ExaCard smart card v 1.0
Security Target

General information

Document control

Project:	ExaCard smart card v 1.0 Common Criteria EAL 4+ certification
Destination entity:	Applus+
Title:	ExaCard smart card v 1.0 Security Target
Reference code:	ExaCard smart card v 1.0 Security Target
Version:	01/01/09
Date:	Wednesday 18 June 2014
File:	exacard_smart_card_v_1_0_security_target.odt
Edition tool:	OpenOffice.org Writer v 3.2.0
Author:	Idoneum Electronic Identity team

Formal state

Prepared by:	Revised by:	Approved by:
Name: Josep Monés Diego Delgado Manel Sardà Francisco Gómez	**Name:** Josep Monés	**Name:** Josep Monés
Date: 15st June 2010	**Date:** 15st June 2010	**Date:** 15st June 2010

Version control

Version	Changed sections	Changes description	Date
1.00	All	All	15th Jun 2010
1.01	2.1 2.2, 5.1.5 6	Added level of conformance in 2.1 Added section 2.2.1 and removed the FPT_AMT.1 SFR Added the Rationale (new section 6)	29th Jul 2010
1.02	5.1.5.2 7.2.1 7.4.5	Added “chip surface attacks” to FPT_FLS.1.1 Merged FDP_ACC.1 and FDP_ACF.1 Added RESET RETRY COUNTER command to FMT_MTD.1.1	23th Sep 2010

Version	Changed sections	Changes description	Date
1.03	2.1 5 6.2.4.2 1.3	Modified conformance to CC part 2 Added Extended Components Definition chapter Added Extended components definition elements Added identification of the TOE guidance document	21th Mai 2013
1.04	6.1.4.3	Fixed SFR FMT_MSA.2 to CC V3.1r3	28th Jun 2012
1.05	1.3	Added reference to different documents.	04th Jun 2014

Table of contents

1 Introduction

1.1 ST reference

ExaCard smart card v 1.0 ST, version 1.05, Idoneum Electronic Identity, 04 June 2014.

1.2 TOE reference

Idoneum Electronic Identity ExaCard smart card v 1.0.

1.3 TOE overview

ExaCard smart card v 1.0 is a secure signature-creation device intended to be used in a Public Key Infrastructure (PKI) system. Its main feature it's the combination of RSA and ECC algorithms for a greater resistance to breakage of some of these signature algorithms.

It addition to signature generation, it allows RSA key generation and export of 2048, 3072 and 4096 bits, ECC key generation of 192, 224, 256, 384 and 521 bits, TDES symmetric key generation, encipher/decipher operations either symmetric or asymmetric, generation of SHA-1, SHA-224 and SHA-256 message digests, generation of pseudo random numbers with the ANSI X9.17 Random Number Generator and it implements the main functionality of the ISO/IEC 7816-3/4/8/9 [7] [8] [9] [10] and CWA 14890-1 [12] specifications.

All the above operations are managed by a complete smart card operating system highly configurable and with protection against accidental data corruption. This feature is provided by the file system which implements a powerful transaction system.

Its support for several logical channels allows for a secure multi-application environment while protecting the privacy of each application user's data.

The whole system supports various SPA, DPA, timing analysis and DFA countermeasures and detection and resistance to several physical attacks.

Exacard v1.0 requires a compliant ISO/IEC 7816-3 [7] smart card reader and a computer with either Windows XP, Windows Vista, Windows 7, Linux or Mac OS X operating systems.

With the TOE is included the guidance document “Exacard smart card v 1.0: AGD_OPE, guía de recomendaciones para el usuario”, version 1.03.

Also, with the TOE is included the document “ExaCard smart card v 1.0 profile”, version 1.00, and the document “Especificación Funcional ExaCard OS v1.03, 29 October 2013”.

1.4 TOE description

The TOE is a secure signature-creation device (SSCD type 3) as defined in the CWA 14169:2004 CEN standard [11]. The CWA 14169:2004 defines security requirements for Secure Signature-Creation Devices (SSCD) according to european directive 1999/93/EC on a Community framework for electronic signatures.

It's main purpose is to be used as secure signature creation device in a PKI system, providing signature operation, key generation, key export, and confidentiality, integrity and protection of user's data.

The TOE is a composite TOE, and it consists of a complete smart card operating system designed

by Idoneum Electronic Identity S.A. built on the certified NXP P5CC081 secure contact PKI smart card controller [5]. The cryptographic operations relies upon the certified “Secured Crypto Library on the P5CD016/021/041/081 and P5CC081” cryptographic subroutine library by NXP Semiconductors [6], in the following NXP Crypto Library.

1.4.1 TOE physical scope

The figure 1 shows the different components of the TOE and its relationships. A more emphasis is given to the operating system.

The TOE communicates via trusted channel with the external applications:

- Certification-generation Application (CGA)
- Signature-creation Application (SCA)

