InCrypto34v2-Security Target

Version 1.58 (A-6)

Foreword

This document has been developed by CE.VA. IMQ/LPS at the request of JDC INCARD - ST (JDC), and maintained by the JDC.
This document is the Security Target of INCRYPTO34v2 product, jointly developed by INCARD and ST.

Revision History

Version	Date of publication	Comments
1.0 Draft Proposal	24.04.2002	First publication of INCRYPTO34v2 Security Target Draft Proposal submitted to JDC INCARD - ST.
1.0 Draft	13.05.2002	Published after revision performed by IMQ and JDC INCARD – ST during technical meeting of 6/7.05.2002 at INCARD Spa.
1.0 Revised Draft	17.05.2002	Published with revision comments of Vittorio Asnaghi.
1.1 Modified Draft	09.09.2002	
1.20	30.10.2002	Modifications based on the TüViT comments
1.30	04.12.2002	Include all the changes based on the TüViT comments
1.40 (A-0)	23.01.2003	Include the changes based on the TüViT comments V 3.0 Date 16.01.2003 Document restyling
1.50 (A-1)	03.02.2003	Include the changes based on the TüViT comments V4.0 and V4.1 Date 29.01.2003
1.51 (A-2)	13.02.2003	Include the changes based on the CC interpretation 065
1.55 (A-3)	25.02.2003	Include the changes based on the TüViT comments V5.0 Date 18.02.2003
1.56 (A-4)	25.03.2003	Include the changes based on BSI comments
1.57 (A-5)	27.03.2003	Added last sentence to paragraph 6
1.57 (A-5)	03.07.2003	Change all the IC platform references to ST19XL34 V2
1.58 (A-6)	23.11.2004	Change all the IC platform references to ST19XL34P

Table Of Contents

List of Tables

List of figures

Conventions

The document follows the rules and conventions laid out in Common Criteria 2.1, part 1 [2], Annex C “Specification of Security Targets”.
As stated in § 7, this Security Target is compliant to Protection Profile [6], which in the following will be referred to as [SSCD PP].
Admissible algorithms and parameters for algorithms for secure signature-creation devices referred hereafter is derived from document [5].

Document Organisation

Section 1	Provides the introductory material for the Security Target.
Section 2	Provides the TOE description.
Section 3	Provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware, the TOE software, or through the environmental controls.
Section 4	Defines the security objectives for both the TOE and the TOE environment.
Section 5	Defines the security requirement for both the TOE and the TOE environment.
Section 6	Summarize security functions and assurance measures implemented by the TOE.
Section 7	Claims Security Target conformity to Protection Profile [6].
Section 8	Includes a rationale for TOE security objectives and requirements, for TOE summary specifications and for PP claims.
Section 9	Includes a reference section to identify background material.
Section 10	Includes a glossary.

1 ST Introduction

1.1. ST Identification

[1] Here are the labeling and descriptive information necessary to control and identify the ST and the TOE to which it refers.

Title:	INCRYPTO34v2 - Security Target
Assurance Level:	EAL 4 augmented with AVA_MSU.3 and AVA_VLA.4.
Strength of Functions:	SOF High
Authors:	Philippe Callot (STMicroelectronics), Saverio Donatiello (Incard spa)
CC Version:	2.1. [2], [3], [4].
PP Conformance:	SSCD Protection Profile Type 3 [SSCD PP] [6].
General Status:	Draft
Version:	1.57
Related ST:	ST19XL34 ICC Security Target lite [9]

1.2. ST Overview

[2] This document provides a complete and consistent statement of the security enforcing functions and mechanisms of INCRYPTO34v2.0 device (hereafter referred to as the TOE, i.e. the Target of Evaluation).

[3] The Security Target details the TOE security requirements and the countermeasures proposed to address the perceived threats to the assets protected by the TOE.

[4] INCRYPTO34v2 is a multifunctional smartcard product implementing a type 3 Secure Signature-Creation Device as described in [SSCD PP] [6] § 2.1.

[5] Main INCRYPTO34v2 functionalities cover following areas:

- Cryptographic key generation and secure management;
- Secure signature generation with secure management of data to be signed;
- Identification and Authentication of trusted users and applications;
- Data storage and protection from modification or disclosures, as needed,
- Secure exchange of sensitive data between the TOE and a trusted applications
- Secure exchange of sensitive data between the TOE and a trusted human interface device.

[6] INCRYPTO34v2 was developed on a STMicroelectronics microcontroller: ST19XL34P ICC, a hardware platform offering 34Kb of EEPROM and cryptographic support, especially designed for secure application based on high performance Public and Secret key algorithms (i.e. RSA, DES, TripleDES). The chip includes a Modular Arithmetic Processor (MAP), based on an 1088-bit processor architecture, and a DES accelerator, both designed to speed up cryptographic calculations. Furthermore the hardware also includes a true random number generator compliant to [13].

[7] HW platform has been certified under the French Scheme (see [10], ST19XL34P ICC product certificate) and it is compliant with PP9806 Protection Profile for smartcard integrated circuit [7]. Therefore references are made in this document to ST19XL34P ICC Security Target [9].

1.3. CC conformance claim

[8] This ST is conformant with Common Criteria (CC) Version 2.1 Part 1 (ISO/IEC 15408 Evaluation Criteria for Information Technology Security; Part1: Introduction and general model 1999 [2]).

This ST is conformant with Common Criteria (CC) Version 2.1 Part 2 (ISO/IEC 15408 Evaluation Criteria for Information Technology Security; Part 2: Security functional requirements 1999 [3]) with extension "FPT_EMSEC.1" made in the SSCD Protection Profile [SSCD PP] [6].

This ST is conformant with Common Criteria (CC) Version 2.1 Part 3 (ISO/IEC 15408 Evaluation Criteria for Information Technology Security; Part 3: Security Assurance Requirements 1999 [4]) based only on CC Part 3 assurance components.

This ST is compliant with the SSCD Protection Profile [SSCD PP] [6].

The TOE assurance level claim is EAL 4 augmented with AVA_MSU.3 and AVA_VLA.4.

The TOE meets the SSCD Type 3 Protection Profile [SSCD PP] [6].

The TOE is conformant with Common Criteria Version 2.1, with part 2 and part 3 augmented as stated in [SSCD PP] [6].

The minimum strength of function level for the SFR is SOF-high.

2 TOE Description

[9] This part of the ST describes the TOE as an aid to the understanding of its security requirements, and addresses the product. The scope and boundaries of the TOE are described in general terms both in a physical way (hardware and/or software components/modules) and a logical way (IT and security features offered by the TOE).

2.1. Product type

[10] The Target Of Evaluation (TOE) is the Secure Signature Creation Device (SSCD) defined by:

- The SSCD Application INCRYPTO34 V2.00
- The INCRYPTO34 devices drivers INCRYPTO34 V2.00
- The Integrated Circuit and its libraries ST19XL34P
- User and Administrator guidance

2.2. TOE functionalities

[11] INCRYPTO34v2 multifunctional smartcard product is intended to provide all capabilities required to devices involved in creating qualified electronic signatures (see next figure to identify main TOE functional components and interfaces with TOE environment and TOE boundaries):

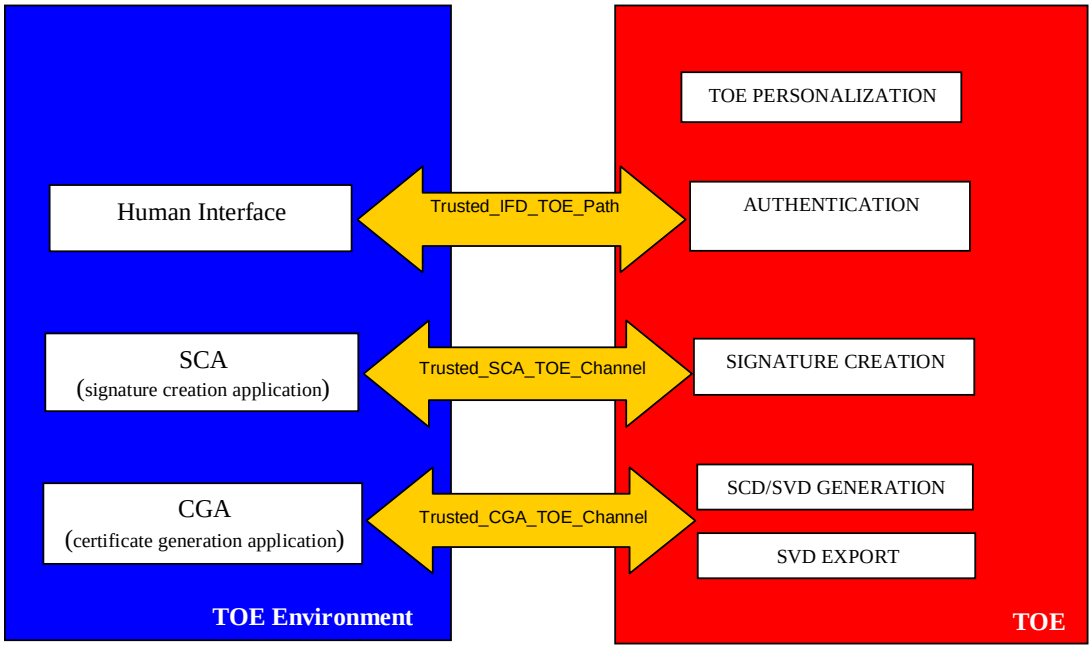

Figure 1: TOE boundaries

[12] The CGA, the SCA and the Human Interface are part of the immediate environment of the TOE.

[13] The TOE is securely personalized by a trusted and competent administrator according to Administrator Documentation: during TOE personalization, the administrator is responsible for INCRYPTO34v2 File System creation and configuration via a Personalization application.

[14] After its personalization, the TOE is ready to be:

- Securely used for signature under sole control of one specific user (the *signatory* in the remainder of the document);

- Securely administered by an authorized Administrator.

[15] The TOE is able to generate its own signature keys (the SCD/SVD pair): an authorized Administrator uses the CGA to initiate SCD/SVD generation and to ask the SSCD to export the SVD for generation of the corresponding certificate.

[16] The TOE holds the SVD and, before exporting the SVD to a CGA for certification purposes, it provides a trusted channel in order to maintain its integrity.

[17] The TOE is able to perform the signature operation using the RSA cryptographic algorithm and the parameters agreed as suitable according to [5].

[18] The signatory must be authenticated before signatures creation is allowed: for this reason he sends his authentication data (a PIN) to the TOE using a trusted path between the interfaces device (IFD) used, i.e. a smartcard reader, and the TOE.

[19] The smartcard reader is also used:

- by the Signatory or the Administrator to change his Reference Authentication Data (RAD) held by the TOE against which the TOE verifies a user PIN;
- by the Administrator to unblock the Signatory's Reference Authentication Data, when needed.

[20] The data to be signed (DTBS) or their representation (DTBSR) are transferred by the SCA to the TOE only over a trusted channel in order to maintain their integrity. The same channel is used to return the signed data object (SDO) from the TOE to the SCA (see [SSCD PP] § 2.1).

[21] The TOE, when requested by the SCA, is able to generate data to be signed representation (DTBSR) using a hash function agreed as suitable according to [5].

[22] As depicted in the next figure, INCRYPTO34v2 embedded SW is structured on two layers consisting of the devices drivers and the SSCD application, in which SW functions are implemented as APDU commands compliant with ISO/IEC 7816- part 4 and 8 (see [11]).

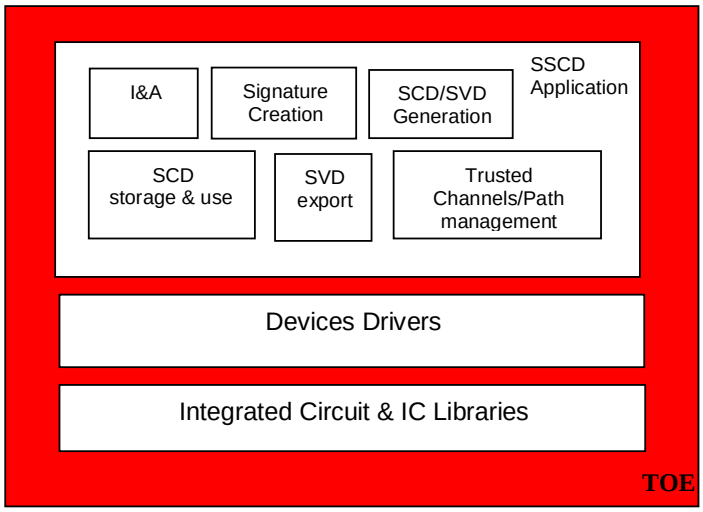

Figure 2: TOE components

2.3. TOE life cycle

[23] The typical TOE lifecycle is shown in Figure 3. Basically, it consists of a design and development phase and an operational phase.

[24] As already stated, INCRYPTO34v2 HW platform design and development has been certified respect to PP 9806 [7], that includes the phase1 delivery, the phase 2 and phase 3.

[25] TOE lifecycle phases within the scope of the evaluation are those covered by [SSCD PP], which refers to the operational phase. This phase represents installation, generation, start-up and operation in the CC terminology.

