gemalto
security to be free

LINQUS USIM 128K Smartcard

ESIGN PKI Signature Application

On GemXplore Generations G152B-EP3B OS platform,
Running on Infineon SLE88CFX4002P/m8834b17 chip
Ref T1004530 A3 / Version 1.0

Common Criteria V2.3
Security Target – Public version
EAL4+

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

1.1 Security Target Identification

Title:	LINQUS USIM 128K Smartcard: ESIGN PKI Signature Application Security Target
Reference:	ASE10448_Public
Version:	1.0
Date of creation:	10/10/2008
Author:	GEMALTO
TOE:	ESIGN PKI signature application on GemXplore Generations G152B-EP3B OS platform, running on Infineon SLE88CFX4002P/m8834b17 chip; Ref T1004530 A3 / Version 1.0
TOE version:	1.0
Product:	Linqus USIM 128K smartcard
IT Security Certification scheme:	DCSSI

This ST has been built with:

Common Criteria for Information Technology Security Evaluation Version 2.3 (ISO 15408), August 2005 which comprises [CCPART1], [CCPART2], and [CCPART3]

1.2 Security Target Overview

The Target of Evaluation (TOE) is the E-SIGN application and the functionalities/services provided by the GXG software to the E-SIGN application with the Infineon device SLE88CFX4002P/m8834b17 identified in the BSI certificate BSI-DSZ-CC-0269-2006.

The product Linqus USIM 128K is a smart card inserted in a Mobile (i.e. SIM). The SIM is used for network authentication and could embed others applications like PKI signature application E_SIGN. The E_SIGN application is an 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].

The TOE is a Secure Signature Creation Device [SCCD] that provides both SCD/SVD generation and Signature creation as described in the Protection Profile [PP SSCD3].

The product implements [JavaCard 2.2.1] and [GP2.1.1], and E-SIGN.

Part of the code is masked in ROM, the other part is in EEPROM, included the E-SIGN applet.

The Gemalto **E-SIGN** 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 1024 bits.

The Target Of Evaluation defined in this Security Target is the Secure Signature Creation Device (SSCD) functionalities provided by the E-SIGN application, supported by the GXG JavaCard.

TOE Components	Version	Constructor
Micro Controller	SLE88CFX4002P/m8834b17 release b17	INFINEON
GXG JavaCard Embedded Software	GXG -G152B -EP3B	GEMALTO
Digital signature application (Applet)	E-SIGN	GEMALTO

Table 1 – GXG 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 during the 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 PP SSCD3) 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.
It is a composite evaluation.

The TOE provides a Digital Signature application and is based on certified PP SSCD Type 3.

The assurance level is EAL4 augmented with:

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

AVA_VLA.4 (Vulnerability Analysis-Highly resistant

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 a Smart Card that provides Digital Signature creation services.
As shown in Figure 1 the GXG Signature Card is composed of:

- The Integrated Circuit Infineon SLE88CFX4002P/m8834b17,
- The Embedded Software of the GXG JavaCard
- EEPROMed application E-SIGN digital signature application.

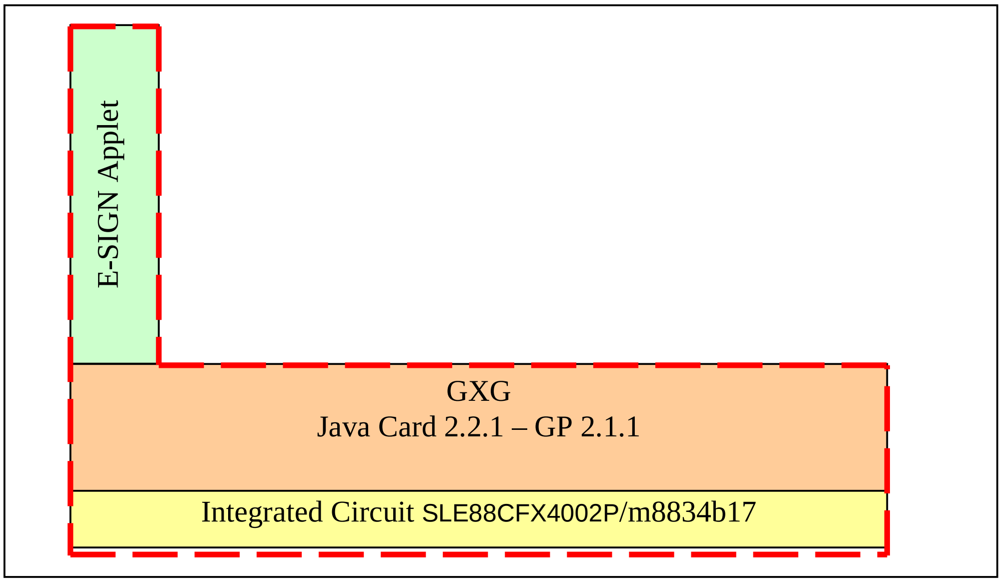
E-SIGN Applet
GXG
Java Card 2.2.1 – GP 2.1.1
Integrated Circuit SLE88CFX4002P/m8834b17