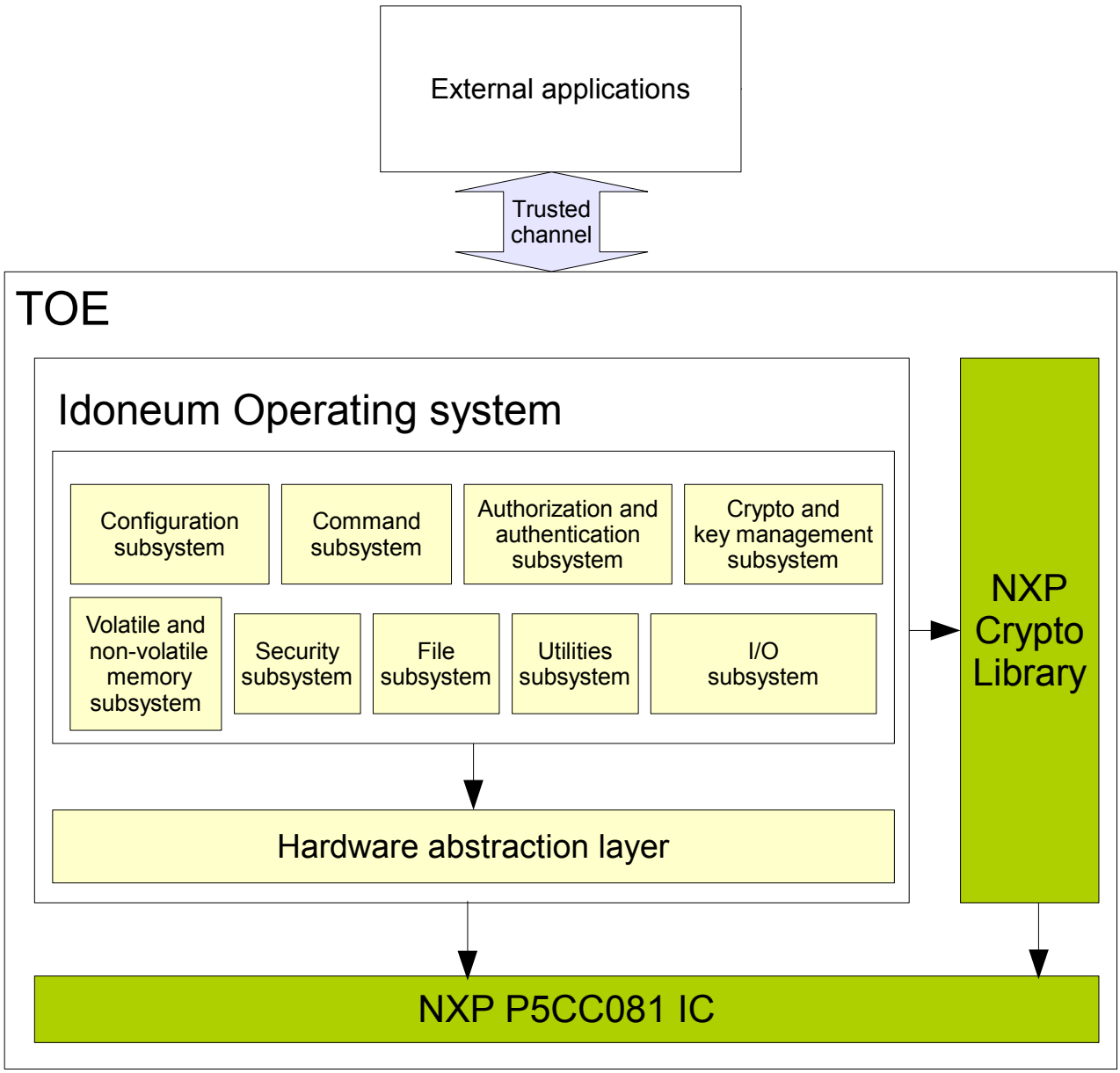

Figure 1: TOE physical description

The main OS subsystems are depicted in the above figure. All of them are interrelated to a greater or lesser degree.

- The configuration subsystem manages the customizable parameters of the operating system and its external functionality.
- The command subsystem is the functional high level for the signature creation, key generation and other smart card user operations.
- The authorization and authentication subsystem controls the access to the resources based on an Access Control List (ACL) system. An ACL is basically a list of permissions attached to a resource. Each entry of the ACL indicates an access mode to the resource and the conditions to be met in order to allow that access. Also it performs the device authentication protocol operations which allows the communication with authorised applications only.
- The crypto and key management subsystem contains the functions that implements the cryptographic operations needed mainly for the signature-creation operation.
- The volatile and non-volatile memory subsystem manages the volatile (RAM) and non-volatile (EEPROM) memory from a low level.
- The security subsystem ensures that the execution flow and the function calls inside the operating system run as expected. Also it manages the unexpected errors from some critical operations and performs the necessary actions.
- The file subsystem manages all the user's data in a secure way, relying on the authorization and authentication subsystem and the crypto and key management subsystem.
- The utilities subsystem offers functionality to be used by the other subsystems. There are functionality for: BER-TLV or simple-TLV structures, CRC, big numbers and memory.
- The I/O subsystem is the responsible of the external communication via the ISO/IEC 7816-3 T=0 protocol.

In a lower level is located the hardware abstraction layer (HAL) which is made up of functions that access the hardware directly, creating an interface for the upper subsystems. The HAL controls the following components of the P5CC081: UART, timers, interruptions, EEPROM, FameXE, Random Number Generator, CPU & coprocessors clock and security hardware.

1.4.2 TOE logical scope

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

(1) to generate the SCD and the correspondent signature-verification data (SVD) and

(2) to create qualified electronic signatures

  (a) after allowing for the data to be signed (DTBS) to be displayed correctly where the display function may either be provided by the TOE itself or by appropriate environment

  (b) using appropriate hash functions that are agreed as suitable for qualified electronic signatures

(c) after appropriate authentication of the signatory by the TOE.

(d) using appropriate cryptographic signature function that employ appropriate cryptographic parameters agreed as suitable.

The TOE implements all IT security functionality which are necessary to ensure the secrecy of the SCD. To prevent the unauthorised usage of the SCD the TOE provides user authentication and access control.

This ST assumes that the Signature Creation Application (SCA) is part of the environment of the TOE.

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

1. Generating a SCD/SVD pair
2. Personalisation for the signatory by means of the signatory's verification authentication data (SVAD).

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

The TOE allows user authentication by means of a trusted human interface (HI) device connected via a trusted channel with the TOE. The HI device is used for the input of verification authentication data (VAD) for authentication by knowledge. The TOE holds reference authentication data (RAD) to check the provided VAD.