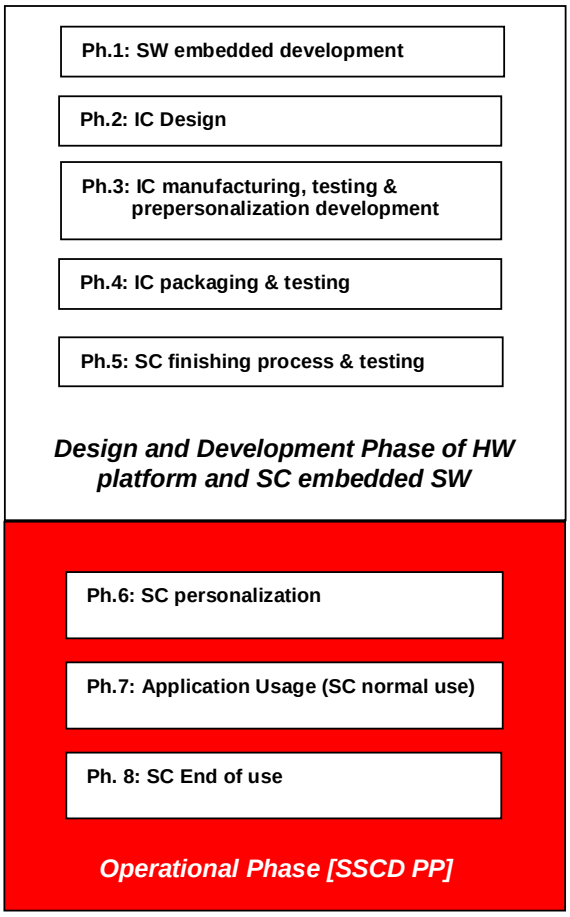

Figure 3: TOE life cycle

[26] The TOE implements a mechanism in order to recognize its operational phase.

[27] TOE operational phase starts after INCRYPTO34v2 smartcard and its HW platform have been successfully designed, developed, manufactured and tested, when it is released from *chip manufacturer* (ST Microelectronics) to *card manufacturer* (Incard Spa.).

[28] The TOE is delivered to the *card manufacturer* with a default Reference Authentication Data to be used for the first Administrator identification and authentication (RAD_A). The TOE is in *SC personalization* state at the beginning of TOE Operational phase.

[29] In *SC personalization* state TOE administrator is responsible for:

- TOE file system configuration according to TOE Administration documentation

- Set the TSF data Access conditions and Secure Messaging conditions according to TOE Administration documentation

So the TOE security is granted in the other states of TOE operational phase.

[30] In *SC personalization* state TOE administrator is in particular responsible for:

- Changing the default RAD_A value;
- Creating the SCD/SVD pair and setting their Access Conditions and Secure Messaging conditions in order to grant that the SCD will be used for signing purposes only by the legitimate Signatory;
- Exporting the SVD for certification purposes;
- Creating Reference Authentication Data to be used for Signatory identification purpose (RAD_S) and setting its Access Conditions and Secure Messaging conditions;
- Importing the cryptographic keys to be used for Secure Messaging (SM_{keys});

[31] After completion of *SC personalization* the administrator put the TOE in *SC normal use* state, when the TOE could be used either by the Signatory or the Administrator.

[32] In *SC normal use* state the TOE allows the Signatory to:

- Change the RAD_S value used by the TOE for his identification and authentication;
- Use the SCD for signing DTBS data.

[33] In *SC normal use* state the TOE allows the Administrator to:

- Change the RAD_A value used by the TOE for his identification and authentication;
- Creation of a new SCD/SVD pair with secure destruction of previously created SCD/SVD pair managed by the TOE;
- Export the SVD for certification purposes.

[34] When a failure occurs in *SC normal use* state, the TOE manages the fault and, according to its severity, enters in one of the following states:

- If a chip integrity violation occurred, the TOE enters *SC end of use* state, where, after having performed all actions needed for its secure disposal, the TOE is no more able to process any APDU command;
- If the failure cannot be recovered, the TOE enters *SC end of use* state, where TOE signing application is no more available;
- In all other cases in which the failure is recovered, the TOE turns back in *SC normal use* state.

2.4. TOE Environment

2.4.1. Development and Production Environment

[35] The TOE described in this ST is developed in the following environments:

PHASE	DESCRIPTION	ENVIRONMENT
1	Embedded Software (OS and application) Development	Incard Caserta
2	IC Design	ST AMK, ST Rousset
3	IC manufacturing and testing	ST Catane, ST Rousset
4	IC Packaging and testing	ST Bouskoura, Incard Caserta.

3 TOE Security Environment

[36] Following paragraphs describe the security aspects of the environment in which the TOE is intended to be used.

3.1. Assets

[37] With regard to INCRYPTO34v2 implementation, assets that need to be protected by the TOE are here defined according to [SSCD PP] [6] § 3. The following table summarizes them for clarity:

ASSET ACRONYM	ASSET DESCRIPTION	SECURITY NEED
SCD:	Private key used to perform an electronic signature operation.	Confidentiality.
SVD:	Public key linked to the SCD and used to perform an electronic signature verification.	Integrity, when it is exported.
DTBS(R):	Set of data, or its representation which is intended to be signed.	Integrity.
VAD:	PIN code entered by the End User to perform a signature operation.	Confidentiality and authenticity as needed by the authentication method employed.
RAD_A:	Reference PIN code used to identify and authenticate the Administrator.	Integrity and confidentiality.
RAD_S:	Reference PIN code used to identify and authenticate the Signatory.	Integrity and confidentiality.
	Signature-creation function of the SSCD using the SCD	The quality of the function must be maintained so that it can participate to the legal validity of electronic signatures.
	Electronic signature	Not forgery (Integrity).

3.2. Subjects

[38] In [SSCD PP] [6] § 3 are defined subjects that can operate with the TOE, here reported for clarity:

SUBJECTS	DEFINITION
S.User	End user of the TOE, which can be identified as S.Admin or S.Signatory.
S.Admin	User who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions.
S.Signatory	User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents.

3.3. Threat agents

[39] In [SSCD PP] [6] § 3 are defined malicious subjects that aim to attack the TOE, here reported for clarity:

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

3.4. Secure usage Assumptions

[40] The same defined in [SSCD PP] [6] § 3.1, with the following addition:

ASSUMPTION	DEFINITION
A.PERSONALIZATION	It is assumed that TOE personalization takes place with the observance of physical and procedural measures granting the integrity, confidentiality and availability of the TOE personalization data. In particular it is assumed that symmetric keys used to implement the trusted channels and path by the secure messaging mechanism are securely imported and stored by the SCA and the CGA applications.
A.MANAGE	It is assumed that the TOE is personalized (in *SC personalization* state) and administered (in *SC normal use*) according to the Administration documentation by a competent individual who is responsible for the security of TOE assets and who is trusted not to abuse his privileges. In particular, it is assumed that TOE Administrator follows the TOE Administration documentation for TOE secure disposal after it entered the *SC end of use* state.
A.VAD	It is assumed that information needed for positive identification and authentication by the TOE are delivered to TOE users in a secure manner.

3.5. Organizational Security Policies

[41] As defined in [SSCD PP] [6] § 3.3.

3.6. Threats to Security

[42] Threats are here reported for clarity as they are defined in [SSCD PP] [6] § 3.2.

T.TYPE	THREAT
T.Hack_Phys	*Physical attacks through the TOE interfaces.* An attacker interacts with the TOE interfaces to exploit vulnerabilities, resulting in arbitrary security compromises. This threat addresses all the assets.
T.SCD_Divulg	*Storing, copying, and releasing of the signature-creation Data* An attacker can store, copy, the SCD outside the TOE. An attacker can release the SCD during generation, storage and use for signature-creation in the TOE
T.SCD_Derive	*Derive the signature-creation data* An attacker derives the SCD from public known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data communicated outside the TOE, which is a threat against the secrecy of the SCD.
T.Sig_Forgery	*Forgery of the electronic signature* An attacker forges the signed data object maybe together with its electronic signature created by the TOE and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature generated by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.
T.Sig_Repud	*Repudiation of signatures* If an attacker can successfully threaten any of the assets, then the no repudiation of the electronic signature is compromised. This result in the signatory is able to deny having signed data using the SCD in the TOE under his control even if the signature is successfully verified with the SVD contained in his un-revoked certificate.
T.SVD_Forgery	*Forgery of the signature-verification data* An attacker forges the SVD presented by the TOE to the CGA. This result in loss of SVD integrity in the certificate of the signatory.
T.DTBS_Forgery	*Forgery of the DTBS-representation* An attacker modifies the DTBS-representation sent by the SCA. Thus the DTBS-representation used by the TOE for signing does not match the DTBS the signatory intended to sign.
T.SigF_Misuse	*Misuse of the signature-creation function of the TOE* An attacker misuses the signature-creation function of the TOE to create SDO for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

4 Security Objectives

4.1. Security objectives for the TOE

[43] Following table summarizes which are the security objectives for the TOE, as they are defined in [SSCD PP] [6] § 4.1.

OT.TYPE	TOE OBJECTIVE
OT.EMSEC_Design	*Provide physical emanations security* The TOE is designed and built in such a way as to control the production of intelligible emanations within specified limits.
OT.Lifecycle_Security	*Lifecycle security* The TOE detects flaws during the initialization, personalization and operational usage. The TOE provides 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.
OT.SCD_SVD_Corresp	*Correspondence between SVD and SCD* The TOE ensures the correspondence between the SVD and the SCD generated by the TOE itself. The TOE verifies the correspondence between the SCD stored by the TOE and the SVD sent to the TOE on demand.
OT.SVD_Auth_TOE	*TOE ensures authenticity of the SVD* The TOE provides means to enable the CGA to verify the authenticity SVD that has been exported by that TOE.
OT.Tamper_ID	*Tamper detection* The TOE provides system features that detect physical tampering of a system component, and use those features to limit security breaches.
OT.Tamper_Resistance	*Tamper resistance* The TOE prevents or resists physical tampering with specified system devices and components.
OT.Init	*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 ensures 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 verifies 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 the SCD against the use of others. The TOE resists to 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

As defined in [SSCD PP] [6] § 4.2 with the addition of the paragraph 4.2.1.

4.2.1. Additional security objective for the non-IT environment

OE.Op_Phase	*TOE operational phase security* The security of the TOE itself, of personalization data to be loaded into the TOE and of related verification authentication data (VAD) is ensured by S.Admin, S.User and S.Signatory in the TOE's non-IT environment throughout the TOE's operational phase, i.e. in personalization, normal use and end of use, and during delivery between operational lifecycle phases

5 IT Security Requirements

[44] Here are defined the functional and assurance security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE.

5.1. TOE Security Functional Requirements

[45] The TOE consists of a combination of hardware and software components implementing the specific TOE Security Functions (TSF) for the functional requirements defined in the PP.

[46] Following table lists each TOE Security Functional Requirement (SFR) included in this Security Target and identifies which Common Criteria operations (assignment (A), selection (S), refinement (R), and/or iteration (I)) have been applied to the requirement relative to the SSCD Protection Profile [SSCD PP] [6].

COMPONENT	NAME	A	S	R	I
FCS_CKM.1	Cryptographic Key Generation	×		×	
FCS_CKM.4	Cryptographic Key Destruction	×			
FCS_COP.1	Cryptographic Operation (SCD/SVD correspondence verification and digital signature generation)	×		×	
FIA_AFL.1.	Authentication Failure handling	×			
FMT_MSA.1	Management of Security Attributes	×			
FMT_MTD.1	Management of TSF Data	×			
FMT_SMF.1	Specification of Management Functions	×			
FPT_AMT.1	Abstract Machine Testing		×		
FPT_EMSEC.1	TOE Emanation	×			
FPT_FLS.1	Failure with preservation of secure state	×			
FPT_PHP.3	Resistance to physical attack	×			
FPT_TST.1	TSF Testing	×	×		
FTP_ITC.1	Inter-TSF trusted channel		×		
FTP_TRP.1	Trusted Path	×	×		

Table 1: Operation performed on TOE SFRs

[47] This paragraph fully restates TOE security functional requirements (see [SSCD PP] [6] in § 5.1) for clarity: operations completed in this ST are shown in ***bold italics***.

5.1.2.	**CRYPTOGRAPHIC SUPPORT (FCS)**	
5.1.2.1.	**Cryptographic key generation (FCS_CKM.1)**	
	FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***RSA*** and specified cryptographic key sizes ***of 1024 bits*** that meet the following list of approved algorithms and parameters ***[5]***.
5.1.2.2.	**Cryptographic key destruction (FCS_CKM.4)**	
	FCS_CKM.4.1	The TSF shall destroy cryptographic keys in case of regeneration of a new SCD in accordance with a specified cryptographic key destruction method ***physical irreversible destruction of the stored key value*** that meets the following standard ***none***.
5.1.2.3.	**Cryptographic operation (FCS_COP.1)**	
	FCS_COP1.1/CORRESP	The TSF shall perform SCD/SVD correspondence verification in accordance with a specified cryptographic algorithm ***RSA*** and cryptographic key sizes ***1024 bits*** that meet the following list of approved algorithms and parameters ***[5]***.
	FCS_COP1.1/SIGNING	The TSF shall perform digital signature-generation in accordance with a specified cryptographic key generation algorithm ***RSA*** and specified cryptographic key sizes ***1024 bits*** that meet the following list of approved algorithms and parameters ***[5]***.