Figure 1 – GXG Digital Signature Card

- **The Integrated Circuit** is the SLE88CFX4002P/m8834b17, evaluated at EAL5+ level.
  The Integrated Circuit certificate reference is **BSI-DSZ-CC-0269-2006**
  The TOE Security Target is built using the Security Function provided by the Integrated Circuit and described in the Security Target reference : **SLE88CFX4000P /m8830 V1.3 – 25/04/2006 [IC-ST]**
  The evaluation of the GXG Digital Signature Card is built upon the results of the evaluation of the Integrated Circuit SLE88CFX4002P

- **GXG JavaCard**, implements latest standards:
  - **Java Card 2.2.1** (including all optional features: int, GC, 4 channels)
  - **Global platform 2.1.1** (including SCP02, delegated management, …)
  - **Full ETSI release 6**
  - **3GPP release 6**

- **E-SIGN** is the Digital Signature applet a Java Card type applet .
  It covers digital signature services. The Digital signature key size is 1024 bit.

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 E-SIGN, the GXG services available to install and support E-SIGN, and the Integrated Circuit SLE88CFX4002P that supports the GXG JavaCard.

The Integrated Circuit full description is available in the Security Target referenced **SLE88CFX4000P /m8830 V1.3 – 25/04/2006.**

The physical interfaces of the TOE are given in the table below:

Name	Short description	Type
VCC	Power supply line	Electrical interface
GND	Power supply line	Electrical interface
CLK	External clock line	Electrical interface
RES	Reset signal pad	Electrical interface
I/O	Data Pads	I/O interface
Temperature sensor	Environment interfaces	Physical Interface
Shield	Physical detectors	Physical Interface
Light UV sensors	Physical detectors	Physical interface
Glitch sensors	Physical detectors	Physical interface

The following sections describes GXG JavaCard and the E-SIGN signature applet.

2.2.1 GXG JavaCard description

The GXG is a JavaCard that implements major industry standards

- **Java Card 2.2.1** (including all optional features: int, GC, 4 channels)
- **Global Platform 2.1.1** (including SCP02, delegated management, …)
- **Full ETSI release 6**
- Maintain **backward compatibility : Full ETSI release 5**
- **3GPP Release 6**

The GXG Embeds (if necessary) **latest version of applications and browsers**

- SAT 4.3, WIB 1.3, WIM, BIP 2.1 (TBC)

The GXG **Support for multiple networks (2G, 3G, CDMA, …)**

- Implies several Network Access Applications working together
- Requires support for **dynamic switching** from 3G to 2G network

Each NAA is designed like a **plug-in.**

The JavaCard includes the following components:

- **The Ukos** layer 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 Kernel**, which provides a secure framework for the execution of Java Card programs and data access management (firewall).

- The **Java Telecom Environment** , which provides Network access applications, File system management, Toolkit services functionalities, and OTA services.

The GXG JavaCard architecture is described in Figure 2

The JavaCard is built upon the SLE88CFX4002P/m8834b17 IC with a 400K EEPROM size.

The GXG JavaCard will provide the following services:

- Initialization of the GP card Manager and management the GP Card Life Cycle,
- Secure installation of the application under Card Manager control during personalization phase,
- Secure Messaging services during Applet personalization
- Deletion of application instances under Card manager control during personalization phase
- 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
  Secure data object handling and backup mechanisms,
  Memory content management,
  Mechanisms to prohibit other applets to interfere with E-SIGN applet.

Once the smart-card is personalized, the card is closed.