The TOE life cycle is shown in Figure 2. Basically, it consists of a development phase and the operational phase. In the initialisation phase the basic structures of the system are built. The operational phase starts with personalisation, including loading of the structures generated during initialisation and generation of the first key pair SCD/SVD. The main functionality in the usage phase is signature-creation including all supporting functionality (e.g., SCD storage and SCD use). The life cycle ends with the destruction of the SSCD.

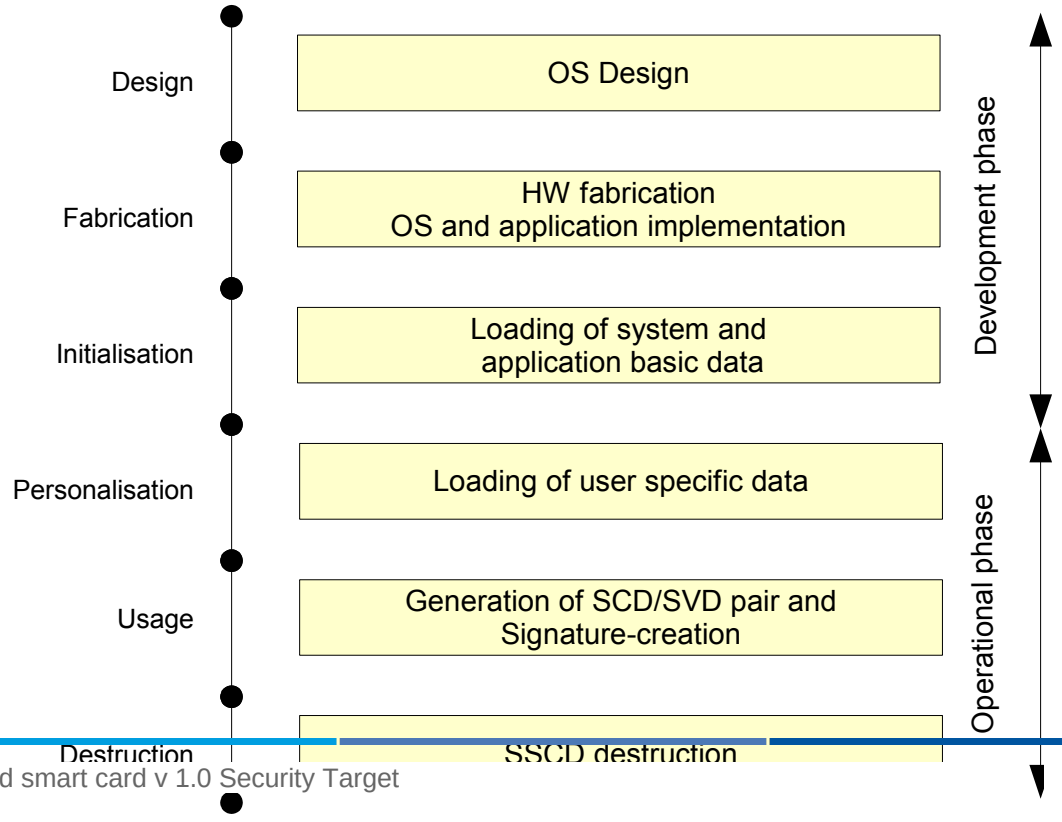

Figure 2: SSCD Life cycle

1.4.3 P5CC081 contact PKI smart card controller features

1.4.3.1 Main features

- EEPROM: 80 KB
  - Data retention time: 25 years minimum
  - Endurance: 500.000 cycles minimum
- ROM 264 KB
- RAM: 7,50 KB
  - 0,25 KB IRAM + 4,75 KB Standard RAM usable for CPU
  - 2,50 KB FXRAM shared with FameXE
- Dedicated, Accelerated Secure_MX51 Smart Card CPU (Memory eXtended/enhanced 80C51)
  - 5-metal layer 0.14 µm CMOS technology
  - Operating in Contact mode
  - Featuring a 24-bit universal memory space, 24-bit program counter
  - Combined universal program/data linear address range up to 16 MB
- ISO/IEC 7816 contact interface
- PKI coprocessor FameXE (Fast Accelerator for Modular Exponentiation -eXtended)
- Support of major Public Key Cryptography (PKC) systems like RSA, Elgamel, DSS, Diffie-Hellman, Guillou-Quisquater, Fiat-Shamir and Elliptic Curves
- High speed Triple-DES coprocessor (64-bit parallel processing DES engine)
- High speed AES coprocessor (128-bit parallel processing AES engine)
- Low power/low voltage design using NXP Semiconductors handshaking technology
- Multiple source vectorized interrupt system with four priority levels
- Two 16-bit timers
- High reliable EEPROM for both data storage and program execution
- Typical EEPROM page erasing time: 1.7 ms
- Typical EEPROM page programming time: 1.0 ms
- Contact configuration and serial interface according to ISO/IEC 7816
- ISO/IEC 7816 UART supporting standard protocols T=0 and T=1 as well as high speed personalization up to 1 Mbit/s
- High speed 16-bit CRC engine according to ITU-T polynomial definition

- Low power Random Number Generator (RNG) in hardware, AIS-31 compliant
- 1.62 V to 5.5 V extended operating voltage range for class C, B and A (for higher security ExaCard only supports class B and A)
- -25 ºC to +85 ºC ambient temperature

1.4.3.2 Security features

- Enhanced security sensors
  - Low / high clock frequency sensor
  - Low / high temperature sensor
  - Low / high supply voltage sensor
  - Single Fault Injection (SFI) attack detection
  - Light sensors (included Integrated memory light sensor functionality)
- Electronic fuses for safeguarded mode control
- Active Shielding
- Clock input filter for protection against spikes
- Power-up / Power-down reset
- Memory security (encryption and physical measures) for RAM, EEPROM and ROM
- Optional disabling of ROM read instructions by code executed in EEPROM
- EEPROM programming:
  - No external clock
  - Hardware sequencer controlled
  - On-chip high voltage generation
  - Enhanced error correction mechanism