5.1.3.	USER DATA PROTECTION (FDP)	
5.1.3.1.	**Subset access control (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 SCA, 2. signing of DTBS-representation by Signatory.
5.1.3.2.	**Security attribute based access control (FDP_ACF.1)**[1]	
	Initialisation SFP	
	FDP_ACF.1.1/Initialisation SFP	The TSF shall enforce the Initialisation SFP to objects based on General attribute and initialisation attribute.
	FDP_ACF.1.2/Initialisation SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to "authorized" is allowed to generate SCD/SVD pair.
	FDP_ACF.1.3/Initialisation SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
	FDP_ACF.1.4/Initialisation SFP	The TSF shall explicitly deny access of subjects to objects based on the 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 authorized" is not allowed to generate SCD/SVD pair.
	SVD Transfer SFP	
	FDP_ACF.1.1/ SVD Transfer SFP	The TSF shall enforce the SVD Transfer SFP to objects based on General attribute.
	FDP_ACF.1.2/ SVD Transfer SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The user with the security attribute "role" set to "Administrator" or to "Signatory" is allowed to export SVD.
	FDP_ACF.1.3/ SVD Transfer SFP	The TSF shall explicitly 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.

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

USER, SUBJECT OR OBJECT THE ATTRIBUTE IS ASSOCIATED WITH	ATTRIBUTE	STATUS
USER ATTRIBUTE GROUP		
User	Role	Administrator, signatory
GENERAL 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

	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: 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.	**Export of user data without security attributes (FDP_ETC.1)**	
	FDP_ETC.1.1/SVD Transfer	The TSF shall enforce the SVD Transfer 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.	**Import of user data without security attributes (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.
5.1.3.5.	**Subset residual information protection (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 the resource from the following objects: SCD, VAD, RAD.
5.1.3.6.	**Stored data integrity monitoring and action (FDP_SDI.2)**[2]	
	FDP_SDI.2.1/Persistent	The TSF shall monitor user data stored within the TSC for integrity error on all objects, based on the following attributes: integrity checked persistent stored data.
	FDP_SDI.2.2/Persistent	Upon detection of a data integrity error, the TSF shall: 1. prohibit the use of the altered data 2. inform the Signatory about integrity error.
	FDP_SDI.2.1/DTBS	The TSF shall monitor user data stored within the TSC for integrity error on all objects, based on the following attributes: integrity checked stored data.
	FDP_SDI.2.2/DTBS	Upon detection of a data integrity error, the TSF shall: 1. prohibit the use of the altered data 2. inform the Signatory about integrity error.
5.1.3.7.	**Data exchange integrity (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 the 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.	**IDENTIFICATION AND AUTHENTICATION (FIA)**	
5.1.4.1.	**Authentication failure handling (FIA_AFL.1)**	
	FIA_AFL.1.1	The TSF shall detect when ***3*** unsuccessful authentication attempts occur related to consecutive failed authentication attempts.
	FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall block RAD.
5.1.4.2.	**User attribute definition (FIA_ATD.1)**	
	FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: RAD.

[2] Note that The following data persistently stored by TOE have the user data attribute "integrity checked persistent stored data":
1. SCD
2. RAD
3. SVD
Note also that The DTBS-representation temporarily stored by TOE has the user data attribute "integrity checked stored data".

5.1.4.3.	**Timing of authentication (FIA_UAU.1)**	
	FIA_UAU.1.1	The TSF shall allow 1. Identification of the user by means of TSF required by FIA_UID.1. 2. Establishing a trusted path between local user[3] and the TOE by means of TSF required by FTP_TRP.1/TOE. 3. Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import. on behalf of the user to be performed before the user is authenticated.
	FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
5.1.4.4.	**Timing of identification (FIA_UID.1)**	
	FIA_UID.1.1	The TSF shall allow 1. Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE. 2. Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import. on behalf of the user to be performed before the user is identified.
	FIA_UID.1.2	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.	**SECURITY MANAGEMENT (FMT)**	
5.1.5.1.	**Management of security functions behaviour (FMT_MOF.1)**	
	FMT_MOF.1.1	The TSF shall restrict the ability to enable the signature-creation function to Signatory.
5.1.5.2.	**Management of security attributes (FMT_MSA.1)**	
	FMT_MSA.1.1 Administrator	The TSF shall enforce the Initialization SFP to restrict the ability to modify 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.	**Secure security attributes (FMT_MSA.2)**	
	FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for security attributes.
5.1.5.4.	**Static attribute initialization (FMT_MSA.3)**	
	FMT_MSA.3.1	The TSF shall enforce the Initialization SFP and Signature-creation SFP to provide restrictive default values for security attributes that are used to enforce the SFP. Refinement The security attribute of the SCD "SCD operational" is set to "no" after generation of the SCD.
	FMT_MSA.3.2	The TSF shall allow the Administrator to specify alternative initial values to override the default values when an object or information is created.
5.1.5.5.	**Management of TSF data (FMT_MTD.1)**	
	FMT_MTD.1.1	The TSF shall restrict the ability to modify the RAD to Signatory.
5.1.5.6.	**Specification of Management Functions (FMT_SMF.1)** [4]	
	FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: ***Identification and Authentication management, access condition management.***
5.1.5.7.	**Security roles (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.

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

[4] This SFR has been added as suggested in the CC interpretation 065

5.1.6.	PROTECTION OF THE TSF (FPT)	
5.1.6.1.	**Abstract machine testing (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.	**TOE Emanation (FPT_EMSEC.1)**	
	FPT_EMSEC.1.1	The TOE should not emit ***Side Channel Current*** in excess of ***States of Art limits*** enabling access to RAD and SCD
	FPT_EMSEC.1.2	The TSF shall ensure ***all users*** are unable to use the following interface ***external contacts*** to gain access to RAD and SCD.
5.1.6.3.	**Failure with preservation of secure state (FPT_FLS.1)**	
	FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: ***Power shortage, over voltage, over and under clock frequency, integrity problems***.
5.1.6.4.	**Passive detection of physical attack (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.
5.1.6.5.	**Resistance to physical attack (FPT_PHP.3)**	
	FPT_PHP.3.1	The TSF shall resist ***operating changes by the environment, and physical integrity,*** to the ***clock, voltage supply and shield layers*** by responding automatically such that the TSP is not violated.
5.1.6.6.	**TSF Testing (FPT_TST.1)**	
	FPT_TST.1.1	The TSF shall run a suite of self-tests ***during initial start-up or when calling a sensitive module*** to demonstrate the correct operation of the TSF.
	FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
	FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

5.1.7.	TRUSTED PATH/CHANNELS (FTP)	
5.1.7.1.	**Trusted path/channels (FTP)**	
	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.
	FTP_ITC.1.2/SVD Transfer	The TSF shall permit ***the remote trusted IT product*** to initiate communication via the trusted channel.
	FTP_ITC.1.3/SVD Transfer	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 the 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 DTBS-representation.
5.1.7.2.	**Trusted path (FTP_TRP.1)**	
	FTP_TRP.1.1/TOE	The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
	FTP_TRP.1.2/TOE	The TSF shall permit ***local users*** to initiate communication via the trusted path.
	FTP_TRP.1.3/TOE	The TSF shall require the use of the trusted path for ***initial user authentication***.

5.2. TOE Security Assurance Requirements

[48] TOE assurance requirements are those stated in [SSCD PP] [6] § 5.2, here reported in tabular form:

ASSURANCE CLASS	ASSURANCE COMPONENTS
ACM	ACM_AUT.1 - ACM_CAP.4 - ACM_SCP.2
ADO	ADO_DEL.2 - ADO_IGS.1
ADV	ADV_FSP.2 - ADV_HLD.2 - ADV_IMP.1 - ADV_LLD.1 - ADV_RCR.1 - ADV_SPM.1
AGD	AGD_ADM.1 - AGD_USR.1
ALC	ALC_DVS.1 - ALC_LCD.1 - ALC_TAT.1
ATE	ATE_COV.2 - ATE_DPT.1 - ATE_FUN.1 - ATE_IND.2
AVA	AVA_MSU.3 - AVA_SOF.1 - AVA_VLA.4

Table 2: Assurance Requirements - EAL 4 extended with AVA_MSU.3 and AVA_VLA.4

5.3. IT Environment Security requirements

[49] Following table lists each IT Environment Security Functional Requirement (SFR) included in this Security Target and identifies which Common Criteria operations (assignment (A), selection (S), refinement (R), and/or iteration (I)) have been applied to the requirement relative to the SSCD Protection Profile [SSCD PP] [6].

COMPONENT	NAME	A	S	R	I
FCS_CKM.2/CGA	Cryptographic Key Distribution	×		×	
FCS_CKM.3/CGA	SVD Import	×			
FCS_COP.1/SCA Hash	Cryptographic Operation	×		×	
FTP_ITC.1/SVD import	Inter-TSF trusted channel		×		
FTP_TRP.1/SCA	Trusted Path		×		

Table 3: Operation performed on ENVIRONMENT SFRs

[50] Following paragraph fully restates security requirements for the IT environment presented in [SSCD PP] [6] § 5.3 for clarity.

[51] Numbering of SFRs in this ST is the same proposed in [SSCD PP] [6]: operations completed in this ST are shown in ***bold italics***.

5.3.2.	**CERTIFICATION GENERATION APPLICATION (CGA)**	
5.3.2.1.	**Cryptographic key distribution (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 ***for DES or Triple DES***.
5.3.2.2.	**Cryptographic key access (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: ***none***.
5.3.2.3.	**Data Exchange Integrity (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.
5.3.2.4.	**Inter-TSF trusted channel (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.

5.3.3.	**SIGNATURE CREATION APPLICATION (SCA)**	
5.3.3.1.	**Cryptographic Operation (FCS_COP.1)**	
	FCS_COP.1.1/ SCA Hash	The TSF shall perform hashing the DTBS in accordance with a specified cryptographic algorithm ***SHA-1*** and cryptographic key sizes none that meet the following: list of approved algorithms and parameters ***to be the Secure Hash Algorithm, SHA-1 as specified in the standard FIPS 180-1 [14].***
5.3.3.2.	**Data Exchange Integrity (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.
5.3.3.3.	**Inter-TSF trusted channel (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 DTBS-representation by means of the SSCD.
5.3.3.4.	**Trusted path (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.1.2/ SCA	The TSF shall require the use of the trusted path *for* ***initial user authentication.***

5.3.4. Non-IT Environment Security requirements

[52] As defined in § 5.4 of [SSCD PP] [6].

6 TOE Summary Specification

[53] This section contains a high-level specification of each TOE Security Function (TSF) that contributes to satisfaction of the Security Functional Requirements of chapter 5.

[54] The specifications cover following major areas: identification and authentication, access controls, key management, data transfer over trusted path and channels, stored data protection, test management, failure management and TOE life cycle management.

[55] Following table lists the SFRs, which are not satisfied by any TSF because they specify null functionality.

FDP_ACF.1.3/Initialization SFP
FDP_ACF.1.3/SVD Transfer SFP
FDP_ACF.1.4/SVD Transfer SFP
FDP_ACF.1.3/Personalization SFP
FDP_ACF.1.4/ Personalization SFP
FDP_ACF.1.3/Signature creation SFP

[56] Following table lists the SFRs not mentioned in the [SSCD PP] [6] but included in this Security Target due to the CC interpretation 065

FMT_SMF.1

[57] The Table 7 shows that all the SFRs are satisfied by at least one TSF and that every TSF is used to satisfy at least one SFR.

.