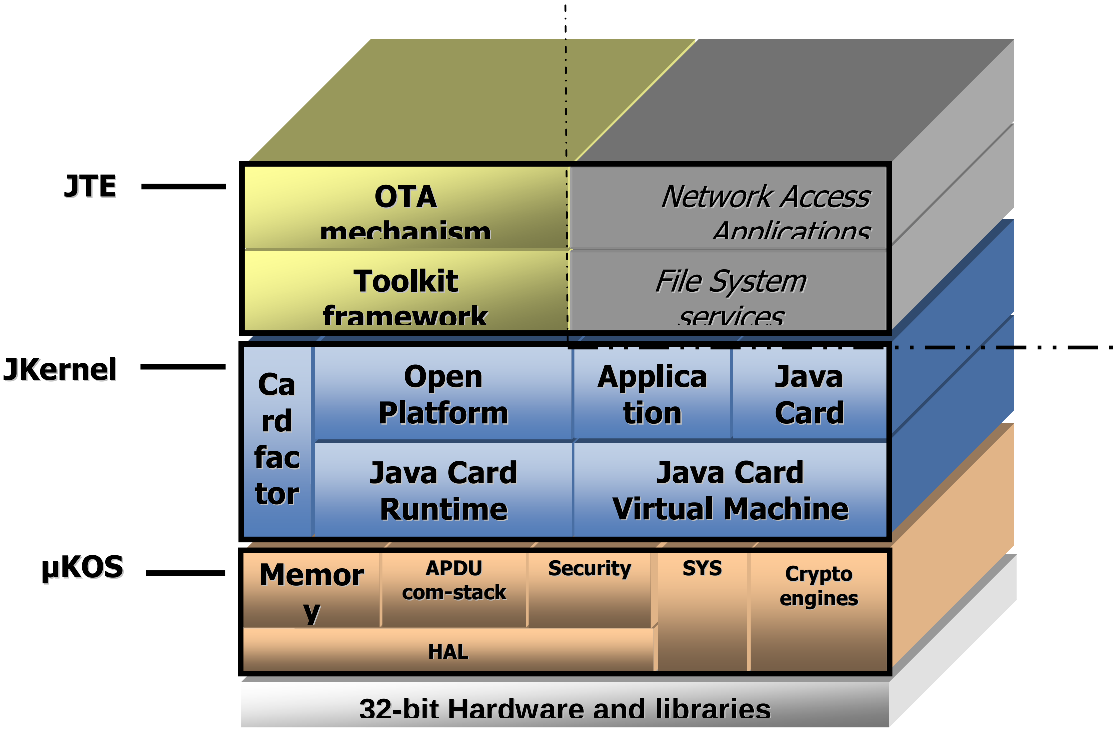

Figure 2 – GXG JavaCard architecture

The Target Of Evaluation defined in this Security Target is limited to the Secure Signature Creation Device (SSCD) functionalities provided by the E-SIGN application, supported by the GXG JavaCard services. Part of the JTE outside the dot line (grey color) on Figure 2 is not in the scope of the evaluation.

2.2.2 E-SIGN Applet description

E-SIGN 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 **E-SIGN** application is based to a TOE Type 3 and supports

- The generation of SCD/SVD pairs on-board [PP SSCD3].
- The generation of electronic signatures.

Regarding [PP SSCD3] document:

- The Certification generation application (CGA) is the operator. The Operator is in charge of final verification of Signatory identity and manages the WPKI platform. PKI activation is triggered by WPKI platform centrally. This consists of 03.48 OTA SMS. The CGAverify the authenticity of SVD generated and sent by the TOE.
- The Signature-creation application (SCA)is a set merchant site- operator in charge of performing the presentation of the DTBS to the signatory prior to the signature process according to the signatory's decision, sending a DTBS-representation to the TOE (using 03.48 OTA SMS), if the signatory indicates the intend to sign, and attaching the qualified electronic signature generated by the TOE to the data or providingthe qualified electronic signature as separate data..
- The administrator is the operator of in charge of WPKI platform.
- The signatory is the user of the Mobile who record to the service.

E-SIGN features the following options:

The purpose of the application is to use PKI features so that the user is able to sign, encrypt or make secure transactions using Public key/Private key generated in the SIM and stored securely within.

The applet is implemented in Java language, and it is interoperable, in order to ensure easy mounting on non-Gemalto cards compatible to JavaCard 2.2.1

The applet content is:

- OTA SMS reception
- Dynamic menu
- Key generation

- Key renewal
- Signing
- Modify PIN
- Retry PIN
- Reset PIN

PKI applet is triggered by 03.48 SMS for Key generation, Key renewal, Signing or Reset PIN. But Key generation can be launch by menu selection with dynamic menu mechanism.
Change PIN and Retry PIN features are embedded to allow PIN management.

The main purpose of the application is to use PKI features so that the user is able to sign, encrypt or make secure transactions using Public key/private key generated in the SIM and stored securely within.

User Registration
The user have to follow the registration process and following several off-line security controls, a Customer Call Center agent call him/her for final verification of identity. PKI activation is triggered by WPKI platform centrally. This consists of 03.48 OTA SMS.
Registration code is embedded inside the registration request (inside SMS) and is used to compare user registration code.
During this operation, the user is asked to choose a 6 digits secure user-signing PIN.
Once registration is successful, Key generation takes place and a certificate is generated using PKCS#10 format. Signed PKCS#10 certificate and SVD are sent via SMS.

Signing
The user is asked to sign with Display Text on the mobile after a request signature received by 03.48 OTA SMS. The hash to sign is displayed on the Mobile. The user is requested to enter PIN. If PIN is correct, the signature is computed and the signed hash is sent by SMS.
If the user has blocked PIN, he may have the possibility to try it 2 more times after verification of correct passcode stored in SIM at perso time.
NB: The passcode functionality is out of scope of this Security target.

2.3 TOE LIFE CYCLE

The TOE is composed of a JavaCard and a EEPROMed Java Card Applet.
The life cycle is described in table 2.

For this product, the JavaCard Software is masked partially in ROM during IC manufacturing where the rest of the OS and the applet are stored into EEPROM during Initialization/Personalization phase.

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 JavaCard and Digital signature application software, during phase 1. For this product, the developer is **GEMALTO**.

