.1	EAL4, OT.Lifecycle_Security
ATE_COV.2	EAL 4
ATE_DPT.1	EAL 4
ATE_FUN.1	EAL 4
ATE_IND.2	EAL 4
AVA_MSU.3	OT.Sigy_SigF
AVA_SOF.1	EAL 4, OT.SCD_Secrecy, OT.Sigy_SigF
AVA_VLA.4	OT.SCD_Secrecy, OT.Sig_Secure,

TOE security assurance requirements dependencies

SAR	Dependency	Which is
ACM_AUT.1	ACM_CAP.3	Included (in augmentation with ACM_CAP.4)
ACM_CAP.4	ALC_DVS.1	Included
ACM_SCP.2	ACM_CAP.3	Included (in augmentation with ACM_CAP.4)
ADO_DEL.2	ACM_CAP.3	Included (in augmentation with ACM_CAP.4)
ADO_IGS.1	AGD_ADM.1	Included
ADV_FSP.2	ADV_RCR.1	Included
ADV_HLD.2	ADV_FSP.1 ADV_RCR.1	Included Included
ADV_IMP.2	ADV_LLD.1 ADV_RCR.1 ALC_TAT.1	Included Included Included
ADV_LLD.1	ADV_HLD.2 ADV_RCR.1	Included Included
ADV_RCR.1	None	-
ADV_SPM.1	ADV_FSP.1	Included
AGD_ADM.1	ADV_FSP.1	Included
AGD_USR.1	ADV_FSP.1	Included
ALC_DVS.1	None	-
ALC_LCD.1	None	-
ALC_TAT.1	ADV_IMP.1	Included (in augmentation to ADV_IMP.2)
ATE_COV.2	ADV_FSP.1 ATE_FUN.1	Included Included
ATE_DPT.1	ADV_HLD.1 ATE_FUN.1	Included Included
ATE_FUN.1	None	-
ATE_IND.2	ADV_FSP.1 AGD_ADM.1	Included Included

SAR	Dependency	Which is
	AGD_USR.1 ATE_FUN.1	Included Included
AVA_MSU.3	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1	Included Included Included Included
AVA_SOF.1	ADV_FSP.1 ADV_HLD.1	Included Included
AVA_VLA.4	ADV_FSP.1 ADV_HLD.2 ADV_IMP.2 ADV_LLD.1 AGD_ADM.1 AGD_USR.1	Included Included Included Included Included Included

5. Rational for extension (PP SSCD 6.6)

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.

FPT_EMSEC TOE Emanation
Family behavior
This family defines requirements to mitigate intelligible emanations.
Component leveling:

FPT_EMSEC TOE Emanation	1

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.1.1, FPT_EMSEC.1.2
There are no actions identified that should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.

FPT_EMSEC.1 TOE Emanation

FPT_EMSEC.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_EMSEC.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*].

Hierarchical to: No other components.

Dependencies: No other components.

<END OF DOCUMENT>