MultiApp ID Citizen 72K with HIC/HPC applet

Security Target

TABLE OF CONTENTS

Figures

Tables

1 ST introduction

1.1 ST reference

Title:	IAS Classic Security Target: Heathcare configuration
Reference:	D1077227_Heathcare
Origin:	GEMALTO
ITSEF:	SERMA
Evaluation scheme:	French

Component	Reference/Version	Supplier
Hardmask in ROM	1.0	Gemalto
Softmask in EEPROM	4	Gemalto
Micro-controller S3CC91C	0	Samsung
AIS20-certified Deterministic Random Number Generator (DRNG)	2.0	Samsung
TORNADO RSA library	3.5S	Samsung

Table 1. TOE component

1.2 TOE overview

The Target of Evaluation (TOE) is composed of the **MultiApp** platform and the electronic signature application **IAS Classic**. The platform includes the hardware and the operating system.

The product is a Smart Card Integrated Circuit (IC) with the **MultiApp** platform, the **IAS Classic** applet and the (out-of-TOE) applications defined in Tables 2: all ROMed applets are desactivated and a heathcare application (HIC/HPC) is installed in EEPROM.

TOE Components	**Identification**	**Constructor**
IC	S3CC91C rev 0	Samsung
Platform	MultiApp version 1.1	Gemalto
Electronic signature application	IAS Classic version 3.0	Gemalto
ROMed out-of-TOE Components	**Identification**	**Constructor**
Deactivated non-instanciable applications	CIE/CNS Step 2 MPCOS v3.8 OATH v2.10 Biomatch J API v3.0.1 & Cryptomanager v2.0 PIV v1.20	Gemalto Gemalto Gemalto Precise Biometrics Gemalto

	EID2048 v2.10 Almerys PayPass MCHIP Select v2.7 VSDC v2.7.1 Dual PSE	Gemalto Gemalto Gemalto Visa Gemalto
EEPROmed out-of-TOE Component	**Identification**	**Constructor**
Instanciable application	HIC/HPC	Gemalto

Table 2. Product component (Usecase 1)

The TOE defined in this Security Target is the electronic signature functionalities provided by the **IAS Classic** application, and supported by the MultiApp platform. The other applications are not in the TOE scope and therefore not part of the evaluation. The TOE will be designed and produced in a secure environment and used by each citizen in a hostile environment.

The product is compliant with:
- Java Card 2.2.1
- Global Platform 2.1.1

The electronic signature security functions take advantage on the platform security functions:
- Hardware Tamper Resistance: this is the chip security layer that meets PP SSVG [PP/BSI-0002].
- Secure operation of the MultiApp platform: the part of this ST covering MultiApp is described in [ST_ PLTF].

1.2.1 TOE type

The product is a smartcard including a plastic card and a module performing the interface between reader and the embedded chip. Other smart card product elements (such as holograms, security printing…) are outside the scope of this Security Target. The Target of Evaluation (TOE) is the Smart Card Integrated Circuit with Embedded Software in operation and in accordance to its functional specifications.

1.2.2 TOE boundaries

The TOE is composed of the IC, the software platform and a electronic signature application:

- **S3CC91C** IC including its crypto libraries, which has been certified separately according to [ST/SAMSUNG] claiming [PP/BSI-0002]
- **MultiApp** platform (see detail in [ST_ PLTF])
- **IAS Classic** application

The **TSFs** are composed of:

1. The secure-signature related functions of the **IAS Classic** application: Signatory Authentication, Signature Creation, SCD/SVD Generation, SCD Import & storage, SVD Export.
2. Part of MultiApp platform that installs and supports the IAS Classic application.
3. The **S3CC91C** IC including its crypto libraries tat supports the MultiApp platform.

Figure 1 represents the TOE. The TOE is bodered with bold and un-continuous line. The architecture of MultiApp inside the TOE is presented in [ST_ PLTF].

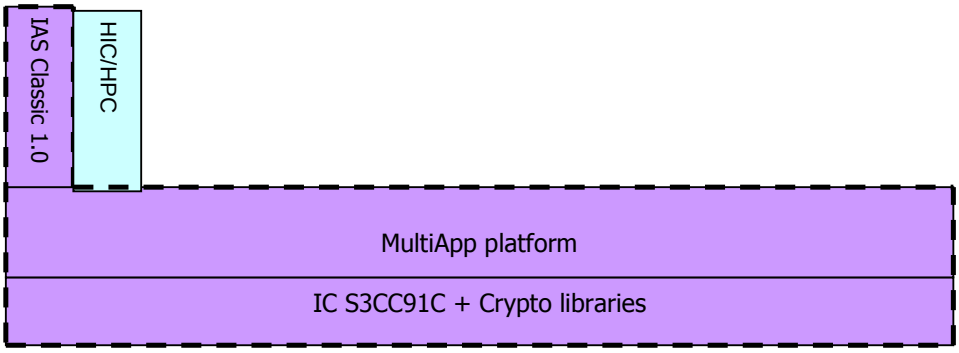

Figure 1. The TOE inside the product

Beside the TOE, the product also contains the following Java Card application:

- **HIC/HPC** provides the healthcare service for both health insurees and health professionals.

1.3 References, Glossary and Abbreviations

Reference	Title
[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCIMB-2005-08-001, version 2.3, August 2005 (conform to ISO 15408).
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCIMB-2005-08-002, version 2.3, August 2005 (conform to ISO 15408).
[CC-3]	Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Requirements CCIMB-2005-08-003, version 2.3, August 2005 (conform to ISO 5408).
[CEM]	Common Methodology for Information Technology Security Evaluation CCIMB-2005-08-004, version 2.3, August 2005.
[PP/SSCD-TYPE2]	Secure Signature-Creation device Protection Profile Type 2 v1.04, EAL4+, 2001
[PP/SSCD-TYPE3]	Secure Signature-Creation device Protection Profile Type 3 v1.05, EAL4+, 2001
[PP/BSI-0002]	Smart Card IC Platform Protection Profile, version 1.0, registered by BSI in 2001 under PP-BSI-0002, Eurosmart document (SSVG Protection Profile).
[ST/SAMSUNG]	Security Target of S3CC91C 16-bit RISC Microcontroller for Smart Cards. Version 1.0, August 2007.
[FIPS 46-3]	FIPS 46-3: DES Data Encryption Standard (DES and TDES). National Institute of Standards and Technology
[FIPS 197]	FIPS 197: AES Advanced Encryption Standard. National Institute of Standards and Technology.
[RSA PKCS#1]	PKCS #1 v2.1: RSA Cryptography Standard
[FIPS 180-2]	FIPS-46-3: Secure Hash Standard (SHA). National Institute of Standards and Technology.
[ISO 7816-4]	Identification cards - Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for interchange.