- The IC Manufacturer or founder- designs the IC during phase 2 and manufactures the Smart Card IC with part of 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,
  Loading part of the OS in EEPROM, Card initialization (loading of data and setting JavaCard to OP-READY state) during phase 5,
  Applet installation during phase 5.
  For this product the card manufacturer is **GEMALTO**

- The JavaCard 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 **GEMALTO.**

- The Applet Personalizer will
  Generate instance of the installed application,
  Load secret data as keys and PIN.
  This occurs also during phase 6. For this product, the JavaCard Personalizer and Applet Personalizer is **GEMALTO**

- 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, Operators, Private companies or governmental organizations.
  The card issuer is the subject S.admin defined in section 3.2

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 End User is the subject S.Signatory defined in section 3.2

2.3.2 Limits of the TOE

Table 2 presents the TOE product type life-cycle with the logical phases and related Card 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	Smart Card fabrication	Development	JavaCard Software	JavaCard design	*Product developer*	None	None
			Application	Applet design	*Application developer*	None	None
2	Smart Card fabrication	Development	Hard mask set	IC design	*IC manufacturer*	None	None
3	Smart Card fabrication	Production	Wafers with Chips	IC Initialization	*IC manufacturer*	none	noe
4	Smart Card fabrication	Production	Modules	IC Packaging	*Card manufacturer*	none	none
5	Smart Card fabrication	Production	Card with JavaCard software	EEPROM part of the OS Card Initialization	*Card manufacturer*	OP_READY INITIALIZED (SECURED)	
			And Applications	Applet Installed and selectable	Card manufacturer		INSTALLED SELECTABLE
6	Smart Card usage	Personalization	Card personalized	Card Personalization	*Platform Personalizer*	SECURED	INSTALLED SELECTABLE
			Applet personalized	Applet personalized	*Applet personalizer*		INSTALLED SELECTABLE
7	Smart Card usage	User – Use		Card Distribution Card Termination	*Card issuer* *End User*	SECURED LOCKED TERMINATED	SELECTABLE LOCKED

Table 2 – GXG E-SIGN Life Cycle

The TOE limits correspond to the Phase 1 to the phase 3.

The TOE provides security mechanisms to allow only authorized administrator to securely initialize and install and personalize the JavaCard and applets.
Secure configuration and set up of the TOE are specified in Administrator and User Guidance documents.

Logical phases of the JavaCard 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 Integration Circuit (phase 3), the manufacturing of the card (phase 4), the initialization of the JavaCard (phase 5) and the installation of the applet (phase 5), the test operations, and initialization of the JavaCard;
- Personalization environment corresponding to phase 6 including personalization and testing of the Open JavaCard with the user data, the personalization of the Applet.
- User environment corresponding to phase 7.

2.4.1 Development environment

2.4.1.1 Software development ((Phase 1)

This environment is limited to GEMALTO 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 GEMALTO 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 Munich and Graz sites.
The IC development environment is described in SLE88CFX4002P security target IC Security Target reference.

2.4.2 Production environment

2.4.2.1 IC initialization (Phases 3)

This environment is limited to INFINEON Dresden and Corbeil-Essonnes sites.
The IC development environment is described in SLE88CFX4002P security target IC Security Target reference.

2.4.2.2 IC Packaging (phase 4)

This environment is limited to GEMALTO Gemenos 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 GEMALTO 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 GEMALTO Gemenos 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 the Mobile and via OTA Platform.
The signatory will generate the SCD/SVD keys pair.
The signatory will export the public key (SVD)

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 JavaCard life cycle and the applet 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 JavaCard 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 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 during issuance. It should be notice that the TOE is closed (loading and deleting applet are not possible) during the state SECURED. The state transition from INITIALIZED to SECURED is irreversible.
  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 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 JavaCard 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 manager is fully operational. This phase is used to load additional personalization data.

2.5.4 Usage

2.5.4.1 JavaCard logical states

During usage phase the JavaCard 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

Applets are assigned Selectable, and Locked life cycle states as follows:
• **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 should 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.
• **LOCKED**
The state LOCKED is used as a security management control for the GlobalPlatform Runtime Environment or the off-card entity authenticated by the ISD to prevent the selection, and therefore the execution, of the application. If an application is in its LOCK state, only the ISD is allowed to unlock it, and the OPEN is in the role to ensure the Application Life Cycle returns to its previous state

2.6 TOE INTENDED USAGE

The TOE is dedicated to generate digital signature using a Mobile.

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.

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 (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).

According [CC-COMP] document the assets defined in [IC-ST] are also assets of the TOE defined in this Security Target.

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.

3.3 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.

3.4 ASSUMPTIONS

This section defines assumptions related to the Digital Signature application as stated in PP SSCD and as stated in [BSI-PP] for composite evaluation.

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.

3.5 ORGANIZATIONAL SECURITY POLICIES

This section defines OSPs related to the Digital Signature application as stated in PP SSCD3.

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.
P.IC_Usage	The Smartcard Embedded Software developers follows the IC guidance documents given by the IC manufacturer .
P.Gemalto_Security	All employees follows the security requirements for the materials and documentations given by the IC manufacturer .

4. TOE SECURITY OBJECTIVES

4.1 SECURITY OBJECTIVES FOR THE TOE

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 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 of re-generation
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.Init	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	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.

4.2 Security objectives for the 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.IC_Usage_and_Protection	The user guidance of the hardware (data-sheet, ….) are followed by the software developer. Gemalto people shall follows Security measures to ensure the confidentiality and the Integrity of the IC after delivery by the IC manufacturer until the IC is given to the End User.

5. IT SECURITY REQUIREMENTS

Security functional requirements components given in section 5.1 “TOE security functional requirements” excepting FPT_EMSEC.1 which is explicitly stated in [PP SSCD3], are drawn from [CCPART2]. FPT_TST.1.3 is concerning the integrity verification of the ESIGN applet code during the load of the applet.