6.1. TOE Security Functions

This part lists the TOE Security Functions. They are grouped as shown in the table below:

FAMILY	SECURITY FUNCTION	DESCRIPTION
Identification and Authentication	SF.AUTH SF.RAD	Authentication functions RAD management
Access Control	SF.AC	Access Control
Key Management and Cryptography	SF.KEY_GEN SF.HASH SF.MAC SF.SIGN	Key Generation Hash computation MAC computation Crypto functions
Secure Messaging	SF.SM	Secure Messaging
Stored Data Protection	SF.OBS_A SF.INT_A SF.DATA_ERASE SF.TRANSACTION	Un-observability TOE logical integrity Secure destruction of the data Anti-tearing function
Test	SF.TEST	Self Test and Audit
Failure	SF.EXCEPTION	Error message and exception
TOE life cycle	SF.LIFE_CYCLE	TOE life phase management

Table 4: List of TOE security functions

6.1.1. Identification and authentication

SF.AUTH				
[58] This function updates the security status, after a successful internal or external authentication. The external authenticate requires a challenge generated by the TOE by means of a random number generator implemented in the IC which is compliant with [13]. The internal authenticate requires a challenge generated by the IFD. Both internal and external authentications use the DES, TripleDES or RSA. The user authentication is realized with the PIN. This function is realized by a permutation mechanism. The strength of this function is SOF High.				
MAPPED TOE SFRS				
FDP	FDP	FIA	FMT	FTP
ETC.1.1 SVD Transfer	**ACC.1.1 Signature Creation SFP**	**AFL.1.1**	**MTD.1.1**	**ITC.1.1 SVD Transfer**
ETC.1.2 SVD Transfer	**ACF.1.2 Initialization SFP**	**AFL.1.2**	**SMF.1.1**	**ITC.1.2 SVD Transfer**
ITC.1.1. DTBS	**ACF.1.4 Initialization SFP**	**UAU.1.1**		**ITC.1.3 SVD Transfer**
ITC.1.2. DTBS	**ACF.1.2 SVD Transfer SFP**	**UAU.1.2**		**ITC.1.1 DTBS Import**
ITC.1.3. DTBS	**ACF.1.2 Personalization SFP**	**UID.1.1**		**ITC.1.2 DTBS Import**
ACC.1.1 SVD Transfer SFP	**ACF.1.2 Signature Creation SFP**	**UID.1.2**		**ITC.1.3 DTBS Import**
ACC.1.1 Initialization SFP	**ACF.1.4 Signature Creation SFP**			**TRP.1.1 TOE**
ACC.1.1 Personalization SFP				**TRP.1.2 TOE**
				TRP.1.3 TOE

SF.RAD
[59] This function controls all operations related to the Reference Authentication Data (RAD) management. It includes the verification, unblock, and change of the RAD.
[60] Verification - In case a user is successfully identified, the TOE verify that his VAD corresponds to RAD related to the user claimed identity; - If the user claimed to be the Administrator, his VAD is checked by the TOE against RAD_A value: if the comparison succeed the user is uniquely identified and authenticated as the Administrator; - If the user claimed to be the Signatory, his VAD is checked by the TOE with RAD_S value: if the comparison succeed the user is uniquely identified and authenticated as the Signatory. - In case the verification is not successful, the TOE records this condition decrementing the Retry Counter of the RAD. When the value of the Retry Counter reaches 0, the RAD's state is Blocked. A blocked RAD is no more available for verification.
[61] Unblock - The Unblock function can be performed only if the security status satisfies the security attributes for this command. - The Unblock function resets the RAD retry counter to its initial value. - After a successful unblocks, the RAD may be used for verification.
[62] Change - This function replaces the RAD stored in the TOE with a new RAD sent by the IFD. - The Change function can be performed only if the security status satisfies the security attributes for this command.

MAPPED TOE SFRs			
FDP	**FIA**	**FMT**	**FTP**
ACC.1.1 SVD Transfer SFP	**AFL.1.1**	**MTD.1.1**	**ITC.1.1 SVD Transfer**
ACC.1.1 Initialization SFP	**AFL.1.2**		**ITC.1.2 SVD Transfer**
ACC.1.1 Personalization SFP			**ITC.1.3 SVD Transfer**
ACC.1.1 Signature Creation SFP			**ITC.1.1 DTBS Import**
ACF.1.2 Initialization SFP			**ITC.1.2 DTBS Import**
ACF.1.4 Initialization SFP			**ITC.1.3 DTBS Import**
ACF.1.2 SVD Transfer SFP			**TRP.1.1 TOE**
ACF.1.2 Personalization SFP			**TRP.1.2 TOE**
ACF.1.2 Signature Creation SFP			**TRP.1.3 TOE**
ACF.1.4 Signature Creation SFP			

6.1.2. Access Control

SF.AC			
[63] This function compares the security status to process commands and / or to access files and data objects. The security status represents the current state possibly achieved after completion of the answer to reset and a possible protocol and parameter selection and / or a single command or a sequence of commands possibly performing authentication procedures. The security attributes, when they exist, define which actions are allowed, and under which conditions. For example: • To authorized user is allowed generate the SCD/SVD key pair • To authorized user is allowed export the SVD • To the "Administrator" is allowed the management of the SCD/SVD security attributes • To the "Administrator" is allowed the creation of the RAD_S • To the "Signatory" is allowed sign DTBS-representation • To the "Signatory" is allowed change in ***"active"*** the operational state of the SCD			
MAPPED TOE SFRs			
FDP	**FDP**	**FMT**	**FIA**
ACC.1.1 SVD Transfer SFP	**ACF.1.2 SVD Transfer SFP**	**MOF.1.1.**	**ATD.1.1**
ACC.1.1 Initialization SFP	**ACF.1.1 Personalization SFP**	**MSA.1.1 Administrator**	
ACC.1.1 Personalization SFP	**ACF.1.2 Personalization SFP**	**MSA.1.1 Signatory**	
ACC.1.1 Signature Creation SFP	**ACF.1.1 Signature Creation SFP**	**MSA.2.1**	
ACF.1.1 Initialization SFP	**ACF.1.2 Signature Creation SFP**	**MSA.3.1**	
ACF.1.2 Initialization SFP	**ACF.1.4 Signature Creation SFP**	**MSA.3.2**	
ACF.1.4 Initialization SFP		**MTD.1.1**	
ACF.1.1 SVD Transfer SFP		**SMF.1.1**	
		SMR.1.1	
		SMR.1.2	

6.1.3. Key Management and Cryptography

SF.KEY_GEN		
[64]	This function generates the SCD/SVD pair according to the RSA algorithm (see [5]), using a length of 1024 bits. The function checks the SCD/SVD correspondence.	
MAPPED TOE SFRs		
FCS		
CKM.1.1		
COP.1.1 correspondence		

SF.HASH		
[65]	This function generates a hashing of data, using the algorithm SHA-1. The obtained hash (160 bits) is stored in the TOE and may be used for another computation. The TOE can complete the hashing process on imported data and on intermediate hash result.	
MAPPED TOE SFRs		
FCS		
COP.1.1 signing		

SF.MAC		
[66]	This function generates a and verifies a MAC, using a DES or Triple DES with 2 or 3 keys, as defined in the following standards: FIPS 113 “Computer Data Authentication” [12].	
MAPPED TOE SFRs		
FDP	FTP	FTP
SDI.2.1. DTBS	**ITC.1.1 SVD Transfer**	**TRP.1.1 TOE**
SDI.2.2. DTBS	**ITC.1.2 SVD Transfer**	**TRP.1.2 TOE**
UIT.1.1 SVD Transfer	**ITC.1.3 SVD Transfer**	**TRP.1.3 TOE**
UIT.1.2 SVD Transfer	**ITC.1.1 DTBS Import**	
UIT.1.1 TOE DTBS	**ITC.1.2 DTBS Import**	
UIT.1.2 TOE DTBS	**ITC.1.3 DTBS Import**	

SF.SIGN		
[67]	This function signs imported data, using a RSA 1024 bits private key in conformance with the standard RSA PKCS#1 v1.5: “RSA Cryptography Standard”, 1998.	
MAPPED TOE SFRs		
FCS		
COP.1.1 signing		

6.1.4. Secure Messaging

SF.SM		
[68]	This function establishes a secure channel between the TOE and the IFD. The goal is to protect [part of] any command-response pair to and from the card by ensuring two basic security functions: data confidentiality and data authentication. The confidentiality is obtained by the encipherment of the transmitted message. This operation use DES or Triple DES with 2 or 3 Keys. The authentication uses a cryptogram based on MAC. In case of an unsuccessful authentication, a counter of the used keys is decremented in order to limit the authentication attempts.	
MAPPED TOE SFRs		
FDP	FTP	FTP
SDI.2.1. DTBS	**ITC.1.1 SVD Transfer**	**TRP.1.1 TOE**
SDI.2.2. DTBS	**ITC.1.2 SVD Transfer**	**TRP.1.2 TOE**
UIT.1.1 SVD Transfer	**ITC.1.3 SVD Transfer**	**TRP.1.3 TOE**
UIT.1.2 SVD Transfer	**ITC.1.1 DTBS Import**	
UIT.1.1 TOE DTBS	**ITC.1.2 DTBS Import**	
UIT.1.2 TOE DTBS	**ITC.1.3 DTBS Import**	

6.1.5. Stored Data Protection

SF.OBS_A		
[69]	This function addresses the TOE emanation security functional requirements. This function is mostly realized by Integrated Circuit design and implementation of the TSF. This function provides mechanism to avoid information leakage.	
MAPPED TOE SFRs		
FPT		
EMSEC.1.1.		
EMSEC.1.2		

SF.INT_A		
[70]	This function addresses the TOE logical integrity. It includes the check of the integrity of the TSF code and the integrity of the cryptographic keys, authentication data and DTBS. If an integrity error is found, depending on the type of data, the TOE may abort the current operation or may change the TOE life cycle state.	
MAPPED TOE SFRs		
FDP	FPT	FPT
SDI.2.1. Persistent	PHP.1.1	TST.1.2
SDI.2.2. Persistent	PHP.1.2	TST.1.3

SF.DATA_ERASE		
[71]	This function is responsible to erase the data. It includes mainly two types of operations: - Erase the data before starting a new working session. - Erase the data before allocation and after deallocation of sensitive data	
MAPPED TOE SFRs		
FCS	FDP	
CKM.4.1	RIP.1.1	

SF.TRANSACTION		
[72]	This function is responsible to manage the transaction of the TOE, and addresses the requirement of secure state of the TOE data. A transaction is a logical set of updates of persistent data. It is important for transactions to be *atomic*: either all of the data fields are updated, or none are.	
MAPPED TOE SFRs		
FPT		
FLS.1.1		

6.1.6. *Test*

SF.TEST		
[73]	This function ensures the tests of TOE functionality. It includes the Integrated Circuit and its environment. Depending on the test, it is executed at power-up or before/after sensitive operation. Upon detection of an anomaly, the TOE ends the working session or changes its life cycle state.	
MAPPED TOE SFRs		
FPT	FPT	
AMT.1.1	PHP.1.2	
FLS.1.1	PHP.3.1	
PHP.1.1	TST.1.1	

6.1.7. *Failure*

SF.EXCEPTION		
[74]	This function addresses the exception management. The reasons of these exceptions are: range of operating conditions, integrity errors, life cycle and TOE internal audit failure. Upon detection, depending on the exception reason, the current operation is aborted; the TOE life cycle is changed.	
MAPPED TOE SFRs		
FDP	FPT	FPT
SDI.2.1. Persistent	FLS.1.1	PHP.1.2
SDI.2.2. Persistent	PHP.1.1	PHP.3.1

6.1.8. *TOE Life Cycle*

SF.LIFE_CYCLE		
[75]	This function manages the TOE life cycle, as described in chapter *2.3 TOE life cycle*. It ensures the detection of the current state and the switching of the state. The change of phase is irreversible.	
MAPPED TOE SFRs		
FDP	FPT	FPT
SDI.2.1. Persistent	FLS.1.1	PHP.1.2
SDI.2.2. Persistent	PHP.1.1	PHP.3.1

6.2. Assurance Measures

[76] Appropriate assurance measures have been and are being employed to meet the assurance requirements for the Common Criteria EAL4 evaluation level augmented with AVA_VLA.4 and AVA_MSU.3 components.

7 SSCD PP Claims

[77] INCRYPTO34v2 conforms to the requirements of SSCD PP [6].

7.1. PP reference

[78] The ST is in compliance with the SSCD PP [6], identified as follows:

Title:	Protection Profile — Secure Signature-Creation Device Type 3
Authors:	Wolfgang Killmann, Herbert Leitold, Reinhard Posch, Patrick Sallé, Bruno Baronnet
Vetting Status:	
CC Version:	2.1 Final
General Status:	Approved by WS/E-SIGN on 2001-11-30
Version Number:	1.05
Registration:	BSI-PP-0006-2002
Keywords:	Secure signature-creation device, electronic signature

7.2. PP tailoring

[79] Tables in chapter 5 identifies each SFR for this Security Target and the tailoring operations performed relative to [SSCD PP] [6]. The tailoring is identified ***bold italics*** within the text of each SFR. All of the tailoring operations performed are in conformance with the assignment and selections in [SSCD PP] [6].

7.3. PP additions

[80] This Security Target includes one additional security objective for the non-IT environment **OE.Op_Phase** in 4.2.1.

[81] Due to CC interpretation 065 this Security Target includes one additional TOE security functional requirement **FMT_SMF.1** in 5.1.5.6.

[82] Due to the fact that both TOE Administrator and Signatory are identified and authenticated using the same mechanism, i.e. the verification of their PIN against a stored RAD, RAD Asset of [SSCD PP] [6] has been split in RAD_A and RAD_S, which have the same security need.

[83] **A.PERSONALIZATION** states that the TOE personalization must be performed in the observance of proper physical and procedural measures.

[84] **A.MANAGE** states that the TOE secure personalization in *SC Personalization* state and its secure disposal, after having entered *SC End of Use* state, are managed under responsibility of competent and trusted Administrator, according to the Administration Documentation.

[85] **A.VAD** covers the procedural measures needed for the secure distribution of PIN codes to related TOE users.