Reference	Title
[ISO 7816-6]	Identification cards - Integrated circuit(s) cards with contacts, Part 6: Interindustry data elements.
[ISO 7816-9]	Identification cards - Integrated circuit(s) cards with contacts, Part 9: Additional Inter industry commands and security attributes.
[ISO 9796-2]	ISO/IEC 9796-2
[JCAPI221]	Java Card™ APIs specification version 2.2.1, Sun Microsystems, Inc, June 23, 2003.
[JCAPN221]	Application Programming Notes for the Java Card™ Platform, Sun Microsystems, Inc, version 2.2.1, October 2003.
[JCRE221]	Java Card™ Runtime Environment Specification version 2.2.1, Sun Microsystems, Inc, 2003.
[JCVM221]	Java Card™ Virtual Machine Specification version 2.2.1, Sun Microsystems, Inc, 2003.
[JVM]	The Java Virtual Machine Specification. Lindholm, Yellin. ISBN 0-201-43294-3.
[GP]	Global Platform. Card Specification – v2.1.1, March 2003.
[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)
[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
[ST_PLFT]	MultiApp Platform Security Target

2 TOE Description

The description of the MultiApp platform is described in [ST_PLTF].

2.1 IAS Classic description

IAS Classic 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.

Three Protection Profiles have been defined. The SSCD PP 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/SSCD-TYPE1].

- The SSCD PP for a TOE Type 2, which is a Signature creation and verification component [PP/SSCD-TYPE2]. 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/SSCD-TYPE3].

In this document the terminology of [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] is used. In particular, the Signatory's Reference Authentication Data (RAD) is the PIN stored in the card and the Signatory's Verification Authentication Data (VAD) is the PIN provided by the user.

The IAS Classic application is compliant to **both the SSCD Type 2** and **Type 3** and supports:

- The import of the SCD via a trusted channel
- The (on-board) generation of SCD/SVD pairs
- The generation of electronic signatures
- The export of the SVD to the certification generation application (CGA)

IAS Classic is aimed to create legal valid signatures and therefore provides mechanisms to ensure the secure signature creation as:

- Authentication of the signatory (by PIN),
- Authentication of the administrator (mutual authentication):
  - Symmetric scheme with TDES or
  - Asymmetric scheme with Diffie-Hellman
- Integrity of access conditions to protected data (SCD, RAD),
- Integrity of the data to be signed (DTBS),
- External communication protection against disclosure and corruption (secure messaging),
- Access control to commands and data by authorized users.

2.2 TOE Life-cycle

The product life cycle is described in Figure 2. Some remarks are added to explain this figure:

- The TOE is the product at the end of the phase 5.
- **Platform design** and **application design** correspond to the phase 1.
- **Hardware design** corresponds to the phase 2.
- **Hardware fabrication** corresponds to the phase 3.
- **Application installation** is done in the phase 5.
- **Loading of corrective softmask** is done in the phase 5.
- **Loading of application data**, **SCD import (type 2), and SVD export (for certificate)** are done in the phase 6.
- **SCD/SVD generation (type 3) and signature creation** correspond to the phase 7.
- **SSCD destruction** corresponds to the end of the phase 7.

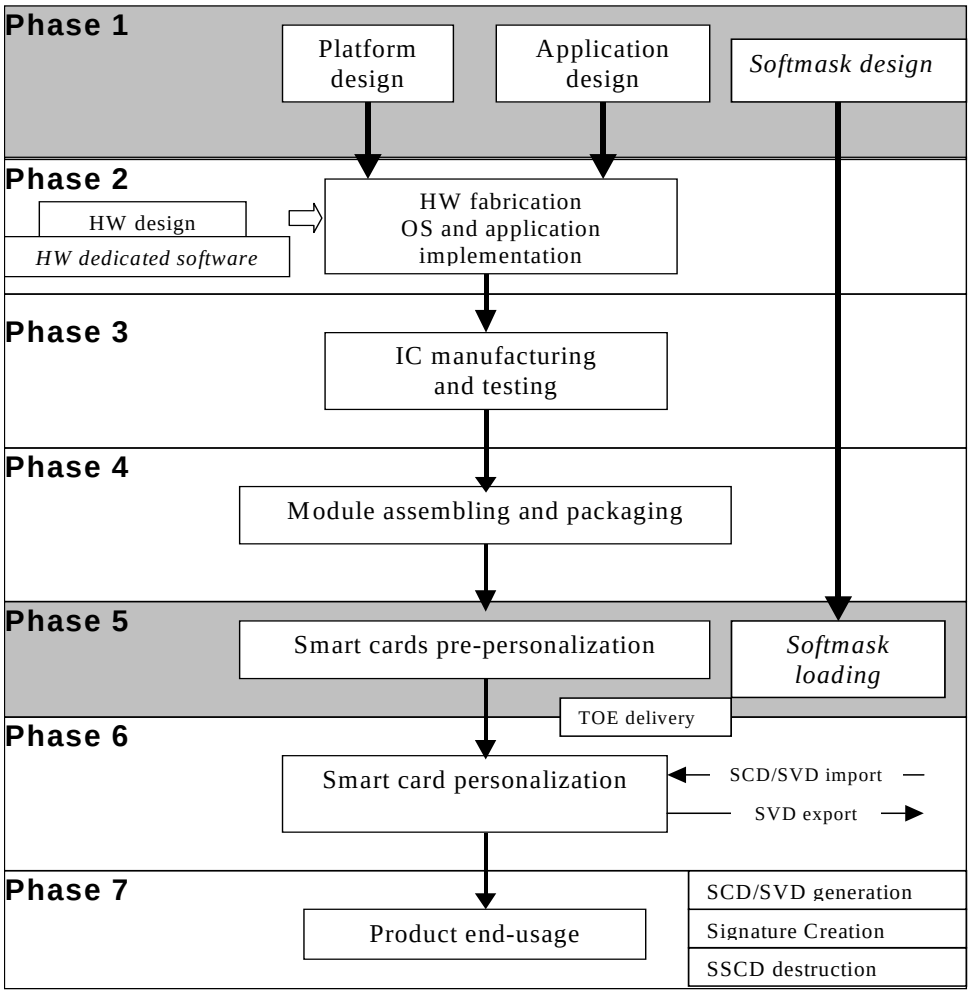

Figure 2. Product Life Cycle

The global security requirements of the TOE mandate to consider, during the development phase, the threats to security occurring in the other phases. Therefore, this ST addresses the functions used in the phases 6 and 7 but developed during the phases 1 to 5. The limits of the evaluation process

correspond to phases 1 to 5 including the TOE under development delivery from the party responsible of each phase to the parties responsible of the following phases.