1.4.4 NXP Secured Crypto Library features

- Various algorithms
  - Pseudo random number generator (PRNG) seeded by the hardware random number generator with a test to ensure the quality of the hardware random number generator
  - AES encryption and decryption using the AES coprocessor.
  - DES and Triple-DES encryption and decryption using the DES coprocessor.
  - RSA encryption and decryption, signature generation and verification for straightforward and CRT keys up to 5024 bits
  - RSA key generation
  - ECC over GF(p) signature generation and verification (ECDSA) and Diffie-Hellman key exchange for keys up to 544 bits
  - ECC over GF(p) key generation

  - SHA-1, SHA-224 and SHA-256 hash
  - Secured memory copy
- Secure operation in contact as well as in the contactless mode
- Internal security measures for residual information protection
- Latest built-in security features to avoid power (SPA/DPA), timing and fault attacks (DFA)

1.4.5 Operating system features

1.4.5.1 File system

Manages storage, reading, writing and destruction of the persistent user data:

- Distribution of the user data using files and directories in a tree hierarchy.
- ISO/IEC 7816-4 [8] file structures supported
  - Transparent structure
  - Linear structure with records of fixed size
  - Linear structure with records of variable size
  - Cyclic structure with records of fixed size
  - TLV structure
- Highly configurable. During the pre-personalisation phase it's possible to define parameters which configure some properties of the file system, e.g. Adapt the system to the EEPROM available.
- High failure tolerance. The transactional subsystem provides a great stability against power supply failures and/or attacks.
- Monitoring of data integrity.
- Mechanisms to ensure the confidentiality of the sensible data.
- The access permissions to each resource are managed by the authorization and authentication subsystem.

1.4.5.2 Commands supported

- ISO/IEC 7816-4 [8] interindustry commands for:
  - Selection
  - Data unit handling
  - Record handling
  - Data object handling
  - Basic security handling
  - Transmission handling
- ISO/IEC 7816-8 [9] interindustry commands for cryptographic operations
- ISO/IEC 7816-9 [10] interindustry commands for card management

- Proprietary commands for:
  - Extra key management operations
  - Symmetric keys management
  - Extra card management operations

2 Conformance claims

2.1 CC Conformance Claim

This Security Target claims to be conformant to version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- “Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 3, July 2009, CCMB-2009-07-002” **extended** due to the use of the component FPT_EMSEC.1
- “Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 3, July 2009, CCMB-2009-07-003” **conformant** as only assurance components as defined in [4] have been used.

2.2 PP Claim

This Security Target claims strict conformance to the Protection Profile (PP) “Protection Profile – Secure Signature-Creation Device Type 3, Version 1.05, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference EAL4+ BSI-PP-0006-2002”, from now on referred as PP.

Since the Security Target claims conformance to this PP, the concepts are used in the same sense. For the definition of terms please refer to the PP. These terms also apply to this Security Target.

2.2.1 Discrepancy with the CC version of the PP

The EAL4 security assurance requirements (SARs) expressed in the PP are from CC version 2.3. Instead, as this ST is conformant to CC version 3.1, the EAL4 SARs are taken from this version.

Moreover, the PP's EAL4 augmentations, the Security assurance requirements AVA_MSU.3 and AVA_VLA.4, exists only in CC version 2.3. According to *ExaCard smart card v 1.0 Conformance Declaration* document those SARs have been mapped to another requirements. MSU is moved into AGD families and some aspects remains in VAN. And VLA is moved to VAN family, vulnerability analysis.

Again, the FPT_AMT.1 security functional requirement (SFR) component expressed in the PP is part of the CC v2.3. In the CC v3.1 it's covered by the SAR ADV_ARC.1.

2.3 Package Claim

This Security Target claims conformance to the assurance package EAL4 augmented. The

augmentation is:

- Vulnerability assessment: AVA_VAN.5 (Advanced methodical vulnerability analysis)

2.4 Conformance Claim Rationale

The TOE is a smart card to be used as secure signature-creation device (SSCD) of type 3 which combines the major tasks of a SSCD (i.e., signature-creation and SCD/SVD generation).

It follows the CWA 14169:2004, Secure signature-creation devices “EAL4+” specification [11].

This is justified by the need to obtain an standardized product, highly resistant to different attacks and free of vulnerabilities.

Conformance to the PP, as claimed in section 2.2, is required by CWA 14169:2004.

All the security problem definition, objectives and security requirements are taken from the PP. The operations (e.g., selection, assignment) done for the SFRs are clearly indicated.

3 Security problem definition

Assets:

1. SCD: private key used to perform an electronic signature operation(confidentiality of the SCD must be maintained).
2. SVD: public key linked to the SCD and used to perform an electronic signature verification(integrity of the SVD when it is exported must be maintained).
3. DTBS and DTBS-representation: set of data, or its representation which is intended to be signed (Their integrity must be maintained).
4. VAD: PIN code or biometrics data entered by the End User to perform a signature operation (confidentiality and authenticity of the VAD as needed by the authentication method employed)
5. RAD: Reference PIN code or biometrics authentication reference used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained)
6. 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)
7. Electronic signature: (Unforgeabilty of electronic signatures must be assured).

Subjects:

1. S.User: End user of the TOE which can be identified as S.Admin or S.Signatory
2. S.Admin: User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions.
3. 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.

Threat agents:

1. 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 attack potential** and **knows no secret**.