8 Rationale

8.1. Security Objectives Rationale

8.1.1. Security Objectives Coverage.

[86] As for [SSCD PP] [6] § 6.2.1

Threats - Assumptions - Policies / Security objectives	OT.EMESEC_Design	OT.Lifecycle_Security	OT.Init	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure	OE.CGA_QCert	OE.SVD_Auth_CGA	OE.HI_VAD	OE.SCA_Data_Intend	OE.OP_Phase
T.Hack_Phys	√			√			√	√									
T.SCD_Divulg				√													
T.SCD_Derive									√			√					
T.SVD_Forgery						√								√			
T.DTBS_Forgery										√						√	
T.SigF_Misuse										√	√				√	√	
T.Sig_Forgery	√	√		√	√	√	√	√				√	√	√		√	
T.Sig_Repud	√	√		√	√	√	√	√	√	√	√	√	√	√		√	
A.CGA													√	√			
A.SGA																√	
A.Personalization																	√
A.Manage																	√
A.VAD																	√
P.CSP_QCert					√								√				
P.QSign											√	√	√			√	
P.Sigy_SSCD			√						√		√						

Table 5: Threats, Assumptions and Policy to Security objective mapping

8.1.2. Security Objectives Sufficiency.

[87] As for [SSCD PP] [6] § 6.2.2 with the addition of the paragraph 8.1.2.2.

8.1.2.2. Additional assumptions and Security Objective Sufficiency

[88] **A.PERSONALIZATION (TOE personalization data integrity, confidentiality and availability)** establishes the trustworthiness of the personalization data, RAD, secret Key etc., stored in the TOE. This is addressed by the security objective for the non-IT environment OE.Op_Phase (*TOE operational phase security*), which ensures the security of the TOE during personalization.

[89] **A.MANAGE (TOE lifecycle state management)** enforces the security required during the whole operational phase of the TOE. It establishes that the TOE's operational phase is under the full control of competent user and trusted TOE administrator. This is addressed by the security objective for the non-IT environment OE.Op_Phase (*TOE operational phase security*), which ensures the security of the TOE by proper administration and proper usage.

[90] **A.VAD (TOE VAD delivery)** establishes that a secure user VAD delivery enforces the security needed for the identification and authentication procedures. This is addressed by the security objective for the non-IT environment OE.Op_Phase (*TOE operational phase security*), which ensures that only authorized and legitimate TOE users receive the VAD required to use the signature generation TOE functionality.

8.2. Security Requirements Rationale

8.2.1. Security Requirements coverage

[91] There are no additional security objectives. Therefore, this Security Target fully complies with [SSCD PP] [6].

[92] Due to CC interpretation 065 this Security Target includes one additional TOE security functional requirement **FMT_SMF.1** in 5.1.5.6. This Security Target fully complies with [SSCD PP] [6] § 6.3.1 with the following line added to the table 6.2 in [SSCD PP] [6] § 6.3.1.

TOE Security Functional Requirement / TOE Security objectives	OT.EMESEC_Design	OT.Lifecycle_Security	OT.Init	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure
FMT_SMF.1			√	√							√	

8.2.2. TOE Security Requirements sufficiency

[93] This Security Target fully complies with [SSCD PP] [6] § 6.3.2.1 with the additions to the justification for **OT.Init**, **OT.SCD_Secrecy** and **OT.Sigy_SigF** to reflect the additional TOE security functional requirement **FMT_SMF.1 :**

[94] **OT.Init (SCD/SVD generation):** The management specification for Identification and Authentication and access control is provided by **FMT_SMF.1**

[95] **OT.SCD_Secrecy (Secrecy of signature-creation data):** The management specification for Identification and Authentication and access control is provided by **FMT_SMF.1**

[96] **OT.Sigy_SigF (Signature generation function for the legitimate signatory only):** The management specification for Identification and Authentication and access control is provided by **FMT_SMF.1**

8.2.3. Assurance Requirements Suitability

[97] According to [SSCD PP] [6], the target assurance level is EAL4 augmented by AVA_MSU.3 and AVA_VLA.4 assurance components.

[98] The TOE includes the ST19XL34P ICC HW platform, which is evaluated against [PP9806] [7] with assurance level EAL4 augmented by AVA_VLA.4, ADV_IMP.2 and ALC_DVS.2 assurance components.

[99] The fact that HW platform evaluation result refers to AVA_MSU.2 assurance component instead of AVA_MSU.3 included in [SSCD PP] [6], does not weaken TOE evaluation results since HW platform MSU is not addressed to TOE end user but to TOE embedded SW developer.

8.3. TOE Summary Specification Rationale

[100] The TOE summary specification rationale is intended to show that the TOE security functions and assurance measures are suitable to meet the TOE security (functional and assurance) requirements.

[101] To show that the selection of TOE security functions and assurance measures are suitable to meet TOE security requirements (functional and assurance), it is important to demonstrate the following:

[102] 1) that the combination of specified TOE IT security functions work together so as to satisfy the TOE security functional requirements;

[103] 2) that the strength of TOE function claims made are valid, or that assertions that such claims are unnecessary are valid.

[104] 3) that the claim is justified that the stated assurance measures are compliant with the assurance requirements.

8.3.2. TOE Security Functions rationale

Following Tables demonstrates that TOE Security Functions address at least one SFR and that for each SFR the TOE Security Functions are suitable to meet the SFR, and the combination of TOE Security functions work together so as to satisfy the SFR:

FAMILY	SFRs	TOE SECURITY FUNCTIONS RATIONALE	
FCS	CKM.1.1	[105]	**SF.KEY_GEN** grants the FCS_CKM.1.1 satisfaction specifying that the TOE correctly internally generate a key of length 1024 bit for the RSA algorithms.
	CKM.4.1	[106]	**SF.DATA_ERASE** grants the FCS_CKM.4.1 satisfaction specifying that the TOE correctly erase the data before allocation and after deallocation of sensitive data. Once the data are erased from memory is not more possible to retrieve them.
	COP.1.1/CORRESP	[107]	**SF.KEY_GEN** grants the FCS_COP.1.1/CORRESP satisfaction specifying that the TOE moreover to correctly produce RSA key of length 1024 bit, perform a check to verify the SCD/SVD correspondence.
	COP.1.1/SIGNING	[108]	**SF.SIGN** grants the FCS_COP.1.1/SIGNING satisfaction specifying that the TOE correctly perform a digital signature generation using a key of length 1024 bit and the RSA algorithms.
		[109]	**SF.HASH** contributes to FCS_COP.1.1/SIGNING satisfaction. This function generates a hashing of data, using the algorithm SHA-1.
FDP	ACC.1.1 SVD Transfer SFP	[110]	**SF.AC** contributes to FDP_ACC.1.1 SVD Transfer SFP satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed transfer SVD for certification purposes. This function compares the security status required to process the command and allows or denies the SVD transfer.
		[111]	**SF.AUTH** grants the FDP_ACC.1.1 SVD Transfer SFP satisfaction. This function addresses the user authentication by the TOE allowing or denying the SVD transfer. The user authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACC.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
		[112]	**SF.RAD** contributes to FDP_ACC.1.1 SVD Transfer SFP satisfaction. The function acts as a support mechanism in the user authentication process. The function performs a match between a VAD and a RAD stored in the TOE. The function is executed in a secure manner.

	ACC.1.1 Initialization SFP	[113]	**SF.AC** contributes to FDP_ACC.1.1 Initialization SFP satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed generate the SCD/SVD key pair. This function compares the security status required to process the command and allows or denies the SCD/SVD key pair generation.
		[114]	**SF.AUTH** grants the FDP_ACC.1.1 Initialization SFP satisfaction. This function addresses the user authentication by the TOE allowing or denying the SCD/SVD key pair generation. The user authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACC.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
		[115]	**SF.RAD** contributes to FDP_ACC.1.1 Initialization SFP satisfaction. The function acts as a support mechanism in the user authentication process. The function performs a match between a VAD and a RAD stored in the TOE. The function is executed in a secure manner.
	ACC.1.1 Personalization SFP	[116]	**SF.AC** contributes to FDP_ACC.1.1 Personalization SFP satisfaction. The function specifies that, during TOE Operational phase only to the "Administrator" is allowed create the RAD_S. This function compares the security status required to process the command and allows or denies the RAD_S creation.
		[117]	**SF.AUTH** grants the FDP_ACC.1.1 Personalization SFP satisfaction. This function addresses the "Administrator" authentication by the TOE allowing or denying the RAD_S creation. The "Administrator" authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACC.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
		[118]	**SF.RAD** contributes to FDP_ACC.1.1 Personalization SFP satisfaction. The function acts as a support mechanism in the "Administrator" authentication process. The function performs a match between a VAD and the RAD_A stored in the TOE. The function is executed in a secure manner.
	ACC.1.1 Signature Creation SFP	[119]	**SF.AUTH** grants the FDP_ACC.1.1 Signature Creation SFP satisfaction. The function grants that only to the "Signatory" is allowed to sign the DTBS-representation sent by an authorized SCA. This function addresses the SCA authentication. Moreover this function addresses the "Signatory" authentication by the TOE allowing or denying the DTBS sign functionality. The "Signatory" authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACC.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
		[120]	**SF.AC** contributes to FDP_ACC.1.1 Signature Creation SFP satisfaction. The function specifies that, during TOE Operational phase only to the "Signatory" is allowed sign DTBS-representation. This function compares the security status required to process the command and allows or denies the DTBS-representation signing.
		[121]	**SF.RAD** contributes to FDP_ACC.1.1 Signature Creation SFP satisfaction. The function acts as a support mechanism in the "Signatory" authentication process. The function performs a match between a VAD and the RADs stored in the TOE. The function is executed in a secure manner.

	ACF.1.1 Initialization SFP	[122]	**SF.AC** contributes to FDP_ACF.1.1 Initialization SFP satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed generate the SCD/SVD key pair. This function compares the security status required to process the command and allows or denies the SCD/SVD key pair generation.
	ACF.1.2 Initialization SFP	[123]	**SF.AC** contributes to FDP_ACF.1.2 Initialization SFP satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed generate the SCD/SVD key pair. This function compares the security status required to process the command and allows or denies the SCD/SVD key pair generation.
		[124]	**SF.AUTH** grants the FDP_ACF.1.2 Initialization SFP satisfaction. This function addresses the user authentication by the TOE allowing or denying the SCD/SVD key pair generation. The user authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACF.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
		[125]	**SF.RAD** contributes to FDP_ACF.1.2 Initialization SFP satisfaction. The function acts as a support mechanism in the user authentication process. The function performs a match between a VAD and a RAD stored in the TOE. The function is executed in a secure manner.
	ACF.1.3 Initialization SFP	**NONE**	
	ACF.1.4 Initialization SFP	[126]	**SF.AC** contributes to FDP_ACF.1.4 Initialization SFP satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed generate the SCD/SVD key pair. This function compares the security status required to process the command and allows or denies the SCD/SVD key pair generation.
		[127]	**SF.AUTH** grants the FDP_ACF.1.4 Initialization SFP satisfaction. This function addresses the user authentication by the TOE allowing or denying the SCD/SVD key pair generation. The user authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACF.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
		[128]	**SF.RAD** contributes to FDP_ACF.1.4 Initialization SFP satisfaction. The function acts as a support mechanism in the user authentication process. The function performs a match between a VAD and a RAD stored in the TOE. The function is executed in a secure manner.
	ACF.1.1 SVD Transfer SFP	[129]	**SF.AC** grants the FDP_ACF.1.1 SVD Transfer SFP satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed transfer SVD for certification purposes. This function compares the security status required to process the command and allows or denies the SVD transfer.

	ACF.1.2 SVD Transfer SFP	[130]	**SF.AC** contributes to FDP_ACF.1.2 SVD Transfer SFP satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed transfer SVD for certification purposes. This function compares the security status required to process the command and allows or denies the SVD transfer.
		[131]	**SF.AUTH** grants the FDP_ACF.1.2 SVD Transfer SFP satisfaction. This function addresses the user authentication by the TOE allowing or denying the SVD transfer. The user authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACF.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
		[132]	**SF.RAD** contributes to FDP_ACF.1.2 SVD Transfer SFP satisfaction. The function acts as a support mechanism in the user authentication process. The function performs a match between a VAD and a RAD stored in the TOE. The function is executed in a secure manner.
	ACF.1.3 SVD Transfer SFP	**NONE**	
	ACF.1.4 SVD Transfer SFP	**NONE**	
	ACF.1.1 Personalization SFP	[133]	**SF.AC** grants to FDP_ACF.1.1 Personalization SFP satisfaction. The function specifies that, during TOE Operational phase only to the “Administrator” is allowed create the RAD_S. This function compares the security status required to process the command and allows or denies the RAD_S creation.
	ACF.1.2 Personalization SFP	[134]	**SF.AC** contributes to FDP_ACF.1.2 Personalization SFP satisfaction. The function specifies that, during TOE Operational phase only to the “Administrator” is allowed create the RAD_S. This function compares the security status required to process the command and allows or denies the RAD_S creation.
		[135]	**SF.AUTH** grants the FDP_ACF.1.2 Personalization SFP satisfaction. This function addresses the “Administrator” authentication by the TOE allowing or denying the RAD_S creation. The “Administrator” authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACF.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
		[136]	**SF.RAD** contributes to FDP_ACF.1.2 Personalization SFP satisfaction. The function acts as a support mechanism in the “Administrator” authentication process. The function performs a match between a VAD and the RAD_A stored in the TOE. The function is executed in a secure manner.
	ACF.1.3 Personalization SFP	**NONE**	
	ACF.1.4 Personalization SFP	**NONE**	
	ACF.1.1 Signature Creation SFP	[137]	**SF.AC** grants to FDP_ACF.1.1 Signature Creation SFP satisfaction. The function specifies that, during TOE Operational phase only to the “Signatory” is allowed sign DTBS-representation. This function compares the security status required to process the command and allows or denies the DTBS-representation signing.