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

5.1 SECURITY FUNCTIONAL REQUIREMENTS

5.1.1 security functional requirements list

Identification	DESCRIPTION
FCS	**Cryptographic support**
FCS_CKM.1 (option b)	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP	**User data protection**
FDP_ACC.1	Complete access control
FDP_ACF.1	Security attribute 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_UIT.1	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.	Management of security functions 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 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	Inter-TSF trusted channel

Table 3 – Digital signature Security Functional Requirements list

[(1)] This requirement is [CCPART2] extend.

5.1.2 FCS – Cryptographic support

5.1.2.1 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 and specified cryptographic key sizes that meet the following: List of approved algorithms and parameters. **Algorithm** | **Key size** | **Standard** **RSA with CRT key generation** | **1024** | **[JC2.2.1]**
FCS_CKM.1.1/DES	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **DES or 3-DES** and specified cryptographic key sizes **of single (64 bits) and double (128 bits) or triple length (192 bits)** that meet the following standards: **[GP2.1.1]**

5.1.2.2 FCS_CKM.4

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in case of regeneration of new SCD accordance with a specified cryptographic key destruction method: **clear and overwrite the key** that meets the following: **none**

Application notes:
The cryptographic key SCD will be destroyed on demand of the Signatory or Administrator. The destruction of the SCD is mandatory before the SCD/SVD pair is re-generated by the TOE.

5.1.3.2 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 **1024 bit** that meet the following: List of approved algorithms and parameters. **[JC2.2.1].**
FCS_COP.1.1/ SIGNING	The TSF shall perform digital signature generation in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1024 bit** that meet the following: List of approved algorithms and parameters **[JC2.2.1].**

FCS_COP.1.1/DES	The TSF shall perform **encryption and decryption operations** in 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**

5.1.3 FDP – User data protection

5.1.3.1 FDP_ACC.1

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

FDP_ACC.1.1/ Initialization SFP	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
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	The TSF shall enforce the initialization SFP to objects based on General attribute and Initialization attribute**.**
FDP_ACF.1.2 / Initialization SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The user with the security attribute “role” set to “Administrator” or set to “Signatory” and with the security attribute “SCD / SVD

	management" set to " authorised" is allowed to generate SCD/SVD pair.
FDP_ACF.1.3/ Initialization SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ Initialization SFP	The TSF shall explicitly deny access of subjects to objects based on the 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.

Note: For this TOE, SCD/SVD pair is generated by S.Signatory.

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.

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/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.

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.

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

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

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. Card is muted or terminated

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.Administrator about integrity error.

Application Note:

The integrity of D.DTBS is checked at the reception by the TOE before the signature operation. This SFR support the FDP_ITC.1.1/DTBS which ensures that DTBS is sent by authorized SCA. The administrator is informed if the Proof of Receipt is requested when the SMS is sent.

5.1.3.7 FDP_UIT.1

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 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 **3** unsuccessful authentication attempts occur related to consecutive failed authentication attempts **using RAD**.
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	The TSF shall allow[1. Identification of the user by means of TSF required FIA_UID.1 2. Establishing path between local user and the 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	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 path provided between the SGA in the TOE environment and the TOE

5.1.4.4 FIA_UID.1

FIA_UID.1.1	The TSF shall allow[1. Establishing a path between local user and the 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	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	The TSF shall enforce the Initialization SFP to restrict the ability to modify **[no other operation]** the security attributes SCD/SVD Management to Administrator .

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

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.

5.1.5.7 FMT_SMF.1

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: • **Enable Signature creation function (FMT_MOF.1),** • **Restrict ability to modify security attributes and TSF**

	data **(FMT_MSA.1.1 /Administrator** **FMT_MSA.1.1 / Signatory** **FMT_MTD1.1).**

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,** 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

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.

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

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

5.1.6.7 FPT_TST.1

FPT_TST.1.1	The TSF shall run a suite of self-tests **during initial startup** to demonstrate the correct operation of **part of TSF**.
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of **part 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 :** The integrity of the applet E-SIGN is ensured during the **load operation** by the usage of secure messaging .

Application note:
The tests covered by FPT_TST.1 are the following:
- Test of random numbers
- Test of Card life Cycle consistency
- Test of filter Table consistency
- Test of Table of Registry Integrity
- Test of Cryptoalgo entry table integrity

The test covered by FPT_TST.1.3 is the verification of E_SIGN applet code integrity during the loading of the applet during the personalization phase.

5.1.6.8 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.

5.1.7 FTP – Trusted path/channels

5.1.7.1 FTP_ITC.1

FTP_ITC.1.1 / SVD Transfer	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. **Refinement :** Only identification of its end points and protection from modification is ensured for public key transfer .
FTP_ITC.1.2 / SVD Transfer	The TSF shall permit **the TSF** to initiate communication via the trusted channel.
FTP_ITC.1.3 / SVD Transfer	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**.**

5.2 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)**
- And **AVA_VLA.4 (Vulnerability Analysis - Highly resistant).**

5.2.1 TOE security assurance requirements list

All requirements below are those from [PP SSCD3].