3.1 Assumptions

A.CGA Trustworthy certification-generation application

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

A.SCA Trustworthy signature-creation application

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

3.2 Threats to Security

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

T.Sig_Forgery Forgery of the electronic signature

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

T.Sig_Repud Repudiation of signatures

If an attacker can successfully threaten any of the assets, then the non-repudiation of the electronic signature is compromised. This results 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.

3.3 Organisational Security Policies

P.CSP_QCert Qualified certificate

The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Annex I of the Directive, i.e., inter alia the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE is evident with signatures through the certificate or other publicly available information.

P.QSign Qualified electronic signatures

The signatory uses a signature-creation system to sign data with qualified electronic signatures. The DTBS are presented to the signatory by the SCA. The qualified electronic signature is based on a qualified certificate (according to directive Annex 1) and is created by a SSCD.

P.Sigy_SSCD TOE as secure signature-creation device

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

4 Security Objectives

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

4.1 Security Objectives for the TOE

OT.EMSEC_Design Provide physical emanations security

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

OT.Lifecycle_Security Lifecycle security

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

OT.SCD_Secrecy Secrecy of the signature-creation data

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

OT.SCD_SVD_Corresp Correspondence between SVD and SCD

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

OT.SVD_Auth_TOE TOE ensures authenticity of the SVD

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

OT.Tamper_ID Tamper detection

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

OT.Tamper_Resistance Tamper resistance

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

OT.Init SCD/SVD generation

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

OT.SCD_Unique Uniqueness of the signature-creation data

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

OT.DTBS_Integrity_TOE Verification of the DTBS-representation integrity

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

OT.Sigy_SigF Signature generation function for the legitimate signatory only

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

OT.Sig_Secure Cryptographic security of the electronic signature

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

4.2 Security Objectives for the Environment

OE.CGA_QCert Generation of qualified certificates

The CGA generates qualified certificates which include inter alia

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

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

(c) the advanced signature of the CSP.

OE.SVD_Auth_CGA CGA verifies the authenticity of the SVD

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

OE.HI_VAD Protection of the VAD

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

OE.SCA_Data_Intend Data intended to be signed

The SCA

(a) generates the DTBS-representation of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE,

(b) sends the DTBS-representation to the TOE and enables verification of the integrity of the DTBS-representation by the TOE

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

5 Extended components definition

5.1 Definition for FPT_EMSEC.1

The FPT_EMSEC.1 TOE Emanation component is defined in CWA 14169:2004 [11].

6 Security Requirements

This chapter gives the security functional requirements and the security assurance requirements for the TOE and the environment.

Security functional requirements components given in section 5.1 “TOE security functional requirements” excepting FPT_EMSEC.1 which is explicitly stated, are drawn from Common Criteria part 2 [3]. Some security functional requirements represent extensions to [3]. Operations for assignment, selection and refinement have been made.

The TOE security assurance requirements statement given in section 5.2 “TOE Security Assurance Requirement” is drawn from the security assurance components from Common Criteria part 3 [4].

Section 5.3 identifies the IT security requirements that are to be met by the IT environment of the TOE.

The non-IT environment is described in section 5.4.

6.1 Functional Requirements

For the operations applied to these CC functional components, the following notation and conventions apply:

- The iteration operation is indicated by the slash ('/') symbol and is applied always to the last level of abstraction possible, either to an element or to an element's iteration. In both cases the iteration is applied to all elements belonging to a component.
- The assignment and the selection operations applied by the PP author are highlighted with underline.
- The assignment and the selection operations applied by the ST author are highlighted with **bold** and square brackets ('[]') to delimit it.
- A text highlighted with **underline and bold** means that the PP author made a selection or assignment which the ST author specified according to his own implementation.
- The refinement operation is indicated explicitly when it appears.

6.1.1 Cryptographic support (FCS)

6.1.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1/RSA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA (straight forward) and RSA-CRT**] and specified cryptographic key sizes [**2048, 3072, 4096 bits**] that meet the following: **"Regulierungsbehörde für Telekommunikation und Post: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), German "Bundesanzeiger Nr. 59", p.4695-4696, March 30th, 2005".**

FCS_CKM.1.1/ECC	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**ECC over GF(p)**] and specified cryptographic key sizes [**192, 224, 256, 384, 521 bits**] that meet the following: **ISO 15946-1-2008 and "Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht übergeeignete Algorithmen".**

6.1.1.2 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 [**memory erase of encrypted key**] that meets the following: [**EEPROM erase according to NXP Semiconductors Data Sheet P5CD016/021/041 and P5Cx081 family *Secure dual interface and contact PKI smart card controller,* Revision 3.1, sec 10.9 EEPROM**].

Application notes:

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

6.1.1.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ CORRESP/RSA	The TSF shall perform SCD / SVD correspondence verification in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**2048,3072,4096 bits**] that meet the following: **PKCS#1 v2.1**.
FCS_COP.1.1/ CORRESP/ECC	The TSF shall perform SCD / SVD correspondence verification in accordance with a specified cryptographic algorithm [**ECC**] and cryptographic key sizes [**192, 224, 256, 384, 521 bits**] that meet the following: **ANSI X9.62, ISO/IEC 15946 Part1.**
FCS_COP.1.1/ SIGNING/RSA	The TSF shall perform digital signature-generation in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**2048,3072,4096 bits**] that meet the following: **PKCS#1 v2.1**.
FCS_COP.1.1/ SIGNING/ECC	The TSF shall perform digital signature-generation in accordance with a specified cryptographic algorithm [**ECC**] and cryptographic key sizes [**192, 224, 256, 384, 521 bits**]

that meet the following: **ISO 14888-3.**

6.1.2 User data protection (FDP)

6.1.2.1 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/ Initialisation SFP	The TSF shall enforce the Initialisation SFP on generation of SCD/SVD pair by User.
FDP_ACC.1.1/ Personalisation SFP	The TSF shall enforce the Personalisation 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.