These different phases may be performed at different sites. This implies that procedures on the delivery process of the TOE must exist and be applied for every delivery within a phase or between phases. This includes any kind of delivery performed from phase 1 to 5 to subsequent phases, including:

- Intermediate delivery of the TOE or the TOE under construction within a phase,
- Delivery of the TOE or the TOE under construction from one phase to the next.

These procedures must be compliant with the security assurance requirements developed in TOE "Security Assurance Requirements" section.

2.2.1 TOE Phases

2.2.1.1 TOE Actors & roles

For the signature application, two roles have been identified, the Administrator and the Signatory.

1. The Administrator acts during the personalization phase (phase 6). (S)he creates the Signatory's PIN and optionally imports the first SCD into the TOE.
2. The Signatory that owns the TOE is the End-User in the usage phase (phase 7). (S)he can sign, destroy the SCD and generate a new SCD/SVD pair.

2.2.1.2 Smart Card product life cycle

The Smart card product life cycle, as defined in [PP/BSI-0002], is split up into 7 phases where the following authorities are involved:

Phase 1	Smart Card software development	The embedded software developer is responsible for the development of the OS (MultiApp) and the application (IAS Classic) as well as the corrective softmask if necessary.
Phase 2	IC design, IC database construction and IC photomask fabrication	The IC manufacturer is responsible for these operations, taking as an input the embedded software data given by Embedded Software developer.
Phase 3	IC manufacturing and testing	The IC manufacturer is responsible for producing and testing the IC through three main steps: IC manufacturing, testing, and IC pre-personalisation.
Phase 4	Module assembling and packaging	The smart card product manufacturer is responsible for assembling the module and then, packaging the module in the plastic card.
Phase 5	Smart card pre-personalization	The smart card product manufacturer is responsible for the smart card initialization, for installing the application (if needed) and for testing, and the smart card pre-personalization. The corrective softmask is also load in this phase if necessary.
Phase 6	Smart card Personalization	The Personaliser is responsible for the IAS Classic personalization and for final tests. The IAS Classic application can also be installed in this phase.
Phase 7	Smart card Usage	The smart card issuer is responsible for the smart card product delivery to the smart card end-user, and for the end of life process.

Table 3. Smart Card Product Life cycle

2.3 TOE Environment

Considering the TOE, four types of environment are defined:

1. Development and production environment (phase 1 to 4),
2. Initialisation environment corresponding to smart card pre-personalization (phase 5) and personalization (phase 6),
3. Usage environment, during which the card generates the signatures on behalf of the end-user. The card also destructs and generates new SCD/SVD (phase 7),
4. End-of-life environment, during which the TOE is made inapt for the signature creation (end of the phase 7).

2.3.1 Development & Production Environment

The TOE described in this ST is developed in different places as indicated below:

IC design	Samsung Giheung (see [ST/SAMSUNG])
Software Design (MultiApp, IAS Classic)	Gemalto Meudon
Pre-personalization design	Gemalto Meudon
IC manufacturing	Samsung Giheung (see [ST/SAMSUNG])
Module assembling	Gemalto Gemenos (or Pont-Audemer)
Module packaging	Gemalto Vantaa (or Gemenos)
Pre-personalization	Gemalto Vantaa (or Gemenos)

The IC development and production are protected as decribed in the ST of the IC [ST/SAMSUNG]. A transport key protects the IC delivery from Samsung to Gemalto. We are only interested below in the software aspect of the TOE.

In order to ensure security, the environment in which the development takes place must be made secure with access control tracing entries. Furthermore, it is important that all authorized personnel feels involved and fully understands the importance and the rigid implementation of the defined security procedures.

The development begins with the TOE specification. All parties in contact with sensitive information are required to abide by Non-disclosure Agreement (NDA).

Design and development of the embedded software then follows. The engineers use a secure computer system (preventing unauthorised access) to make the conception, design, implementation, and test performances. Storage of sensitive documents, databases on tapes, diskettes, and printed circuit layout information are in appropriately locked cupboards/safe. Of paramount importance also is the disposal of unwanted data (complete electronic erasures) and documents (e.g. shredding).

Testing, programming and deliveries of the TOE then take place. When these are done offsite, they must be transported and worked on in a secure environment with accountability and traceability of all (good and bad) products. During the electronic transfer of sensitive data, procedures must be established to ensure that the data arrive, only at the destination and is not accessible at intermediate stages (e.g. stored on a buffer server where system administrators make backup copies). It must also be ensured that transfer is done without modification or alteration.

During the TOE fabrication (phases 3 and 4), all people involved in storage and transportation operations must fully understand the importance of the defined security procedures. Moreover, the environment in which these operations take place must be secured.

The TOE initialisation is performed by Samsung Giheung (phase 3) and Gemalto Vantaa/Gemenos (phase 4) and Gemenos/Pont-Audemer (phase 5). In the initialisation environment of the TOE, smart card pre-personalization takes place (phase 5). During smart card pre-personalisation, the application

data structure is created. The initialisation requires a secure environment, which guarantees the integrity and confidentiality of operations.

2.3.2 Usage Environment

In the usage environment, the personalization takes place (phase 6). Additional data may be loaded and the SCD may be imported. Then the TOE is issued to the end-user. Once delivered to the end user (phase 7), the TOE can generate the SCD/SVD key pair. The TOE then exports the public part of the key to the Certification Authority for certification.

The TOE is owned by the end-user and requires strict security rules. It is the responsibility of the TOE and of the signature protocols to ensure that the signature security requirements are met.

2.3.3 End-of-life Environment.

End-of-life must be considered for several reasons:

- The SCD can be compromised,
- The TOE can be stolen,
- The TOE physical support can come to the end of its useful life.

In all these cases, it must be ensured that the TOE cannot be used any more for signature creation.

2.4 The actors and roles

The actors can be divided in:

Developers

The IC designer and Dedicated Software (DS) developer designs the chip and its DS. For this TOE, it is Samsung.

The Embedded Software developer designs the OS according to IC/DS specifications, the IAS Classic application and the corrective softmask if necessary. For this TOE, it is GEMALTO.

Manufacturers

The IC manufacturer -or founder- designs the photomask, manufactures the IC with its DS and hardmask from the Product Developer. For this TOE, the founder is Samsung.

The IC packaging manufacturer is responsible for assembling the modules using the ICs provided by the founder and then, for packaging the module in plastic cards. For this TOE, the IC packaging manufacturer is GEMALTO.

The smart card product manufacturer (or card manufacturer) is responsible to obtain a pre-personalized card from a packaged card. In the phase 5, the card manufacturer is also responsible for loading additional code belonging to the developer and manufacturer of the Card (the corrective softmask) if necessary. For this TOE, the smart card product manufacturer is GEMALTO.