	ACF.1.2 Signature Creation SFP	[138] **SF.AUTH** grants the FDP_ACF.1.2 Signature Creation SFP satisfaction. The function grants that only to the "Signatory" is allowed to sign the DTBS-representation sent by an authorized SCA. This function addresses the SCA authentication. Moreover this function addresses the "Signatory" authentication by the TOE allowing or denying the DTBS sign functionality. The "Signatory" authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACF.1.because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack. [139] **SF.AC** contributes to FDP_ACF.1.2 Signature Creation SFP satisfaction. The function specifies that, during TOE Operational phase only to the "Signatory" is allowed sign DTBS-representation. This function compares the security status required to process the command and allows or denies the DTBS-representation signing. [140] **SF.RAD** contributes to FDP_ACF.1.2 Signature Creation SFP satisfaction. The function acts as a support mechanism in the "Signatory" authentication process. The function performs a match between a VAD and the RADs stored in the TOE. The function is executed in a secure manner.
	ACF.1.3 Signature Creation SFP	**NONE**
	ACF.1.4 Signature Creation SFP	[141] **SF.AUTH** grants the FDP_ACF.1.4 Signature Creation SFP satisfaction. The function grants that only to the "Signatory" is allowed to sign the DTBS-representation sent by an authorized SCA. This function addresses the SCA authentication. Moreover this function addresses the "Signatory" authentication by the TOE allowing or denying the DTBS sign functionality. The "Signatory" authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FDP_ACF.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack. [142] **SF.AC** contributes to FDP_ACF.1.4 Signature Creation SFP satisfaction. The function specifies that, during TOE Operational phase only to the "Signatory" is allowed sign DTBS-representation. This function compares the security status required to process the command and allows or denies the DTBS-representation signing. [143] **SF.RAD** contributes to FDP_ACF.1.4 Signature Creation SFP satisfaction. The function acts as a support mechanism in the "Signatory" authentication process. The function performs a match between a VAD and the RADs stored in the TOE. The function is executed in a secure manner.
	ETC.1.1 SVD Transfer	[144] **SF.AUTH** grants the FDP_ETC.1.1 SVD Transfer satisfaction. The function grants that the SVD is transferred only towards an authorized CGA. This function addresses the CGA authentication. No security attributes is transferred or visible externally to the TCS.
	ETC.1.2 SVD Transfer	[145] **SF.AUTH** grants the FDP_ETC.1.2 SVD Transfer satisfaction. The function grants that the SVD is transferred only towards an authorized CGA. This function addresses the CGA authentication. No security attributes is transferred or visible externally to the TCS.
	ITC.1.1. DTBS	[146] **SF.AUTH** grants the FDP_ITC.1.1 DTBS satisfaction. The function grants that the TOE signs only DTBS-representation sent by an authorized SCA. This function addresses the SCA authentication.
	ITC.1.2. DTBS	[147] **SF.AUTH** grants the FDP_ITC.1.2 DTBS satisfaction. The function grants that the TOE signs only DTBS-representation sent by an authorized SCA. This function addresses the SCA authentication.

	ITC.1.3. DTBS	[148]	**SF.AUTH** grants the FDP_ITC.1.3 DTBS satisfaction. The function grants that the TOE signs only DTBS-representation sent by an authorized SCA. This function addresses the SCA authentication.
	RIP.1.1	[149]	**SF.DATA_ERASE** grants the FDP_RIP.1.1 satisfaction making unavailable any residual information related to the SCD/RAD/VAD.This function erase the sensitive data before starting a new working session, before allocation and after deallocation.
	SDI.2.1. Persistent	[150]	**SF.INT_A** grants the FDP_SDI.2.1 Persistent satisfaction. This function addresses the TOE data integrity. When an integrity error is found an exception rises. The TOE aborts the current operation and may change the TOE life cycle state. The TOE notifies the abnormal condition externally.
		[151]	**SF.EXCEPTION** contributes to FDP_SDI.2.2 Persistent satisfaction. The function acts as a support mechanism for the TOE's internal data integrity. The function addresses the exception management.
		[152]	**SF.LIFE_CYCLE** contributes to FDP_SDI.2.2 Persistent satisfaction. The function acts as a support mechanism. The function addresses the TOE's life cycle state changes.
	SDI.2.2. Persistent	[153]	**SF.INT_A** grants the FDP_SDI.2.2 Persistent satisfaction. This function addresses the TOE data integrity. When an integrity error is found an exception rises. The TOE aborts the current operation and may change the TOE life cycle state. The TOE notifies the abnormal condition externally.
		[154]	**SF.EXCEPTION** contributes to FDP_SDI.2.2 Persistent satisfaction. The function acts as a support mechanism for the TOE's internal data integrity. The function addresses the exception management.
		[155]	**SF.LIFE_CYCLE** contributes to FDP_SDI.2.2 Persistent satisfaction. The function acts as a support mechanism. The function addresses the TOE's life cycle state changes.
	SDI.2.1. DTBS	[156]	**SF.SM** grants the FDP_SDI.2.1 DTBS satisfaction. The DTBS integrity is checked before its use. When an integrity error is found the TOE aborts the current operation and notifies the condition externally.
		[157]	**SF.MAC** contributes to FDP_SDI.2.1 DTBS satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES or the Triple DES algorithm.
	SDI.2.2. DTBS	[158]	**SF.SM** grants the FDP_SDI.2.2 DTBS satisfaction. The DTBS integrity is checked before its use. When an integrity error is found the TOE aborts the current operation and notifies the condition externally.
		[159]	**SF.MAC** contributes to FDP_SDI.2.2 DTBS satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES or the Triple DES algorithm.
	UIT.1.1 SVD Transfer	[160]	**SF.SM** grants the FDP_UIT.1.1 SVD Transfer satisfaction. To prevent the data to be altered the TOE protects the transmitted data using integrity and authentication mechanisms.
		[161]	**SF.MAC** contributes FDP_UIT.1.1 SVD Transfer satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES or the Triple DES algorithm.

	UIT.1.2 SVD Transfer	[162]	**SF.SM** grants the FDP_UIT.1.2 SVD Transfer satisfaction. To prevent the data to be altered the TOE protects the transmitted data using integrity and authentication mechanisms.
		[163]	**SF.MAC** contributes FDP_UIT.1.2 SVD Transfer satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES or the Triple DES algorithm.
	UIT.1.1 TOE DTBS	[164]	**SF.SM** grants the FDP_UIT.1.1 TOE DTBS satisfaction. The DTBS integrity is checked before its use. When an integrity error is found the TOE aborts the current operation and notifies the condition externally.
		[165]	**SF.MAC** contributes to FDP_UIT.1.1 TOE DTBS satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES or the Triple DES algorithm.
	UIT.1.2 TOE DTBS	[166]	**SF.SM** grants the FDP_UIT.1.2 TOE DTBS satisfaction. The DTBS integrity is checked before its use. When an integrity error is found the TOE aborts the current operation and notifies the condition externally.
		[167]	**SF.MAC** contributes to FDP_UIT.1.2 TOE DTBS satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES or the Triple DES algorithm.
FIA	AFL.1.1	[168]	**SF.AUTH** grants the FIA_AFL.1.1 satisfaction. This function addresses the user authentication. The user authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
		[169]	**SF.RAD** contributes to FIA_AFL.1.1 satisfaction. The function acts as a support mechanism in the user authentication process. The function performs a match between a VAD and a RAD stored in the TOE. The function is executed in a secure manner.
	AFL.1.2	[170]	**SF.AUTH** grants the FIA_AFL.1.2 satisfaction. This function addresses the user authentication. The user authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
		[171]	**SF.RAD** contributes to FIA_AFL.1.2 satisfaction. The function acts as a support mechanism in the user authentication process. The function performs a match between a VAD and a RAD stored in the TOE. When the user authentication attempts reach the 3 consecutive retries then the relevant RAD is blocked. The function is executed in a secure manner.
	ATD.1.1	[172]	**SF.AC** grants the FIA_ATD.1.1 satisfaction. This function specifies that it is possible define in the TOE, relate to each user profile, security attributes based on RAD. These attributes are valid and active for the whole TOE Operational phase.

	UAU.1.1	[173]	**SF.AUTH** grants the FIA_UAU.1.1 satisfaction. The TOE requires that a user is successfully identified and authenticated before allowing any command execution on behalf of that user. In particular, before identifying and authenticating a user, the TOE allows only the execution of an ***"AUTHENTICATION"*** command in order to establish a trusted channel/path. The SOF-High claim of SF.AUTH is adequate for FIA_UAU.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
	UAU.1.2	[174]	**SF.AUTH** grants the FIA_UAU.1.2 satisfaction. The TOE requires that a user is successfully identified and authenticated before allowing any command execution on behalf of that user. In particular, before identifying and authenticating a user, the TOE allows only the execution of an ***"AUTHENTICATION"*** command in order to establish a trusted channel/path. The SOF-High claim of SF.AUTH is adequate for FIA_UAU.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
	UID.1.1	[175]	**SF.AUTH** grants the FIA_UID.1.1 satisfaction. The TOE requires that a user is successfully identified and authenticated before allowing any command execution on behalf of that user. In particular, before identifying and authenticating a user, the TOE allows only the execution of an ***"AUTHENTICATION"*** command in order to establish a trusted channel/path. The SOF-High claim of SF.AUTH is adequate for FIA_UID.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
	UID.1.2	[176]	**SF.AUTH** grants the FIA_UID.1.2 satisfaction. The TOE requires that a user is successfully identified and authenticated before allowing any command execution on behalf of that user. In particular, before identifying and authenticating a user, the TOE allows only the execution of an ***"AUTHENTICATION"*** command in order to establish a trusted channel/path. The SOF-High claim of SF.AUTH is adequate for FIA_UID.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
FMT	MOF.1.1.	[177]	**SF.AC** grants the FMT_MOF.1.1 satisfaction. The function specifies that, during TOE Operational phase only to the "Signatory" is allowed sign DTBS-representation. This function compares the security status required to process the command and allows or denies the DTBS-representation signing.
	MSA.1.1 Administrator	[178]	**SF.AC** grants the FMT_MSA.1.1 Administrator satisfaction. The function specifies that, during TOE Operational phase only to the "Administrator" is allowed the management of the SCD/SVD security attributes. This function compares the security status required to process the command and allows or denies the SCD/SVD security attributes management.
	MSA.1.1 Signatory	[179]	**SF.AC** grants the FMT_MSA.1.1 Signatory satisfaction. The function specifies that, during TOE Operational phase only to the "Signatory" is allowed to change in ***"active"*** the operational state of the SCD. This function compares the security status required to process the command and allows or denies the SCD operational state change.
	MSA.2.1	[180]	**SF.AC** grants the FMT_MSA.2.1 satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed to set and change security attributes. Moreover the function specifies that the security attribute change is possible only when the change doesn't compromise the TOE security state. This function compares the security status required to process the command and allows or denies the set or the change of the security attributes.

	MSA.3.1	[181]	**SF.AC** grants the FMT_MSA.3.1 satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed to set and change security attributes. This function compares the security status required to process the command and allows or denies the set or the change of the security attributes. When the SCD is generated it is recommended that the authorized user set the SCD's security attribute "SCD operational" to "no".
	MSA.3.2	[182]	**SF.AC** grants the FMT_MSA.3.2 satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed to set and change security attributes. This function compares the security status required to process the command and allows or denies the set or the change of the security attributes. At object creation time the "Administrator" decides the security attributes related to the created object.
	MTD.1.1	[183]	**SF.AUTH** grants the FMT_MTD.1.1 satisfaction. The function grants that only to the "Signatory is allowed change the RAD_S. This function addresses the "Signatory" authentication by the TOE allowing or denying the RAD change functionality. The "Signatory" authentication is based on PIN mechanism. The SOF-High claim of SF.AUTH is adequate for FMT_MTD.1 because the required minimum PIN length of 6 together with the low number of possible authentication attempts defined by FIA_AFL.1.1 to be 3 prevents successful PIN attack.
		[184]	**SF.AC** contributes to FMT_MTD.1.1 satisfaction. The function specifies that, during TOE Operational phase only to the "Signatory" is allowed change the RAD_S. This function compares the security status required to process the command and allows or denies the change of the RAD_S.
		[185]	**SF.RAD** contributes to FMT_MTD.1.1 satisfaction. The function acts as a support mechanism in the "Signatory" authentication process. The function performs a match between a VAD and the RADs stored in the TOE. The function is executed in a secure manner.
	SMF.1.1[5]	[186]	**SF.AUTH** grants the FMT_SMF.1.1 satisfaction. The function specifies that, during TOE Operational phase a user must be successfully identified and authenticated before allowing any command execution on behalf of that user.
		[187]	**SF.AC** contributes to the FMT_SMF.1.1 satisfaction. The function specifies that, during TOE Operational phase only to authorized user is allowed to have access to TOE's resources. Each TOE's resources has security attributes assigned. This function compares the security status required to process the command on the relevant TOE's resource and allows or denies the execution of the command.
	SMR.1.1	[188]	**SF.AC** grants the FMT_SMR.1.1 satisfaction. The function specifies that, during TOE Operational phase only to users with role set to "Signatory" or "Administrator" is allowed to interact with the TOE
	SMR.1.2	[189]	**SF.AC** grants the FMT_SMR.1.2 satisfaction. The function specifies that, during TOE Operational phase only to users with role set to "Signatory" or "Administrator" is allowed to interact with the TOE.
FPT	AMT.1.1	[190]	**SF.TEST** grants the FPT_AMT.1.1 satisfaction This function specifies that, during the whole TOE Operational phase, at each TOE start-up, a suit of TOE's internal components tests are performed.
	EMSEC.1.1	[191]	**SF.OBS_A** grants the FPT_EMESEC.1.1 satisfaction. This function assures that, during the whole TOE Operational phase, the TOE will not emit electrical signals that an attacker can easily exploit to gain access to the RAD and SCD stored in the TOE. This function is mainly implemented by IC platform mechanisms.