6.1.2.2 Security attribute based access control (FDP_ACF.1)

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

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

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 “ authorised” is allowed to generate SCD/SVD pair.
FDP_ACF.1.3/ Initialisation SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ Initialisation SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: The user with the security attribute “role” set to “Administrator” or set to “Signatory” and with the security attribute “SCD / SVD management” set to “not authorised” is not allowed to generate SCD/SVD pair.

SVD Transfer

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 authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ SVD Transfer SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: none.

Personalisation SFP

FDP_ACF.1.1/ Personalisation SFP	The TSF shall enforce the Personalisation SFP to objects based on General attribute.
FDP_ACF.1.2/ Personalisation SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: User with the security attribute “role” set to “Administrator” is allowed

	to create the RAD.
FDP_ACF.1.3/ Personalisation SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ Personalisation SFP	The TSF shall explicitly deny access of subjects to objects based on the 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 authorised SCA with SCD by the Signatory which security attribute “SCD operational” is set to “yes”.
FDP_ACF.1.3/ Signature-creation SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ Signature-creation SFP	The TSF shall explicitly deny access of subjects to objects based on the 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 authorised SCA with SCD by the Signatory which security attribute “SCD operational” is set to “yes”. (b) User with the security attribute “role” set to “Signatory” is not allowed to create electronic signatures for DTBS sent by an authorised SCA with SCD by the Signatory which security attribute “SCD operational” is set to “no”.

6.1.2.3 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.

6.1.2.4 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 authorised SCA.

Application note:

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

6.1.2.5 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.

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

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

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

FDP_SDI.2.1/ 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.

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

stored data":

FDP_SDI.2.1/DTBS	The TSF shall monitor user data stored within the TSC for integrity 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.

6.1.2.7 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.

6.1.3 Identification and authentication (FIA)

6.1.3.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1	The TSF shall detect when [**three**] 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.

6.1.3.2 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.

6.1.3.3 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 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.

Application note:

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

6.1.3.4 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.

6.1.4 Security management (FMT)

6.1.4.1 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.

6.1.4.2 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1/ Administrator	The TSF shall enforce the Initialisation SFP to restrict the ability to modify [**none**] 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.

6.1.4.3 Secure security attributes (FMT_MSA.2)

FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for [**security attributes defined in FDP_ACF.1**]

6.1.4.4 Static attribute initialisation (FMT_MSA.3)

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

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.

6.1.4.5 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1	The TSF shall restrict the ability to modify [**none**] the RAD to Signatory.

6.1.4.6 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.

6.1.5 Protection of the TSF (FPT)

6.1.5.1 TOE Emanation (FPT_EMSEC.1)

FPT_EMSEC.1.1	The TOE shall not emit [**information extractable from electromagnetic radiation, power consumption and execution times of commands**] in excess of [**unintelligible limits**] enabling access to RAD and SCD.
FPT_EMSEC.1.2	The TSF shall ensure [**S.OFFCARD**] are unable to use the following

interface [**VCC, GND, I/O, CLK**] to gain access to RAD and SCD.

Application note:

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

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

6.1.5.2 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: [**communication protocol disturbance, electrical signal alterations, chip surface attacks**].

6.1.5.3 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.

6.1.5.4 Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1	The TSF shall resist [**physical manipulation and physical testing**] to the **[TSF]** by responding automatically such that the TSP is not violated.

6.1.5.5 TSF testing (FPT_TST.1)

FPT_TST.1.1	The TSF shall run a suite of self tests [**during initial start-up**][**while sending ATR**] to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

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

6.1.6 Trusted path/channels (FTP)

6.1.6.1 Inter-TSF trusted channel (FTP_ITC.1)

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

6.1.6.2 Trusted path (FTP_TRP.1)

The trusted path between the TOE and the SCA will be required only if the human interface for user authentication is not provided by the TOE itself but by the SCA.

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 [**the TSF, 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**][**none**].

6.2 Security Assurance Requirements

Table 5.1 Assurance Requirements: EAL(4) augmented by AVA_VAN.5

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

6.2.1 Development (ADV)

6.2.1.1 Security architecture description (ADV_ARC.1)

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

6.2.1.2 Complete functional specification (ADV_FSP.4)

ADV_FSP.4.1D The developer shall provide a functional specification.

ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.4.1C The functional specification shall completely represent the TSF.

ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.4.4C The functional specification shall describe all actions associated with each TSFI.

ADV_FSP.4.5C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

6.2.1.3 Implementation representation of the TSF (ADV_IMP.1)

ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.

ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.

ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

6.2.1.4 Basic modular design (ADV_TDS.3)

ADV_TDS.3.1D The developer shall provide the design of the TOE.

ADV_TDS.3.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.3.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.3.2C The design shall describe the TSF in terms of modules.

ADV_TDS.3.3C The design shall identify all subsystems of the TSF.

ADV_TDS.3.4C The design shall provide a description of each subsystem of the TSF.

ADV_TDS.3.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.3.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

ADV_TDS.3.7C The design shall describe each SFR-enforcing module in terms of its purpose and relationship with other modules.

ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing modules.

ADV_TDS.3.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.

ADV_TDS.3.10C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

6.2.2 Guidance documents (AGD)

6.2.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available

functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

6.2.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

6.2.3 Life-cycle support (ALC)

6.2.3.1 Production support, acceptance procedures and automation (ALC_CMC.4)

ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.4.2D The developer shall provide the CM documentation.

ALC_CMC.4.3D The developer shall use a CM system.

ALC_CMC.4.1C The TOE shall be labelled with its unique reference.

ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.

ALC_CMC.4.6C The CM documentation shall include a CM plan.

ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

6.2.3.2 Problem tracking CM coverage (ALC_CMS.4)

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

6.2.3.3 Delivery procedures (ALC_DEL.1)

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

6.2.3.4 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1D The developer shall produce and provide development security documentation.