Personalizer

The smart card personalizer personalizes the card by loading the cardholder data as well as cryptographic keys and PINs. The personalizer may also load card issuer applets during this phase. For this TOE, the personalizer may be GEMALTO or the card issuer.

At the end of this phase, no more applets can be loaded on the card (post-issuance is not allowed). The card is issued in SECURED state.

Card Issuer, Administrator

The card issuer -short named "issuer"- is a national administration. They issue cards to the citizens who are the cardholders. The card issuer has also the role of Administrator. Therefore, the card issuer is responsible for selecting and managing the personalization, for managing applets (load, install and delete), for creating the cardholder's PIN, for optionally importing the first SCD into the TOE, as well as for distribution and invalidation of the card.

End-user, Signatory

The Signatory is the end-user in the usage phase (phase 7) and owns the TOE. The card is personalized with their identification and secrets. The Signatory can sign, destroy the SCD and generate a new SCD/SVD pair.

The roles (administration and usage) are defined in the following tables.

Phase	Administrator	Environment
6 and 7	Card Issuer	Personalization and Usage Environment

Phase	User	Environment
7	Signatory	Usage Environment

During the delivery between phases the responsibility is transferred from the current phase administrator to the next phase administrator.

2.5 TOE intended usage

The use cases are depicted in the following figure. The main use case is the electronic signature. Some other use cases are possible, but as they are based on non-evaluated features of the TOE.

The product guidances provide additional information on the TOE administration, configuration or usage. For instance, the optional secure channel between card and PC may be used to protect operations as signature and decryption unless the environment ensures equivalent protection. Also, the guidance provides the minimum IAS Classic personalisation in order to obtain a SSCD configuration.

2.5.1 Evaluated main use cases: signatory and administrator authentication

a. Signatory authenticates to the TOE using their PIN code.
b. Administrator authenticates to the TOE using symmetric scheme (with TDES) or asymmetric scheme (with Diffie-Hellman). After a successful authentication, a secure channel is set up between the TOE and the administrator.

Both these authentication mechanisms are described in the user's manual of the IAS Classic applet.

2.5.2 Evaluated main use cases: Signature

a. SCD import:
1. The SCA authenticates itself to the TOE.
2. The signatory authenticates to the TOE (see above).
3. The signatory requests the import of SCD from a SSCD Type 1 device.
4. The SCD is imported to the TOE.
5. The CGA generates the certificate for the corresponding SVD and sends it ot the TOE.

b. SCD/SVD Key generation:
1. The SCA authenticates itself to the TOE.
2. The signatory authenticates to the TOE.
3. The signatory requests the generation of a SCD / SVD key pair
4. The SCD / SVD is generated in the TOE; the old SCD / SVD key pair is made unavailable.
5. The new SVD is sent to the CGA.
6. The CGA generates the certificate and sends it to the TOE.

c. Signature creation:
1. The SCA authenticates itself to the TOE.
2. The signatory authenticates to the TOE.

3. The signatory sends the DTBS to the TOE through the SCA.
4. The TOE computes the signature.
5. The TOE sends the signature to the SCA.

2.5.3 Evaluated support use cases: Security object system

The card manages a security object system allowing management of access conditions, and cryptographic operations. It is implemented using Security Data Objects (SDO). Each SDO contains in its header its access policy. There is a particular type of SDO which is the security environment (SE) saved in EEPROM. These Ses hold the security policy of the card.

The card is able to import, store and export security object in the security object system. Especially signatory security objects (symmetric keys and Diffie-Hellman data) are stored for authentication purpose.

2.5.4 Use cases outside the evaluation scope

The following use-cases are provided by the card but are not evaluated.

2.5.4.1 File storage

The card manages a file system allowing file creation, modification and deletion. The supporting file types are: Root, Dedicated File (DF) and transparent elementary file (EF).

The supported operations on DF files are: creation, selection and deletion.
The supported operations on EF files are: read binary, update binary, file selection and file deletion.

The card is able to import, store and export data in the file system. The information stored in files is mainly used for signatory identification.

2.5.4.2 Certficate verification

Using the stored root certificate, the card may verify the anthenticity of a certificate sent from an external entity.

2.5.4.3 Ciphering and deciphering use

The card offers a deciphering service using symmetric (TDES) or asymmetric scheme (RSA).

3 Conformance claims

3.1 CC conformance claim

The compliance is assumed with Common Criteria version V2.3 (ISO 15408) ([CC-1], [CC-2], [CC-3]).

This product is a secure signature creation device compliant to the Protection Profile CEN SSCD [PP/SSCD-TYPE2]/[PP/SSCD-TYPE3]. This device uses a certified chip conformant to the Protection Profile SSVG (also known as PP/BSI-0002) from Eurosmart, providing the necessary security so that value added applications can be safely loaded and executed on card without harming the electronic signature application.

3.2 PP claim, Package claim

This ST is CC V2.3 conformant with Part 3 conformant and EAL4 augmented as stated in [PP/SSCD-TYPE2]/[PP/SSCD-TYPE3], [PP/BSI-0002].

The assurance level for this product is EAL4 augmented by:

- ADV_IMP.2 (Developmement – Implementation of the FSP)
- ALC_DVS.2 (Sufficiency of security measures)
- AVA_MSU.3 (Analysis and testing for insecure states)
- AVA_VLA.4 (Highly resistant)

The strength level for the TOE security functional requirements is "SOF high" (Strength Of Functions high).

3.3 Conformance rationale

This ST is conformant with [CC-2] extended due to additional components as stated in Protection Profile [PP/SSCD-TYPE2], [PP/SSCD-TYPE3] and [PP/BSI-0002].
This ST is conformant with [CC-3] augmented due to augmentation given in [PP/SSCD-TYPE2], [PP/SSCD-TYPE3] and [PP/BSI-0002].
The [ST/SAMSUNG] refines the assets, threats, objectives and SFR of [PP/BSI-0002] see BSI certificate and certification report.
The current ST refines the assets, threats, objectives and SFR of [PP/SSCD-TYPE2], [PP/SSCD-TYPE3] and [PP/BSI-0002].

3.4 PP reference

[PP/SSCD-TYPE2], [PP/SSCD-TYPE3] and [PP/BSI-0002] are claimed.

3.5 PP refinements

Refinements of [PP/BSI-0002] are described in [ST/SAMSUNG] and are not repeated here. The table below shows the functional requirements refined in PP and in ST.

FMT_SMF functional requirement is added to [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] to be compliant with the CC version 2.3.