[5] This SFR has been added as suggested in the CC interpretation 065

	EMSEC.1.2	[192]	**SF.OBS_A** grants the FPT_EMESEC.2.1 satisfaction. This function assures that, during the whole TOE Operational phase, the TOE will not permit the user to gain access to the RAD and SCD stored in the TOE through external physical contacts.
	FLS.1.1	[193]	**SF.TEST** grants the FPT_FLS.1.1 satisfaction. This function is mainly implemented by IC platform mechanisms. The function assures that the TOE is operative only when the physical operating parameters are in the accepted range. On test fail an exception rises. The TOE aborts the current operation and may change the TOE life cycle state.
		[194]	**SF.EXCEPTION** contributes to FPT_FLS.1.1 satisfaction. The function acts as a support mechanism for the TOE's operating condition and internal data integrity. The function addresses the exception management.
		[195]	**SF.LIFE_CYCLE** contributes to FPT_FLS.1.1 satisfaction. The function acts as a support mechanism. The function addresses the TOE's life cycle state changes.
		[196]	**SF.TRANSACTION** contributes to FPT_FLS.1.1 satisfaction. The function acts as a support mechanism. The function addresses the atomicity of the TOE transactions.
	PHP.1.1	[197]	**SF.TEST** grants the FPT_PHP.1.1 satisfaction. This function detects the TOE chip integrity violation. When an integrity error is detected an exception rises. The TOE aborts the current operation and may change the TOE life cycle state.
		[198]	**SF.INT_A** contributes to FPT_PHP.1.1 satisfaction. This function addresses the TOE data integrity.
		[199]	**SF.EXCEPTION** contributes to FPT_PHP.1.1 satisfaction. The function acts as a support mechanism for the TOE's operating condition and internal data integrity. The function addresses the exception management.
		[200]	**SF.LIFE_CYCLE** contributes to FPT_PHP.1.1 satisfaction. The function acts as a support mechanism. The function addresses the TOE's life cycle state changes.
	PHP.1.2	[201]	**SF.TEST** grants the FPT_PHP.1.2 satisfaction. This function detects the TOE chip integrity violation. When an integrity error is detected an exception rises. The TOE aborts the current operation and may change the TOE life cycle state.
		[202]	**SF.INT_A** contributes to FPT_PHP.1.2 satisfaction. This function addresses the TOE data integrity.
		[203]	**SF.EXCEPTION** contributes to FPT_PHP.1.2 satisfaction. The function acts as a support mechanism for the TOE's operating condition and internal data integrity. The function addresses the exception management.
		[204]	**SF.LIFE_CYCLE** contributes to FPT_PHP.1.2 satisfaction. The function acts as a support mechanism. The function addresses the TOE's life cycle state changes.

	PHP.3.1	[205]	**SF.TEST** grants the FPT_PHP.3.1 satisfaction. This function detects the TOE environmental physical operating conditions. When a physical operating condition is detected out the range an exception rises. The TOE aborts the current operation and may change the TOE life cycle state.
		[206]	**SF.EXCEPTION** contributes to FPT_PHP.3.1 satisfaction. The function acts as a support mechanism for the TOE's operating condition and internal data integrity. The function addresses the exception management.
		[207]	**SF.LIFE_CYCLE** contributes to FPT_PHP.3.1 satisfaction. The function acts as a support mechanism. The function addresses the TOE's life cycle state changes.
	TST.1.1	[208]	**SF.TEST** grants the FPT_TST.1.1 satisfaction. This function executes a suite of tests to establish the correct functionality of the TOE. The tests are executed at TOE power-up or before/after sensitive operations.
	TST.1.2	[209]	**SF.INT_A** grants the FPT_TST.1.2 satisfaction. This function addresses the TOE integrity as well the TSF code and data integrity. When an integrity error is found the TOE notifies the condition externally. The authorized users are aware about the abnormal TOE condition.
	TST.1.3	[210]	**SF.INT_A** grants the FPT_TST.1.3 satisfaction. This function addresses the TOE integrity as well the TSF code and data integrity. When an integrity error is found the TOE notifies the condition externally. The authorized users are aware about the abnormal TOE condition.
FTP	ITC.1.1 SVD Transfer	[211]	**SF.AUTH** grants the FTP_ITC.1.1 SVD Transfer satisfaction. The function grants that the TOE establishes a trusted channel with a trusted IT product CGA. This function addresses the CGA authentication.
		[212]	**SF.SM** grants the FTP_ITC.1.1 SVD Transfer satisfaction. The function establishes a trusted channel with a remote IT product CGA. The function assures that the data exchanged on the trusted channel are protected against modifications or disclosure.
		[213]	**SF.MAC** contributes to FTP_ITC.1.1 SVD Transfer satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES or the Triple DES algorithm.
	ITC.1.2 SVD Transfer	[214]	**SF.AUTH** grants the FTP_ITC.1.2 SVD Transfer satisfaction. The function grants that the TOE establishes a trusted channel with a trusted IT product CGA. This function addresses the CGA authentication. After positive authentication the data communication can start via the trusted channel.
		[215]	**SF.SM** grants the FTP_ITC.1.2 SVD Transfer satisfaction. The function establishes a trusted channel with a remote IT product CGA. The function assures that the data exchanged on the trusted channel are protected against modifications or disclosure.
		[216]	**SF.MAC** contributes to FTP_ITC.1.2 SVD Transfer satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES or the Triple DES algorithm.

	ITC.1.3 SVD Transfer	[217]	**SF.AUTH** grants the FTP_ITC.1.3 SVD Transfer satisfaction. The function grants that the TOE establishes a trusted channel with a trusted IT product CGA. This function addresses the CGA authentication. After positive authentication the data communication can start via the trusted channel. The trusted channel can be used to export the SVD.
		[218]	**SF.SM** grants the FTP_ITC.1.3 SVD Transfer satisfaction. The function establishes a trusted channel with a remote IT product CGA. The function assures that the data exchanged on the trusted channel are protected against modifications or disclosure.
		[219]	**SF.MAC** contributes to FTP_ITC.1.3 SVD Transfer satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES or the Triple DES algorithm.
	ITC.1.1 DTBS Import	[220]	**SF.AUTH** grants the FTP_ITC.1.1 DTBS Import satisfaction. The function grants that the TOE establishes a trusted channel with a trusted IT product SCA. This function addresses the SCA authentication.
		[221]	**SF.SM** grants the FTP_ITC.1.1 DTBS Import satisfaction. The function establishes a trusted channel with a remote IT product SCA. The function assures that the data exchanged on the trusted channel are protected against modifications or disclosure.
		[222]	**SF.MAC** contributes to FTP_ITC.1.1 DTBS Import satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES or the Triple DES algorithm.
	ITC.1.2 DTBS Import	[223]	**SF.AUTH** grants the FTP_ITC.1.2 DTBS Import satisfaction. The function grants that the TOE establishes a trusted channel with a trusted IT product SCA. This function addresses the SCA authentication. After positive authentication the data communication can start via the trusted channel.
		[224]	**SF.SM** grants the FTP_ITC.1.2 DTBS Import satisfaction. The function establishes a trusted channel with a remote IT product SCA. The function assures that the data exchanged on the trusted channel are protected against modifications or disclosure.
		[225]	**SF.MAC** contributes to FTP_ITC.1.2 DTBS Import satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES or the Triple DES algorithm.
	ITC.1.3 DTBS Import	[226]	**SF.AUTH** grants the FTP_ITC.1.3 DTBS Import satisfaction. The function grants that the TOE establishes a trusted channel with a trusted IT product SCA. This function addresses the SCA authentication. After positive authentication the data communication can start via the trusted channel. The trusted channel can be used to import the DTBS.
		[227]	**SF.SM** grants the FTP_ITC.1.3 DTBS Import satisfaction. The function establishes a trusted channel with a remote IT product SCA. The function assures that the data exchanged on the trusted channel are protected against modifications or disclosure.
		[228]	**SF.MAC** contributes to FTP_ITC.1.3 DTBS Import satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES or the Triple DES algorithm.

	TRP.1.1 TOE	[229]	**SF.AUTH** grants the FTP_TRP.1.1 TOE satisfaction. The function grants that the TOE establishes a trusted path with a local user. This function addresses the user authentication.
		[230]	**SF.SM** grants the FTP_TRP.1.1 TOE satisfaction. The function establishes a trusted path with a local user. The function assures that the data exchanged on the trusted path are protected against modifications or disclosure.
		[231]	**SF.MAC** contributes to FTP_TRP.1.1 TOE satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES or the Triple DES algorithm.
	TRP.1.2 TOE	[232]	**SF.AUTH** grants the FTP_TRP.1.2 TOE satisfaction. The function grants that the TOE establishes a trusted path with a local user. This function addresses the user authentication. After positive authentication the data communication can start via the trusted path.
		[233]	**SF.SM** grants the FTP_TRP.1.2 TOE satisfaction. The function establishes a trusted path with a local user. The function assures that the data exchanged on the trusted path are protected against modifications or disclosure.
		[234]	**SF.MAC** contributes to FTP_TRP.1.2 TOE satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES or the Triple DES algorithm.
	TRP.1.3 TOE	[235]	**SF.AUTH** grants the FTP_TRP.1.3 TOE satisfaction. The function grants that the TOE establishes a trusted path with a local user. This function addresses the user authentication. After positive authentication the data communication can start via the trusted path. The trusted path can be used to exchange data related to the user authentication e.g. the user PIN.
		[236]	**SF.SM** grants the FTP_TRP.1.3 TOE satisfaction. The function establishes a trusted path with a local user. The function assures that the data exchanged on the trusted path are protected against modifications or disclosure.
		[237]	**SF.MAC** contributes to FTP_TRP.1.3 TOE satisfaction. The function acts as a support mechanism in the exchanged data integrity and authentication process. The function performs the DES or the Triple DES algorithm.

Table 6: Functional requirements and TOE security function rational

	TOE Security Functions	I & A		Key and Crypto				Stored Data Protection				TST, FAIL, LIFE CYCLE, AC, SM				
		SF.AUTH	SF.RAD	SF.KEY_GEN	SF.HASH	SF.MAC	SF.SIGN	SF.OBS_A	SF.INT_A	SF.DATA_ERASE	SF.TRANSACTION	SF.TEST	SF.EXCEPTION	SF.LIFE_CYCLE	SF.AC	SF.SM
FCS	CKM.1.1			√												
FCS	CKM.4.1								√							
FCS	COP.1.1 corresp			√												
FCS	COP.1.1 signing				√	√										
FDP	ACC.1.1 SVD Transfer SFP	√	√											√		
FDP	ACC.1.1 Initialization SFP	√	√											√		
FDP	ACC.1.1 Personalization SFP	√	√											√		
FDP	ACC.1.1 Sign. Creation SFP	√	√											√		
FDP	ACF.1.1 Initialization SFP													√		
FDP	ACF.1.2 Initialization SFP	√	√											√		
FDP	ACF.1.3 Initialization SFP	NONE														
FDP	ACF.1.4 Initialization SFP	√	√											√		
FDP	ACF.1.1 SVD Transfer SFP													√		
FDP	ACF.1.2 SVD Transfer SFP	√	√											√		
FDP	ACF.1.3 SVD Transfer SFP	NONE														
FDP	ACF.1.4 SVD Transfer SFP	NONE														
FDP	ACF.1.1 Personalization SFP													√		
FDP	ACF.1.2 Personalization SFP	√	√											√		
FDP	ACF.1.3 Personalization SFP	NONE														
FDP	ACF.1.4 Personalization SFP	NONE														
FDP	ACF.1.1 Sign. Creation SFP													√		
FDP	ACF.1.2 Sign. Creation SFP	√	√											√		
FDP	ACF.1.3 Sign. Creation SFP	NONE														
FDP	ACF.1.4 Sign. Creation SFP	√	√											√		
FDP	ETC.1.1 SVD Transfer	√														
FDP	ETC.1.2 SVD Transfer	√														
FDP	ITC.1.1. DTBS	√														
FDP	ITC.1.2. DTBS	√														
FDP	ITC.1.3. DTBS	√														
FDP	RIP.1.1								√							
FDP	SDI.2.1. Persistent							√				√	√			
FDP	SDI.2.2. Persistent							√				√	√			
FDP	SDI.2.1. DTBS					√									√	
FDP	SDI.2.2. DTBS					√									√	
FDP	UIT.1.1 SVD Transfer					√									√	
FDP	UIT.1.2 SVD Transfer					√									√	
FDP	UIT.1.1 TOE DTBS					√									√	
FDP	UIT.1.2 TOE DTBS					√									√	