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

6.2.3.5 Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

6.2.3.6 Well-defined development tools (ALC_TAT.1)

ALC_TAT.1.1D The developer shall provide the documentation identifying each development tool being used for the TOE.

ALC_TAT.1.2D The developer shall document and provide the selected implementation-dependent options of each development tool.

ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

6.2.4 Security Target evaluation (ASE)

6.2.4.1 Conformance claims (ASE_CCL.1)

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

6.2.4.2 Extended components definition (ASE_ECD.1)

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

6.2.4.3 ST introduction (ASE_INT.1)

ASE_INT.1.1D The developer shall provide an ST introduction.

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

6.2.4.4 Security objectives (ASE_OBJ.2)

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

6.2.4.5 Derived security requirements (ASE_REQ.2)

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

6.2.4.6 Security problem definition (ASE_SPD.1)

ASE_SPD.1.1D The developer shall provide a security problem definition.

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

6.2.4.7 TOE summary specification (ASE_TSS.1)

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

6.2.5 Tests (ATE)

6.2.5.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

6.2.5.2 Testing: basic design (ATE_DPT.1)

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.1.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.

ATE_DPT.1.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

6.2.5.3 Functional testing (ATE_FUN.1)

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

6.2.5.4 Independent testing – sample (ATE_IND.2)

ATE_IND.1.1D The developer shall provide the TOE for testing.

ATE_IND.1.1C The TOE shall be suitable for testing.

6.2.6 Vulnerability assessment (AVA)

6.2.6.1 Advanced methodical vulnerability analysis (AVA_VAN.5)

AVA_VAN.5.1D The developer shall provide the TOE for testing.

AVA_VAN.5.1C The TOE shall be suitable for testing.

6.2.7 Documentation to evaluate

The security assurance requirements are justified by the the presentation to the evaluation of several documents that demonstrate compliance with these requirements.

Assurance components	Documentation
ADV_ARC.1 Security architecture description	Descripción de la arquitectura de seguridad.
ADV_FSP.4 Complete functional specification	Especificación funcional.
ADV_IMP.1 Implementation representation of the TSF	Código fuente del proyecto.
ADV_TDS.3 Basic modular design	Documentación de diseño.
AGD_OPE.1 Operational user guidance	Guía de uso.
AGD_PRE.1 Preparative procedures	Guía primeros preparativos.
ALC_CMC.4 Production support, acceptance procedures and automation	Documentación de gestión de proyectos y gestión de la configuración.
ALC_CMS.4 Problem tracking CM coverage	Lista de elementos de la configuración.
ALC_DEL.1 Delivery procedures	Procedimientos de entrega y recepción.
ALC_DVS.1 Identification of security measures	Descripción de las medidas de seguridad durante el desarrollo del proyecto.
ALC_LCD.1 Developer defined life-cycle model	Ciclo de vida de ExaCard smart card v 1.0
ALC_TAT.1 Well-defined development tools	Herramientas de desarrollo del proyecto.
ASE_CCL.1 Conformance claims	ExaCard smart card ST.
ASE_ECD.1 Extended components definition	

ASE_INT.1 ST introduction	
ASE_OBJ.2 Security objectives	
ASE_REQ.2 Derived security requirements	
ASE_SPD.1 Security problem definition	
ASE_TSS.1 TOE summary specification	
ATE_COV.2 Analysis of coverage	Análisis de la cobertura de los tests.
ATE_DPT.1 Testing: basic design	Documentación de tests.
ATE_FUN.1 Functional testing	
ATE_IND.2 Independent testing - sample	
AVA_VAN.5 Advanced methodical vulnerability analysis	Documentación de análisis de vulnerabilidades.

6.3 Security Requirements for the IT Environment

6.3.1 Certification generation application (CGA)

6.3.1.1 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: **according to directive 1999/93/EC Annex 1**.

6.3.1.2 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: [**CWA 14890-1**].

6.3.1.3 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.

6.3.1.4 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 TSF**] 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.

6.3.2 Signature creation application (SCA)

6.3.2.1 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 or SHA-2]** and cryptographic key sizes none that meet the following: **FIPS PUB 180-2**.

6.3.2.2 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.

6.3.2.3 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.

6.3.2.4 Trusted path (FTP_TRP.1)

The trusted path between the TOE and the SCA will be required only if the human interface for user authentication is not provided by the TOE itself but by the SCA.

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 or local users**] to initiate communication via the trusted path.
FTP_TRP.1.3/ SCA	The TSF shall require the use of the trusted path for [**initial user authentication**][**none**].

6.4 Security Requirements for the Non-IT Environment

R.Administrator_Guide Application of Administrator Guidance

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

R.Sigy_Guide Application of User Guidance

The SCP implementation of the requirements of the Directive, ANNEX II "Requirements for certification-service-providers issuing qualified certificates", literal (k), stipulates the signatory to follow the user guidance provided for the TOE.

R.Sigy_Name Signatory's name in the Qualified Certificate

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

7 Rationale

7.1 Introduction

The tables in sub-sections 6.2.1 “Security Objectives Coverage” and 6.3.1 “Security Requirement Coverage” provide the mapping of the security objectives and security requirements for the TOE .

7.2 Security Objectives Rationale

7.2.1 Security Objectives Coverage

Table 6.1-: Security Environment to Security Objectives Mapping

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

7.2.2 Security Objectives Sufficiency

7.2.2.1 Policies and Security Objective Sufficiency

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

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

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

7.2.2.2 Threats and Security Objective Sufficiency

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

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

T.SCD_Derive (Derive the signature-creation data) deals with attacks on the SCD via public known data produced by the TOE. This threat is countered by OT.SCD_Unique that provides cryptographic secure generation of the SCD/SVD-pair. OT.Sig_Secure ensures cryptographic secure electronic signatures.