Functional requirement	Refined in [PP/SSCD-TYPE2]	Refined in [PP/SSCD-TYPE3]	Refined in this ST
FCS_CKM.1		_	x
FCS_CKM.4	_	_	x
FCS_COP.1	x	x	x
FDP_ACC.1	x	x	(x)
FDP_ACF.1	x	x	x
FDP_ETC.1	x	x	(x)
FDP_ITC.1	x	x	(x)
FDP_RIP.1	x	x	(x)
FDP_SDI.2	x	x	(x)
FDP_UCT.1	x		(x)
FDP_UIT.1	x	x	(x)
FIA_AFL.1	x	x	x
FIA_ATD.1	x	x	(x)
FIA_UAU.1	x	x	x
FIA_UID.1	x	x	x
FMT_MOF.1	x	x	(x)
FMT_MSA.1	x	x	(x)
FMT_MSA.2	NA	NA	NA
FMT_MSA.3	x	x	(x)
FMT_MTD.1	x	x	(x)
FMT_SMR.1	x	x	(x)
FPT_AMT.1	_	_	x
FPT_EMSEC.1	_	_	x
FPT_FLS.1	_	_	x
FPT_PHP.1	NA	NA	NA
FPT_PHP.3	_	_	x
FPT_TST.1	_	_	x
FTP_ITC.1	x	x	(x)
FTP_TRP.1	x	x	x

The functional requirements are both refined in the claimed PP and in this ST. This section demonstrates the compatibility of the refinements done in both documents.

_: No refinement

(x): no additional refinement has been made in the ST.

NA: the functional requirement requires no refinement.

FCS_CKM.1: Cryptographic key generation

This functional requirement has been refined from [PP/SSCD-TYPE3] with a specific list of approved algorithms that gives the cryptographic key generation algorithms and key sizes used by the TOE.

FCS_CKM.4: Cryptographic key destruction

This functional requirement is refined from [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] with a description of the key destruction method used that follows [no specific standard].

FCS_COP.1: Cryptographic operation

This functional requirement partially refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] has been completed in the ST with a specific list of cryptographic algorithms and key sizes that are used by the TOE. Furthermore, two iterations have been added, one for Hashing and one for the MAC computation.

FDP_ACC.1: Subset access control

This functional requirement is already refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] and no other refinement has been added in the ST.

FDP_ACF.1: Security based access control functions

This functional requirement is already refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3]. Additional refinement is done in the ST.

FDP_ETC.1: Export of user data without security attributes

This functional requirement is already refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] and no other refinement has been added in the ST.

FDP_ITC.1: Import of user data without security attributes

This functional requirement is already refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] and no other refinement has been added in the ST.

FDP_RIP.1: Subset residual information protection

This functional requirement is already refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] and no other refinement has been added in the ST.

FDP_SDI.2: Stored data integrity monitoring and action

This functional requirement is already refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] and no other refinement has been added in the ST.

FDP_UCT.1 Basic data exchange confidentiality

This functional requirement is already refined in [PP/SSCD-TYPE2] and no other refinement has been added in the ST.

FDP_UIT.1: Data exchange integrity

This functional requirement is already refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] and no other refinement has been added in the ST.

FIA_AFL.1: Basic authentication failure handling

This functional requirement is partially refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3]. In the ST the number of authentication failures has been refined.

FIA_ATD.1: User attribute definition

This functional requirement is already refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] and no other refinement has been added in the ST.

FIA_UAU.1: Timing of authentication

This functional requirement is already refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3]. Additional refinement is done in the ST.

FIA_UID.1: Timing of identification

This functional requirement is already refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3]. Additional refinement is done in the ST.

FMT_MOF.1: Management of security functions behavior

This functional requirement is already refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] and no other refinement has been added in the ST.

FMT_MSA.1: Management of security attributes

This functional requirement is already refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] and no other refinement has been added in the ST.

FMT_MSA.2: Secure security attributes

There is no refinement required for this security requirement.

FMT_MSA.3: Static attributes initialization

This functional requirement is already refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] and no other refinement has been added in the ST.

FMT_MTD.1: Management of TSF data

This functional requirement is already refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] and no other refinement has been added in the ST.

FMT_SMF.1: Specification of Management

This functional requirement is added to [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] in order to fulfill dependencies of CC.

FMT_SMR.1: Security roles

This functional requirement is already refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] and no other refinement has been added in the ST.

FPT_AMT.1: Abstract machine testing

This functional requirement is not refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] and is entirely refined in the ST.

FPT_EMSEC.1: TOE emanation

This functional requirement, extended from CC is not refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3]. It is entirely refined in the ST.

FPT_FLS.1: Failure with preservation of secure state

This functional requirement is not refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] and is entirely refined in the ST.

FPT_PHP.1: Passive detection of physical attacks

There is no refinement required for this security requirement.

FPT_PHP.3: Resistance to physical attack

This functional requirement is not refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] and is entirely refined in the ST.

FPT_TST.1: Testing

This functional requirement is not refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] and is entirely refined in the ST.

FTP_ITC.1: Inter-TSF trusted channel

This functional requirement is already refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3] and no other refinement has been added in the ST.

FTP_TRP.1: Trusted path

This functional requirement is partly refined in [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3]. Additional refinement is done in the ST.

3.6 PP additions

The table below shows the functional requirements refined in PP and in ST.

	Addition in ST
Assets	-
Threats	-
Assumptions	X
Organizational Security Policies	X
Security objectives for the TOE	-
Security objectives for the operational environment	X
Security functional requirements	X
security assurance requirements	-
Security Requirements for the IT Environment	-

3.7 Assurance requirements additional to the PP

There is no assurance requirement, which is not in [PP/SSCD-TYPE2], [PP/SSCD-TYPE3] or [PP/BSI-0002].

4 TOE Security Environment

4.1 Assets

The assets of the TOE are those defined in [PP/SSCD-TYPE2], [PP/SSCD-TYPE3] and those of the supporting platform. This Security Target deals with the assets of [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3]. The assets of the platformare defined in [ST_ PLTF].

D.SCD

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

D.SVD

The 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

PIN code 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

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

D.SSCD

Signature-creation function of the SSCD using the SCD: the quality of the function must be maintained so that it can participate in the legal validity of electronic signatures.

D.SIG

Electronic signature: unforgeabilty of electronic signatures must be assured.

4.2 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 initialisation, TOE personalisation or other TOE administrative functions.

S.Signatory

User who holds the TOE and uses it on his/her 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/her 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**.

4.3 Threats

T.Hack_Phys

Physical attacks through the TOE interfaces.

An attacker interacts with the TOE interfaces to exploit vulnerabilities, resulting in arbitrary security compromises.

T.SCD_Divulg

Storing, copying, and releasing of the signature-creation data.

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

T.SCD_Derive

Derive the signature-creation data.

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

T.Sig_Forgery

Forgery of the electronic signature

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

T.Sig_Repud

Repudiation of signatures.

If an attacker can successfully threaten any of the assets, then the non repudation of the electronic signature is compromised.