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.1	Subset of the 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 4 – TOE security assurance requirements list

5.3 Security Requirements for the IT Environment

5.3.1 Certification Generation application (CGA)

5.3.1.1 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

5.3.1.2 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: [assignement: List of Standards]

5.3.1.3 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.

5.3.1.4 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	The TSF or the TOE shall initiate communication via the trusted channel for Import SVD

5.3.2 Signature creation application (SCA)

5.3.2.1 FCS_COP.1

FCS_COP.1.1 / SCA Hash	The TSF shall perform hashing the DTBS in accordance with a specified cryptographic algorithm [assignment: cryptographic algoritm] and cryptographic key sizes none that meet the following: **SHA-1**.

5.3.2.2 FDP_UIT.1

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 modification, deletion**,** and insertion has occurred.

5.3.2.3 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	The TSF or the TOE shall initiate communication via the trusted channel for signing D.DTBS-representation by means of the SSCD**.**

5.3.2.4 FTP_TRP.1

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.**

5.4 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 JavaCard Software
- The security function supplied by the Digital Signature GemSafe/ID

6.1.1 TOE security functions list

Identification	Name
IC Security functions	
SEF1	Operating State checking
SEF2	Phase Management
SEF3	Protection against snooping
SEF4	Data encryption and data distinguish
SEF5	Random number generation
SEF6	TSF self test
SEF7	Notification of physical attack
SEF8	Virtual Memory System
SEF9	Cryptographic support
SEF10	NVM tearing save write
Digital Signature Security Functions	
SF_SIG_AUTHENTICATION	Authentication management
SF_SIG_CRYPTO	Cryptography management
SF_SIG_MANAGEMENT	Management of operations & access control
JavaCard Security Functions	
SF_CARD_AUTHENTICATION	Card authentication
SF_CARD_CRYPTO	Card cryptographic algorithm & key management
SF_CARD_INTEGRITY	Card objects integrity
SF_CARD_PROTECT	Card operation protection

Table 5 – TOE security functions list

6.1.2 Security functions provided by the IC

The security functions listed here after are described in the IC Security Target [IC Security Target reference].

6.1.2.1 SEF1- Operating state checking.

Correct function of the SLE88CFX4002P is only given in the specified range of the environmental operating parameters. 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 (e.g.

light). The TOE falls into the defined secure state in case of a specified range violation5. The defined secure state causes the chip internal reset process.

6.1.2.2 SEF2- Phase management.

The life cycle of the TOE is split-up in several phases. Chip development and production (phase 2, 3, 4) and final use (phase 4-7) is a rough split-up from TOE point of view. These phases are implemented in the SLE88CFX4002P/m8834b17as test mode (phase 2, 3, 4) and user mode (phase 1, 4-7). In addition a chip identification mode exists which is active in all phases.

During the production phase (phase 3) or after the delivery to the customer (phase 5 or phase 6), the TOE provides the possibility to load a user specific encryption key and user code and data encrypted into the empty (erased) NVM area as specified by the associated control information of the loader mode of the loader filter. After finishing the load operation, the loader mode is automatically deactivated, so that no second load operation with the loader mode is possible.

During the operation of the TOE the PSL provides the possibility to load signed code and data in the NVM and RAM areas as specified by the associated control information of the patch loader mode of the loader filter. The public part of the used signing key is stored in the NVM. This function could be deactivated permanently by the user software.

6.1.2.3 SEF3- Protection against snooping.

Several mechanisms protect the SLE88CFX4002P 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 “active shield” 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 smartcard dedicated proprietary CPU with a non public bus protocol is used which makes analysis complicated.

6.1.2.4 SEF4- Data encryption and data distinguish

The readout of data can be controlled with the use of encryption. An attacker can not use the data he has espionaged, because he must break the encryption.
The memory contents of the SLE88CFX4002P are encrypted on chip to protect against data analysis on stored data as well as on internally transmitted data. To prevent interpretation of leaked processed or transferred information additional randomness is inserted in the information. In addition important parts of the CPU and the complete DES component are especially designed to counter leakage attacks like DPA or EMA. A special design method is used to make the current consumption nearly independent of the processed data. The component RSA are protected against information leakage.
The information leakage is kept low with special design measures. An interpretation of the leaked data is prevented as all the data is encrypted

6.1.2.5 SEF5- Random number generating.

Random data is essential for cryptography as well as for physical security mechanisms. The SLE88CFX4002P is equipped with a true random generator based on physical probabilistic 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 SLE88CFX4002P 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 SLE88CFX4002P 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- Virtual Memory System

The VMS in the SLE88CFX4002P controls the address permissions of the privileged packages (memory areas) 1 and 2 and of the regular packages 3 to 15 and gives the software the possibility to define different access rights for the regular packages (memory areas) 16 to 255. The address permissions of the privileged package 0 are controlled by the hardware and the VMS. In case of an access violation the VMS will generate a trap. Then a trap service routine can react on the access violation.

.

6.1.2.9 SEF9- Cryptographic support

The TOE is equipped with several hardware accelerators and software modules 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 as platform for the software. The components are a combination of software and hardware unit to support DES encryption, a combination of software and hardware unit to support RSA cryptography and software units to support the Advanced Encryption Standard (AES) and the Secure Hash Algorithm (SHA-1)

.