Table 7: Functional requirements to TOE security function mapping

		I & A		KEY AND CRYPTO				STORED DATA PROTECTION				TST, FAIL, LIFE CYCLE, AC, SM				
		SF.AUTH	SF.RAD	SF.KEY_GEN	SF.HASH	SF.MAC	SF.SIGN	SF.OBS_A	SF.INT_A	SF.DATA_ERASE	SF.TRANSACTION	SF.TEST	SF.EXCEPTION	SF.LIFE_CYCLE	SF.AC	SF.SM
	AFL.1.1	√	√													
	AFL.1.2	√	√													
	ATD.1.1													√		
	UAU.1.1	√														
	UAU.1.2	√														
	UID.1.1	√														
	UID.1.2	√														
	MOF.1.1													√		
	MSA.1.1 Administrator													√		
	MSA.1.1 Signatory													√		
	MSA.2.1													√		
	MSA.3.1													√		
	MSA.3.2													√		
	MTD.1.1	√	√											√		
	SMF.1.1[6]	√												√		
	SMR.1.1													√		
	SMR.1.2													√		
	AMT.1.1										√					
	EMSEC.1.1						√									
	EMSEC.1.2						√									
	FLS.1.1									√	√	√	√			
	PHP.1.1							√			√	√	√			
	PHP.1.2							√			√	√	√			
	PHP.3.1										√	√	√			
	TST.1.1										√					
	TST.1.2							√								
	TST.1.3							√								
	ITC.1.1 SVD Transfer	√	√			√									√	
	ITC.1.2 SVD Transfer	√	√			√									√	
	ITC.1.3 SVD Transfer	√	√			√									√	
	ITC.1.1 DTBS Import	√	√			√									√	
	ITC.1.2 DTBS Import	√	√			√									√	
	ITC.1.3 DTBS Import	√	√			√									√	
	TRP.1.1 TOE	√	√			√									√	
	TRP.1.2 TOE	√	√			√									√	
	TRP.1.3 TOE	√	√			√									√	

Table 8: Functional requirements to TOE security function mapping (continued)

[6] This SFR has been added as suggested in the CC interpretation 065

8.4. TOE Strength of Function claim

FAMILY	SECURITY FUNCTION	SOF
Identification and Authentication	SF.AUTH	High
	SF.RAD	Not claim
Access Control	SF.AC	Not claim
Key Management and Cryptography	SF.KEY_GEN	Not claim
	SF.HASH	Not claim
	SF.MAC	Not claim
	SF.SIGN	Not claim
Secure Messaging	SF.SM	No claim
Stored Data Protection	SF.OBS_A	No claim
	SF.INT_A	No claim
	SF.DATA_ERASE	No claim
	SF.TRANSACTION	No claim
Test	SF.TEST	No claim
Failure	SF.EXCEPTION	No claim
TOE life cycle	SF.LIFE_CYCLE	No claim

Table 9: TOE SFR SOF claim

8.5. PP claims Rationale

[238] The chapter 5 lists all of the SFRs included in this security target; this list includes all of the SFRs identified in the [SSCD PP] [6]. All of the operations applied to the SFRs are in accordance with the requirements of the [SSCD PP] [6].

8.6. Assurance Measures assignment

In Table 10 is reported the assurance measures assignment. In the following discussion INCRYPTO34v2 is the TOE.

ASSURANCE REQUIREMENT		ASSURANCE MEASURES DOCUMENT DELIVERY REFERENCE
ASE		INCRYPTO34v2_ST
ADV	FSP	INCRYPTO34v2_FSP
	HLD	INCRYPTO34v2_HLD
	LLD	INCRYPTO34v2_LLD
	IMP	INCRYPTO34v2 Source Code
	SPM	INCRYPTO34v2_SPM
	RCR	INCRYPTO34v2_RCR
ACM	AUT	Configuration Management Plan Configuration Management User Guide INCRYPTO34v2 Configuration list INCRYPTO34v2 Reference
	CAP	
	SCP	
ADO	DEL	INCRYPTO34v2 Delivery Procedure
	IGS	INCRYPTO34v2 Installation Procedure
AGD	USR	INCRYPTO34v2 User Guide
	ADM	INCRYPTO34v2 Administrator Guide
ALC	DVS	Security Procedures: • Company Security scheme • Security in the development area • Access Control • Network security
	LCD	Life Cycle Model
	TAT	List Of Tools and Tool User guide
ATE	COV	INCRYPTO34v2 Test Coverage Analysis
	DPT	INCRYPTO34v2 Depth Test Analysis
	FUN	INCRYPTO34v2 Functional Test
	IND	INCRYPTO34v2 Samples
AVA	MSU	INCRYPTO34v2 Guidance Documentation Analysis
	SOF	INCRYPTO34v2 Security Function Strength Analysis
	VLA	INCRYPTO34v2 Vulnerability Analysis

Table 10: Assurance Measures assignment

8.7. Functional Requirements Dependencies

[239] This Security Target fully complies with [SSCD PP] [6] § 6.4. To reflect the additional TOE security functional requirement **FMT_SMF.1** the following additional dependencies, as declared in CC interpretation 065, are defined and completely fulfilled:

FMT_MOF.1: FMT_SMF.1 Specification of Management Functions

FMT_MSA.1: FMT_SMF.1 Specification of Management Functions

FMT_MTD.1: FMT_SMF.1 Specification of Management Functions

9 References

[1] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures.

[2] International Organization for Standardization, *ISO/IEC 15408-1:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*, 1999.

[3] International Organization for Standardization, *ISO/IEC 15408-2:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*, 1999.

[4] International Organization for Standardization, *ISO/IEC 15408-3:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*, 1999.

[5] Algorithms and parameters for algorithms, list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the 'Electronic Signature Committee' in the Directive.

[6] CWA 14169 - Annex C Protection Profile-Secure Signature - Creation Device Type 3, version: 1.05, EAL4+, March 2002 (BSI-PP-0006-2002 EAL 4+).

[7] Protection Profile PP9806 -Smartcard - Integrated Circuit, version: 2.0, EAL4+, September 1998.

[8] CWA 14355- Guidelines for the implementation of Secure Signature - Creation Devices version 0.91, Dec 17, 2001.

[9] ST, ST19XL34v2 Security Target Lite, FNT_GRENAT_ST_02_002_V01.20.

[10] DCSSI, Rapport de Certification 2002/20. Plate-forme ST19X: Microcircuit ST19XL34. Août 2002.

[11] ISO/IEC 7816

Part 3	Signal and transmission protocols Second Edition 1997
Part 4	Interindustry commands for interchange Edition 1995
Part 5	Numbering System and registration procedure for application identifiers First Edition 1994
Part 8	Security related interindustry commands Edition 1998
Part 9	Additional interindustry commands and security attributes First Edition 2001

[12] FIPS 113: Computer Data Authentication (FIPS PUB 113), NIST, 30. May 1985.

[13] FIPS 140-2: Security Requirements for Cryptographic Modules (FIPS PUB 140-2), NIST, 1999.

[14] FIPS 180-1: Secure Hash Standard (FIPS PUB 180-1), NIST, 17. April 1995.

10 Glossary

This section gives definitions and explanations related to frequently used terms and acronyms.

TERM	DEFINITION
Administrator	Means an user that performs TOE initialization, TOE personalization, or other TOE administrative functions
Advanced electronic signature	(Defined in the Directive [1], article 2.2) means an electronic signature which meets the following requirements: a) it is uniquely linked to the signatory; b) it is capable of identifying the signatory; c) it is created using means that the signatory can maintain under his sole control, and d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
Authentication data	The information used to verify the claimed identity of a user.
Authorized user	A user who may, in accordance with the TSP, perform an operation.
Card manufacturer	INCARD Spa.
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)
Certificate 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)	An entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.
Chip Manufacturer	ST Microelectronics Spa.
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 (DTBSR)	Means the data sent by the SCA to the TOE for signing and is a) a hash-value of the DTBS or b) an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS or c) 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.
Directive	The Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1] is also referred to as the 'Directive' in the remainder of the Security Target.
Local User	User using the trusted path provided between the SCA in the TOE environment and the TOE.
PERSO_MODE flag	Flag used to control TOE state transition. Default configuration value for PERSO_MODE flag is set equal to PERSONALIZATION in order to force the TOE in *SC personalization* state at the beginning of TOE Operational phase.

TERM (CONT.)	DEFINITION
Personal Identification Number (PIN)	Value transmitted from the smartcard reader to INCRYPTO34v2 and used for signatory's authentication.
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 (defined in the Directive, article 2.10), here reported: Qualified certificates must contain: (a) an indication that the certificate is issued as a qualified certificate; (b) the identification of the certification-service-provider and the State in which it is established; (c) the name of the signatory or a pseudonym, which shall be identified as such; (d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended; (e) signature-verification data which correspond to signature-creation data under the control of the signatory; (f) an indication of the beginning and end of the period of validity of the certificate; (g) the identity code of the certificate; (h) the advanced electronic signature of the certification-service-provider issuing it; (i) limitations on the scope of use of the certificate, if applicable; and (j) limits on the value of transactions for which the certificate can be used, if applicable.
Reference Authentication Data (RAD)	Means data persistently stored by the TOE for verification of the authentication attempt as authorized user.
Secure Signature Creation Device (SSCD or the TOE described in this Security Target)	Means configured software or hardware which is used to implement the SCD and which meets the requirements laid down in Annex INCRYPTO34v2 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 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 a) to perform the presentation of the DTBS to the signatory prior to the signature process according to the signatory's decision, b) to send a DTBS-representation to the TOE, if the signatory indicates by specific unambiguous input or action the intend to sign, c) 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 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.
SSCD PP	Secure Signature Creation Device Protection Profile [6]
ST ROM	ST Microelectronics ROM code running in ISSUER MODE, i.e. when the smartcard is delivered to the card manufacturer
Verification Authentication Data (VAD)	Means authentication data provided as input by knowledge. For INCRYPTO34v2 this is synonym of PIN.

ACRONYMS	DEFINITION
AC	Access Conditions
BSO	Base Security Object
CC	Common Criteria
CGA	Certificate Generation Application
CSP	Certification Service Provider
DF	Directory file
DTBS	Data to be signed
DTBSR	Data to be signed representation
EAL	Evaluation Assurance Level
IC	Integrated Circuit
IFD	Interface Device, i.e. the smartcard reader
IT	Information Technology
MAC	Message Authentication Code
MAP	Modular Arithmetic Processor
MUT_{KEY}	Cryptographic key used for mutual authentication between the TOE and an external application/device
OS	Operating System
PP9806	Protection Profile [7]
RAD	Reference Authentication Data
RAD_A	Reference Authentication Data stored by the TOE and used to verify the claimed identity of the administrator
RAD_S	Reference Authentication Data stored by the TOE and used to verify the claimed identity of the signatory
SC	Smartcard
SCA	Signature Creation Application
SCD	Signature Creation Data
SDO	Signed Data Object
SF	Security Function
SFP	Security Function Policy
SM	Secure Messaging
SOF	Strength of Function
SSCD (the TOE)	Secure Signature Creation Device
SSCD PP	Protection Profile [6]
ST	Security Target
STM	STMicroelectronics
SVD	Signature Verification Data
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
VAD	Verification Authentication Data

Confidentiality Obligations:

THIS DOCUMENT CONTAINS CONFIDENTIAL INFORMATION.
ITS DISTRIBUTION IS SUBJECT TO THE SIGNATURE OF AN NON-DISCLOSURE AGREEMENT (NDA).
IT IS CLASSIFIED "RESTRICTED DISTRIBUTION"

AT ALL TIMES YOU SHOULD COMPLY WITH THE FOLLOWING SECURITY RULES
(REFER TO NDA AND FOR DETAILED OBLIGATIONS):

DO NOT COPY OR REPRODUCE ALL OR PART OF THIS DOCUMENT
KEEP THIS DOCUMENT LOCKED AWAY

FURTHER COPIES CAN BE PROVIDED ON A "NEED TO KNOW BASIS", PLEASE CONTACT
YOUR LOCAL ST SALES OFFICE OR THE FOLLOWING ADDRESS:

STMicroelectronics SA
SMART CARDS PRODUCTS MARKETING DPT
BP2 / ZI de Peynier Rousset / F-13106 ROUSSET Cedex / FRANCE
Fax: +33 4 42 25 87 29

ST Incard s.r.l.
Z.I. Marcianise Sud
81025 Marcianise (CE) / Italia
Fax: + 39 0823 630 247