The signatory is able to deny having signed data using the SCD in the TOE under his control even if the signature is successfully verified with the SVD contained in his un-revoked certificate.

T.SVD_Forgery

Forgery of the signature-verification data.

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

T.DTBS_Forgery

Forgery of the DTBS-representation.

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

T.SigF_Misuse

Misuse of the signature-creation function of the TOE.

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

4.4 Organisational security policies

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, 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.

4.5 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

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 authorised users only

(e) The SSCD Type1 ensures the authenticity of the SVD it has created and exported.

4.5.1 Additional

These are assumptions additional to [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3].

A.Key_Mngt

Secure Key Management

The IT Environment SCA and CGA shall protect the confidentiality of the keys used for the secure communications with the TOE.

5 Security objectives

5.1 Security objectives for the TOE

This section describes the TOE objectives of [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3].

OT.SCD_Unique is an environment objective in Type 2.

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

Lifecycle security.

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

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.

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 the 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 provides 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 prevents or resists physical tampering with specified system devices and components.

OT.SCD_Transfer

Secure transfer of SCD between SSCD.

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

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 DTBSrepresentation 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 the 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.

OT.SCD_Unique

Uniqueness of the signature-creation data

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

Application note:

Type 3 TOE Objective.

OT.Init

SCD/SVD generation

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

Application note:

This is a Type 3 Objective.

5.2 Security objectives for the environment

The Objectives are those of Type 2 and Type 3 from PP/SSCD.

OE.SCD_SVD_Corresp

Correspondence between SVD and SCD

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

OE.SCD_Transfer

Secure transfer of SCD between SSCD

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

the SSCD Type2. The SCD shall be deleted from the SSCD Type1 whenever it is exported into the TOE.

OE.SCD_Unique

Uniqueness of the signature-creation data

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

OE.CGA_QCert

Generation of qualified certificates

The CGA generates qualified certificates which include inter alia

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

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

(c) the advanced signature of the CSP.

OE.SVD_Auth_CGA

CGA verifies the authenticity of the SVD

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

OE.HI_VAD

Protection of the VAD

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

OE.SCA_Data_Intend

Data intended to be signed

The SCA

(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 enables verification of the integrity of the DTBS-representation by the TOE

(c) attaches the signature produced by the TOE to the data or provides it separately.

5.2.1 Additional

These are environment objectives additional to [PP/SSCD-TYPE2] and [PP/SSCD-TYPE3].

OE.Key_Mngt

Secure management of the keys

The IT Environment SCA and CGA protect the confidentiality of the keys used for the secure communications with the TOE.

6 Security requirements

6.1 TOE security functional requirements

6.1.1 Security functional requirements list

Identification	DESCRIPTION
FCS	**Cryptographic support**
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP	**User data protection**
FDP_ACC.1	Subset Access control
FDP_ACF.1	Security attributes based access control
FDP_ETC.1	Export of user data without security attributes
FDP_ITC.1	Import of User Data without security attributes
FDP_RIP.1	Subset residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
FDP_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Basic data exchange integrity
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
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_SMR.1	Security roles
FMT_SMF.1	Specification of management functions
FPT	**Protection of the TOE Security function**
FPT_AMT.1	Abstract machine testing
FPT_EMSEC.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/Channel**
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	TOE Trusted path

Table 4. IAS Classic security functional requirements list

6.1.2 Cryptographic support (FCS)

FCS_CKM.1/RSA Cryptographic key generation

FCS_CKM.1.1/RSA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA key generation** and specified cryptographic key sizes **1024, 1152, 1280, 1536 and 2048 bits** that meet the following: **no standard.**

Application note:

Type 3 only.

FCS_CKM.4/SCD Cryptographic key destruction

FCS_CKM.4.1/SCD The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwrite the keys** that meets the following: **no standard**.

Application note:

The cryptographic key SCD will be destroyed on demand of the Signatory or Administrator.

The destruction of the SCD is mandatory before the SCD is re-imported into the TOE.

Type 2 (re-importation of SCD) and Type 3 (regeneration of a new SCD).

FCS_COP.1/CORRESP Cryptographic operation

FCS_COP.1.1/CORRESP The TSF shall perform **SCD/SVD correspondence verification** in accordance with a specified cryptographic algorithm **RSA key computation** and cryptographic key sizes **1024, 1152, 1280, 1536 or 2048 bits** that meet the following: **no standard**.

FCS_COP.1/SIGNING Cryptographic operation

FCS_COP.1.1/SIGNING The TSF shall perform **electronic signature-generation** in accordance with a specified cryptographic algorithm **[RSA]** and cryptographic key sizes **1024, 1152, 1280, 1536 or 2048 bits** that meet the following: **[PKCS#1] or [ISO9796-2] or [RFC2409]**.

6.1.3 User data protection (FDP)

6.1.3.1 Access control (FDP_ACC.1)

FDP_ACC.1/Initialisation SFP Subset access control

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

Application note:

Type 3 only.

FDP_ACC.1/SVD Transfer SFP Subset access control

FDP_ACC.1.1/SVD Transfer SFP The TSF shall enforce the **SVD Transfer SFP** on **export of SVD by User**.

FDP_ACC.1/SCD Import SFP Subset access control

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

FDP_ACC.1/Personalisation SFP Subset access control

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

FDP_ACC.1/Signature-creation SFP Subset access control

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

1. **sending of DTBS-representation by SCA,**
2. **signing of DTBS-representation by Signatory**.

6.1.3.2 Security attributes (FDP_ACF.1)

The security attributes for the user, TOE components and related status are:

User, subject or object the attribute is associated with	Attribute	Status
General attribute		
User	Role	Administrator, Signatory
Initialisation attribute group		
User	SCD / SVD management	authorised, not authorised
SCD	Secure SCD import allowed	no, yes
Signature-creation attribute group		
SCD	SCD operational	no, yes
DTBS	sent by an authorised SCA	no, yes

(see tables in §5.1.2.2 of PP SSCD Type 2 and 3 - Security attribute based access control)

FDP_ACF.1/Initialisation SFP Security attribute based access control

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

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

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

FDP_ACF.1.4/Initialisation SFP The TSF shall explicitly deny access of subjects to objects based on the **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**.

Application note:

Type 3 only.

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

FDP_ACF.1.1/SVD Transfer SFP The TSF shall enforce the **SVD Transfer SFP** to objects based on the following: **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 the 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 authorise 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 **none**.

Application note:

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

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

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

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

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

FDP_ACF.1.4/SCD Import SFP The TSF shall explicitly deny access of subjects to objects based on the **(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 authorised" is not allowed to import 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 "authorised" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "no".

Application note:

Type 2 only.

FDP_ACF.1/Personalisation SFP Security attribute based access control

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

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

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

FDP_ACF.1.4/Personalisation SFP The TSF shall explicitly deny access of subjects to objects based on the **none**.