6.1.2.10 SEF10- NVM Tearing save Write

The hardware of the NVM together with the PSL supports the TOE with a function to copy one data block with a defined maximum number of bytes or/and one or a bunch with a maximum number of data blocks of any data size to different NVM locations, under the protection of a data security mechanism. The data security mechanism keeps a backup copy of either the old or the new contents of all addressed NVM pages before they are overwritten. If the update of the data fails due to an unexpected card tearing, the old or the new contents of all target areas affected by the transaction is recovered at the next power-up.

SEF1, SEF3, SEF4, SEF5, SEF6, SEF7, SEF8, SEF9, SEF10 are Security functions provided by the IC contributing directly to the TOE security while SEF2 is contributing indirectly to the TOE security.
The coverage of SFs by the SFRs is given in chapter 8.8.1 table 13.

6.1.3 Security functions provided by the Digital signature application E-SIGN

6.1.3.1 SF_SIG_AUTHENTICATION - Authentication management

This security function manages the authentication mechanisms of the Digital Signature
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.

6.1.3.2 SF_SIG_CRYPTO - Cryptography management

This function manages the cryptographic operations of the Digital signature application.
- Generate cryptographic Signature keys (RSA 1024 bits keys in compliance with [JC2.2.1]
- Destroys the previous Signature cryptographic keys, in case of re-generation .
- Perform Cryptographic operations Signature and verification.
- Performs SCD/SVD correspondence

This function is supported by JavaCard Security Function SF_CARD_CRYPTO .
SF_CARD_CRYPTO provides Cryptographic algorithms RSA, RSA On Board Key generation and Random Generator.
SF_CARD_CRYPTO ensures that D. SCD information is made unavailable after use.

6.1.3.3 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 Initialization SFP attributes,
- specify alternative default values.

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

Access control
This SF ensures that operations on digital signature objects will be executed by authorized roles:
- export of D.SVD by S.User
- Generation of D.SCD/D.SVD pair by S.User with the security attribute “role” set to signatory and the security attribute “SCD/SVD management” set to authorized.
- Creation of D.RAD by S.Admin and modification by S.Signatory
- Sending of D.DTBS-representation by the SCA

Signing of D.DTBS-representation sent by an authorized SCA by S.Signatory with the security attribute “SCD operational” set to “yes”.

This SF will provide Access control to Data Objects according access rules related to the objects.

This SF enforces the security policy on export of user data:

SVD Transfer SFP: The PKCS#10 Certificate is signed using SCD and sent inside a first SMS. Then, the Public key is sent using a second SMS. SHA-1 Algorithm is used for PKCS#10 algorithm.

6.1.4 Security function provided by the JavaCard

6.1.4.1 SF_CARD_AUTHENTICATION card authentication

This security function support SF_SIG_ AUTHENTICATION by managing Pin management at the JavaCard level through JavaCard API..
SF_CARD_AUTHENTICATION ensure the de-allocation of D.VAD and D.RAD after usage.
This Security function is also in charge of secure channel management like establishing a trusted channel between the SCA and the TOE for D.DTBS import. The integrity of SMS containing D.DTBS is checked by SF_CARD_AUTHENTICATION . In case of integrity error detection, this SF will prohibit the use of the altered data, and inform S.Administrator . The security verification of SMS sent for triggering the E-SIGN applet ensures that the SMS is sent by S.Administrator.
This SF enforces the security policy on Import/export of user data:

- SVD Transfer SFP
- Signature-creation SFP: D.DTBS-representation shall be sent by an authorized SCA

This SF uses a permutational mechanism for the Authentication of the users (PIN code).
The strength of the functions is 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 for encryption/decription operations.
- RSA algorithm supports 1024bits to 2048 bits long keys.Concerning E-SIGN application, the key size is 1024 bits for signature and verification operations.
- 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 ..
  DES key generation manages 64, 128, 192 bits long keys.
- Key destruction: the TOE provides specified cryptographic key destruction methods that makes Key Unavailable.

The Random generator is needed for the generation Keys, and Authentication challenge.
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_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.
In case of integrity error detection, this SF will prohibit the use of the altered data, and the card will be Muted or terminated
This SF supports SF_CARD_PROTECT by checking platform data integrity before use an processing.
This SF also provides authorized users with the capability to verify the integrity of stored TSF executable code during loading of the code on the card.

6.1.4.4 SF_CARD_PROTECT : Card operation protection

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

- Analyze potential violation on : illegal access to Java objects.
- Check operating conditions at startup (audit IC sensors)

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 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 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 ensures separation between applications and associated datas (firewalling mechanism).

This SF is supported by the IC SEF1- Operating state checking (and SEF6 Self test), SEF3-Protection against snooping, SEF4- Data encryption and data distinguish, SEF7 (Notification of physical attack), SEF8 (Virtual Memory System) and SEF10 (NVM tearing save write).

The coverage of SFs by the SFRs is given in chapter 8.8.1 table 13.