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

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

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

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

FDP_ACF.1.4/Signature-creation SFP The TSF shall explicitly deny access of subjects to objects based on the **(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 authorised 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 authorised SCA with SCD by the Signatory which security attribute "SCD operational" is set to "no".

6.1.3.3 Export of User Data (FDP_ETC.1)

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

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

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

Application note:

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

6.1.3.4 Import of User Data (FDP_ITC.1)

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

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

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

FDP_ITC.1.3/SCD 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 authorised SSCD**.

Application note:

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

Type 2 only.

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

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

Application note:

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

6.1.3.5 Residual Information Protection (FDP_RIP.1)

FDP_RIP.1 Subset residual information protection

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

6.1.3.6 Stored data integrity monitoring and action (FDP_SDI.2)

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

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

FDP_SDI.2/Persistent Stored data integrity monitoring and action

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

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

1. prohibit the use of the altered data

2. inform the Signatory about integrity error.

FDP_SDI.2/DTBS Stored data integrity monitoring and action

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

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

1. **prohibit the use of the altered data**
2. **inform the Signatory about integrity error**.

Global refinement:

The DTBS-representation temporarily stored by TOE has the user data attribute "integrity checked stored data".

6.1.3.7 Basic data exchange confidentiality (FDP_UCT.1)

FDP_UCT.1/Receiver Basic data exchange confidentiality

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

Application note:

Type 2 only.

6.1.3.8 Data exchange integrity (FDP_UIT.1)

FDP_UIT.1/SVD Transfer Data exchange integrity

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

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

Non editorial refinement:

SVD Transfer SFP will be required only if the TOE holds the SVD and the SVD is exported to the CGA for certification.

FDP_UIT.1/TOE DTBS Data exchange integrity

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

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

6.1.4 Identification and authentication (FIA)

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when

- **3 (for 5-digit RAD) or**
- **5 (for 6-digit RAD)**

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

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

FIA_ATD.1 User attribute definition

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

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

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

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

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

Application note:

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

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

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

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

6.1.5 Security management (FMT)

FMT_MOF.1 Management of security functions behaviour

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

FMT_MSA.1/Administrator Management of security attributes

FMT_MSA.1.1/Administrator The TSF shall enforce the **SCD Import SFP and Initialisation SFP** to restrict the ability to **modify** the security attributes **SCD / SVD management and secure SCD import allowed** to **Administrator**.

Application note:

The SCD Import SFP enforcing comes from Type 2.

The Initialisation SFP enforcing comes from Type 3.

FMT_MSA.1/Signatory Management of security attributes

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

FMT_MSA.2 Secure security attributes

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

FMT_MSA.3/Type2 Static attribute initialisation

FMT_MSA.3.1/Type2 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.

Non editorial refinement:

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

FMT_MSA.3.2/Type2 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/Type3 Static attribute initialisation

FMT_MSA.3.1/Type3 The TSF shall enforce the **Initialisation SFP and Signature-creation SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

Non editorial refinement:

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

FMT_MSA.3.2/Type3 The TSF shall allow the **Administrator** to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

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

FMT_SMR.1 Security roles

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

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

6.1.6 Protection of the TSF (FPT)

FPT_AMT.1 Abstract machine testing

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

Global refinement:

In this document, the underlying abstract machine test is the IC and its crypto libraries.

FPT_EMSEC.1 TOE Emanation

FPT_EMSEC FPT_EMSEC.1.1 The TOE shall not emit **Side channel current** in excess of **State of the art limits** enabling access to **RAD and SCD**.

FPT_EMSEC.1.2 The TSF shall ensure **all users** are unable to use the following interface **external contacts** to gain access to **RAD and SCD**.

Application note:

The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission.

Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: **power shortage, over and under voltage, over and under clock frequency, over and under temperature, integrity problems**, **unexpected abortion of the execution of the TSF due to external events.**

FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist **voltage, clock frequency and temperature out of bounds as well as penetration attacks** to the **integrated circuit** by responding automatically such that the TSP is not violated.

FPT_TST.1 TSF testing

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

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

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

FTP_ITC.1/SCD Import Inter-TSF trusted channel

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

FTP_ITC.1.3/SCD Import [Editorially Refined] The TSF or the trusted IT shall initiate communication via the trusted channel for **SCD import**.

Non editorial refinement:

The mentioned remote trusted IT product is a SSCD of type 1.

Application note:

Type 2 only.

FTP_ITC.1/SVD Transfer Inter-TSF trusted channel

FTP_ITC.1.1/SVD Transfer 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 The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/SVD Transfer [Editorially Refined] The TSF or the trusted IT shall initiate communication via the trusted channel for **transfer of SVD**.

Non editorial refinement:

The mentioned remote trusted IT product is a SSCD of type 1 for SVD import and the CGA for the SVD export.

Application note:

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

FTP_ITC.1/DTBS Import Inter-TSF trusted channel

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

Non editorial refinement:

The remote trusted IT product is the SCA.

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

FTP_TRP.1/TOE Trusted path

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

6.1.7 Additional

6.1.7.1 Cryptographic support (FCS)

Exchanging a shared secret in the external authentication (in usage phase) is done by Diffie-Hellman protocol. The secret is used to generate two session keys for secure messaging.

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1/DH The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Diffie-Helman 1024** and specified cryptographic key sizes **160 bits** that meet the following: **no standard.**

FCS_CKM.1.1/TDES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **IAS Ref. Manual, page 61** and specified cryptographic key sizes **112 bits** that meet the following: **no standard.**

FCS_COP.1 Cryptographic operation

FCS_COP.1.1/MAC The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic algorithm **ANSI X9.19 (Retail MAC)** and cryptographic key sizes **112 bits** that meet the following: **IAS Ref. Manual, page 44.**

6.1.7.2 Security management (FMT)

This SFR is added for compliancy with CC version 2.3; it misses from the PP SSCD.

FMT_SMF.1 Specification of management functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **Identification and authentication management, access condition management**.

6.2 Security requirements for the IT environment

6.2.1 SSCD Type1

This group only comes from the PP SSCD Type 2 and therefore only applies to it. The TSF in this section is the IT environment (the TSF of a SSCD Type1 TOE).

FCS_CKM.1/Type1 Cryptographic key generation

FCS_CKM.1.1/Type1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA key generation** and specified cryptographic key sizes **1024, 1152, 1280, 1536 or 2048 bits** that meet the following: **none**.

FCS_CKM.4/Type1 Cryptographic key destruction

FCS_CKM.4.1/Type1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **making the stored key value unavailable** that meets the following: **no standard**.

Application note:

The cryptographic key SCD will be destroyed automatically after export.