The Table below shows the dependencies between the SEFs provided by the IC and the SFs provided by the TOE

SF_CARD_PROTECT	SEF3 Protection against snooping SEF4- Data encryption and data distinguish. SEF6 Self test SEF8 Virtual Memory System SEF10 NVM tearing write
SF_CARD_CRYPTO	SEF9 Cryptographic support SEF5 Random Number generating

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 ACM10448
AM_ADO	Delivery and Operation, reference ADO10448
AM_ADV	Development, reference ADV10448
AM_AGD	Guidance documents, reference AGD10448
AM_ALC	Life cycle, reference ALC10448
AM_ATE	Tests, reference ATE10448
AM_AVA	Vulnerability assessment, reference AVA10448

Table 6 – 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

This security target is based on the Protection Profiles “Secure Signature Creation Devices” Type 3 [PP SSCD3]. Indeed, the trusted path is not provided ME.

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 PPs are refined.

Component	Iteration	Assignment	Selection	Refinement
TOE				
FCS_CKM.1	–	X	–	x
FCS_CKM.4	–	X	–	–
FCS_COP.1	X	X	–	x
FDP_ACC.1	–	–	–	–
FDP_ACF.1	–	–	–	X
FDP_ETC.1 identical	–	–	–	–
FDP_ITC.1	–	–	–	–
FDP_RIP.1	–	–	–	X
FDP_SDI.2	–	–	–	X
FDP_UIT.1 identical	–	–	–	–
FIA_AFL.1	–	X	–	X
FIA_ATD.1 identical	–	–	–	–
FIA_UAU.1 identical	–	–	–	–
FIA_UID.1 identical	–	–	–	–
FMT_MOF.1 identical	–	–	–	–
FMT_MSA.1	–	X	–	-
FMT_MSA.2 identical	–	–	–	–
FMT_MSA.3 identical	–	–	–	–
FMT_MTD.1		X	–	–
FMT_SMR.1 identical	–	–	–	–
FMT_SMF.1*		X		
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	–	–	X	x

Component	Iteration	Assignment	Selection	Refinement
IT Environnement CGA				
FCS_CKM.2 identical	–	–	–	–
FCS_CKM.3 identical	–	–	–	–
FDP_UIT.1 identical	–	–	–	–
FTP_ITC.1	–	–	X	X
IT Environnement SCA				
FCS_COP.1 identical	–	–	–	X
FDP_UIT.1 identical	–	–	–	–
FTP_ITC.1 identical	–	–	–	–
FTP_TRP.1	–	–	x	–

Table 7 – Mapping of the performed operations and the IT security functional requirements

Note: the requirement FTP_TRP/TOE defined in [PP SSCD3] is removed in this Security Target
Note: The integrity of D.DTBS is checked at the reception by the TOE before the signature operation. This SFR support the FDP_ITC.1.1/DTBS which ensures that DTBS is sent by authorized SCA.
Note: Only identification of its end points and protection from modification is ensured for public key transfer (FTP_ITC/SVD Transfer.).

7.3 PP ADDITIONS

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.

7.3.2 Additional Organizational Security Policy

Following PP SSCD3 OSP has been refined
P.CSP_Qcert.

7.3.3 Additional threats

All threats from PP SSCD3 have been refined with the assets refined names.

7.3.4 Additional security objectives

The following PPSSCD security objective have been refined:
OT.SCD_Secrecy (Secrecy of the SCD) is refined with D.VAD, D.RAD and D.SCD

7.3.5 Additional security functional requirements

Following Security Functional Requirements has been added to the claimed PP:
FCS_CKM.1/DES, FCS_COP.1/DES: Cryptographic operations (for DES operations concerning session key and SMS deciphering).

FMT_SMF.1: Specification of management functions
The PP was written using CC V2.1. This security target is build using CC V2.3. This SFR was added to respect FMT_SMF.1 dependency required in CC2.3 for FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1.

FPT_SEP.1: TSF Domain separartion
This requirement has been added taking account the Java Card maintains a security domain for E-SIGN applet execution

7.3.6 Additional security assurance requirements

There are no additional security assurance requirements.

8. 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.

9. REFERENCES

Short Reference	Title - Reference
CCPART1	Common Criteria for Information Technology Security Evaluation. Part 1: Introduction & general model,. Version 2.3. August, 2005. CCMB- 2005-08-001
CCPART2	Common Criteria for Information Technology Security Evaluation. Part 2: Functional security requirements, Version 2.3. August, 2005. CCMB- 2005-08-001
CCPART3	Common Criteria for Information Technology Security Evaluation. Part 3: Assurance security requirements, Version 2.3. August, 2005. CCMB- 2005-08-001
CEM	Common Methodology for Information Technology Evaluation, CCMB- 2005-08-001
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
BSI PP	Smartcard IC Protection Profile - BSI-PP-0002; Version 1.0, July 2001
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)
[IC-ST]	SLE88CFX4000P / m8830 Security Target Version 1.3 Date 25-04-2006 Author Jürgen Noller
[CC-COMP]	Composite product evaluation for Smart Card and similar devices – ISCI-WG1
[JC2.2.1]	Java Card™ 2.2.1 Virtual Machine - 2.2.1 - Oct 2003
[GP2.1.1]	Global Platform - Card specification v2.1.1 - 2.1.1 - March 2003

<END OF DOCUMENT>