FCS_COP.1/CORRESP-Type1 Cryptographic operation

FCS_COP.1.1/CORRESP-Type1 The TSF shall perform **SCD/SVD correspondence verification** in accordance with a specified cryptographic algorithm **RSA key computation** and cryptographic key sizes **1024, 1152, 1280, 1536 or 2048 bits** that meet the following: **no standard**.

FDP_ACC.1/SCD Export SFP Subset access control

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

FDP_UCT.1/Sender Basic data exchange confidentiality

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

FTP_ITC.1/SCD Export Inter-TSF trusted channel

FTP_ITC.1.1/SCD Export The TSF shall provide a communication channel between itself and 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 remote trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/SCD Export [Editorially Refined] The TSF or the SSCD Type2 shall initiate communication via the trusted channel for **SCD export**.

Non editorial refinement:

The mentioned remote trusted IT product is a SSCD Type2.

Application note:

If the SSCD Type 1 exports the SVD to a SSCD Type2 and the SSCD Type 2 holds the SVD then the trusted channel between the SSCD Type 1 and the SSCD Type 2 will be required.

6.2.2 Certification generation application (GGA)

FCS_CKM.2/CGA Cryptographic key distribution

FCS_CKM.2.1/CGA The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **qualified certificate** that meets the following: **TDES 112 bits or Diffie-Hellman 1024.**

FCS_CKM.3/CGA Cryptographic key access

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: **no standard**.

FDP_UIT.1/SVD Import Data exchange integrity

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.

FTP_ITC.1/SVD Import Inter-TSF trusted channel

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

FTP_ITC.1.3/SVD Import [Editorially Refined] The TSF or the remote trusted IT product shall initiate communication via the trusted channel for **import SVD**.

6.2.3 Signature creation application (SCA)

FCS_COP.1/SCA Hash Cryptographic operation

FCS_COP.1.1/SCA Hash The TSF shall perform **hashing the DTBS** in accordance with a specified cryptographic algorithm **SHA-1 or SHA-256** and cryptographic key sizes **none** that meet the following: **[FIPS 180-2],** hash **length = 160 or 256 bits**.

FDP_UIT.1/SCA DTBS Data exchange integrity

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

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

FTP_ITC.1/SCA DTBS Inter-TSF trusted channel

FTP_ITC.1.1/SCA DTBS The TSF shall provide a communication channel between itself and 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 [Editorially Refined] The TSF or the remote trusted IT product shall initiate communication via the trusted channel for **signing DTBS-representation by means of the SSCD**.

FTP_TRP.1/SCA Trusted path

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

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

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

6.3 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.

7 TOE summary specification

The security functions provided by the IC are described in [ST/SAMSUNG]. The security functions provided by the platform are described in [ST_PLTF].

This section presents the security functions provided by the IAS Classic applet.

Identification	Name
SF_SIG_AUTHENTICATION	Authentication management
SF_SIG_CRYPTO	Cryptography management
SF_SIG_INTEGRITY	Integrity monitoring
SF_SIG_MANAGEMENT	Operation management and access control
SF_SIG_SECURE_MESSAGING	Secure messaging management

Table 5. TOE security functions list

7.1 SF_SIG_AUTHENTICATION: Authentication management

This security function manages the authentication mechanisms such as:

- Authentication operations for role management (i.e. PIN verification)
- Authentication operations for secure channel management (i.e. external authentication with symmetric and asymmetric schemes).

This security function:

- Manages authentication failure: when the **3 (for 5-digit RAD) or 5 (for 6-digit RAD)** unsuccessful authentication attempts has been met or surpassed, the TSF shall block D.RAD.
- Manage the asset D.RAD.
- Handles the authentications (for opening a secure channel) during the personalization and application phases.

This SF allows the following operations to be performed before the user is authenticated:

- Identification of 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 Type 1 for D.SCD import

This function is supported by the platform security function SF_CARD_AUTHENTICATION.

7.2 SF_SIG_CRYPTO: Cryptography management

This function manages the cryptographic operations of the electronic signature application:

- Key generation and correspondence verification (for RSA keypairs)
- Key destruction
- Perform cryptographic operations

This function is supported by platform security function SF_CARD_CRYPTO that provides cryptographic algorithms TDES, RSA and RNG and ensures that D.SCD information is made unavailable after use (key destruction).

7.3 SF_SIG_INTEGRITY: Integrity monitoring

This SF monitors the integrity of sensitive user data and the integrity of the DTBS. The integrity of persistently stored data such as 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, and
- Inform the S.Signatory about integrity error.

This SF also monitors the integrity of the access conditions of created data objects.

7.4 SF_SIG_MANAGEMENT: operation management and access control

This SF provides application operation management and access control.

Operation management
This SF manages the electronic signature application during its initialization and operation. This SF manages the security environment of the application and:
- Maintains the roles S.Signatory, S.Admin.
- Controls if the authentication required for a specific operation has been performed with success.
- Manages restriction to security function access and to security attribute modification.
- Ensures that only secure values are accepted for security attributes.

This SF restricts the ability to perform the function **Signature-creation SFP** to S.Signatory. This SF ensures that only S.Admin is authorized to
- Modify **Initialization SFP** and **Signature-creation SFP** attributes
- Specify alternative default values

Access control
This SF provides the electronic signature application with access control and ensures that the following operations are executed by authorized roles:
- Export of D.SVD by S.User
- Import of D.SCD by S.User
- Generation of D.SCD/D.SVD pair by S.User
- Creation of D.RAD by S.Admin
- Signing of D.DTBS-representation by S.Signatory

This SF provides access control to data objects.

This SF enforces the security policy on the import and the export of user data on:
- **SVD Transfer SFP:** D.SVD shall be sent to an authenticated CGA.
- **Signature-creation SFP**: D.DTBS shall be sent by an authenticated SCA.

7.5 SF_SIG_SECURE_MESSAGING: secure messaging management

This SF ensures the integrity and the confidentiality of exchanged user data.

This SF ensures that the TSF is able to
- Receive D.SCD with protection from unauthorized disclosure.
- Transmit D.SVD with protection from modification and insertion errors.
- Receive D.DTBS with protection from modification, deletion and insertion errors.
- Determine on received user data whether modification, deletion or insertion has occurred.

This SF manages four modes of secure channel during the personalization phase
- No secure messaging
- Integrity mode
- Confidentiality mode

- Integrity and confidentiality mode

This SF is supported by the platform security function SF_CARD_SECURE_MESSAGING during the application personalization phase.

In the application phase, secure channel is opened by a mutual authentication with two modes:

- Integrity mode
- Integrity and confidentiality mode

Index

T

MODIFICATION SHEET

Date	Modifications	Author
April 23, 2009	Creating from evaluated ST (V1.6)	Quang-Huy Nguyen

END OF SECURITY TARGET