T.DTBS_Forgery (Forgery of the DTBS-representation) addresses the threat arising from modifications of the DTBS-representation sent to the TOE for signing which than does not correspond to the DTBS-representation corresponding to the DTBS the signatory intends to sign.

The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by verifying the integrity of the DTBS-representation. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.SCA_Data_Indent.

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

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

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

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

signed) and OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity).

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

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

7.2.2.3 Assumptions and Security Objective Sufficiency

A.SCA (Trustworthy signature-creation application) establishes the trustworthiness of the SCA according to the generation of DTBS-representation. This is addressed by OE.SCA_Data_Intend (Data intended to be signed) which ensures that the SCA generates the DTBS-representation of the data that has been presented to the signatory as DTBS and which the signatory intends to sign in a form which is appropriate for being signed by the TOE

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

7.3 Security Requirements Rationale

7.3.1 Security Requirement Coverage

Table 6.2-: Functional Requirement to TOE Security Objective Mapping

TOE Security Functional Requirement / TOE Security objectives	OT.EMSEC_Design	OT.lifecycle_Security	OT.Init	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure
FCS CKM.1/RSA				x	x				x			
FCS CKM.1/ECC				x	x				x			
FCS CKM.4		x		x								
FCS COP.1/CORRESP/RSA					x							
FCS COP.1/CORRESP/ECC					x							
FCS COP.1/SIGNING/RSA												x
FCS COP.1/SIGNING/ECC												x
FDP ACC.1/SVD TRANSFER SFP						x						
FDP ACC.1/INITIALISATION SFP			x	x								
FDP ACC.1/PERSONALISATION SFP											x	
FDP ACC.1/SIGNATURE-CREATION SFP										x	x	
FDP ACF.1/INITIALISATION SFP			x	x								
FDP ACF.1/SVD TRANSFER SFP						x						
FDP ACF.1/PERSONALISATION SFP											x	
FDP ACF.1/SIGNATURE-CREATION SFP										x	x	
FDP ETC.1/SVD TRANSFER						x						
FDP ITC.1/DTBS										x		
FDP RIP.1				x							x	
FDP SDI.2/Persistent				x	x						x	x
FDP SDI.2/DTBS										x		
FDP UIT.1/SVD TRANSFER						x						
FDP UIT.1/TOE DTBS										x		
FIA AFL.1			x								x	
FIA ATD.1			x								x	
FIA UAU.1			x								x	
FIA UID.1			x								x	
FMT MOF.1				x							x	
FMT MSA.1/ADMINISTRATOR			x	x								
FMT MSA.1/SIGNATORY											x	
FMT MSA.2											x	
FMT MSA.3/			x	x							x	
FMT MTD.1											x	
FMT SMR.1				x							x	
FPT EMSEC.1	x											
FPT FLS.1				x								
FPT PHP.1							x					
FPT PHP.3								x				
FPT TST.1		x										x

FTP ITC.1/SVD TRANSFER						x						
FTP ITC.1/DTBS IMPORT										x		
FTP TRP.1/TOE											x	

Table 6.3-: IT Environment Functional requirements to Environment Security Objective Mapping

Environment Security Requirement / Environment Security objectives	OE.CGA_Qcert	OE.HI_VAD	OE.SCA_Data_Intend	OE.SVD_Auth_CGA
FCS_CKM.2/CGA	x			
FCS_CKM.3/CGA	x			
FCS_COP.1/SCA HASH			x	
FDP_UIT.1/SVD IMPORT				x
FTP_ITC.1/SVD IMPORT				x
FDP_UIT.1/SCA DTBS			x	
FTP_ITC.1/SCA DTBS			x	
FTP_TRP.1/SCA		x		
R.Sigy_Name	x			

Objectives	Requirements
	Security Assurance Requirements
OT.Lifecycle_Security	ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ALC_DEL.1, AGD_PRE.1
OT.SCD_Secrecy	ADV_IMP.1, AVA_VAN.5
OT.Sigy_SigF	AGD_OPE.1 , AVA_VAN.5
OT.Sig_Secure	AVA_VAN.5
Security Objectives	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, AVA_VAN.5

7.3.2 Security Requirements Sufficiency

7.3.2.1 TOE Security Requirements Sufficiency

OT.EMSEC_Design (Provide physical emanations security) covers that no intelligible information is emanated. This is provided by FPT_EMSEC.1.1.

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

OT.Lifecycle_Security (Lifecycle security) is provided by the security assurance requirements ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ALC_DEL.1, and AGD_PRE.1 that ensure the lifecycle security during the development, configuration and delivery phases of the TOE. The test functions FPT_TST.1 provide failure detection throughout the lifecycle. FCS_CKM.4 provides secure destruction of the SCD.

OT.SCD_Secrecy (Secrecy of signature-creation data) counters that, with reference to recital (18) of the Directive, storage or copying of SCD causes a threat to the legal validity of electronic signatures. OT.SCD_Secrecy is provided by the security functions specified by FDP_ACC.1/INITIALISATION SFP and FDP_ACF.1/INITIALISATION SFP that ensure that only authorised user can initialise the TOE and create or load the SCD. The authentication and access management functions specified by FMT_MOF.1, FMT_MSA.1, FMT_MSA.3 corresponding to the actual TOE (i.e., FMT_MSA.1/ADMINISTRATOR, FMT_MSA.3), and FMT_SMR.1 ensure that only the signatory can use the SCD and thus avoid that an attacker may gain information on it.

The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD.

The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_TST.1 and FPT_FLS.1 test the working conditions of the TOE and guarantee a secure state when integrity is violated and thus assure that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS is differential fault analysis (DFA).

The assurance requirements ADV_IMP.1 by requesting evaluation of the TOE implementation, and AVA_VAN.5 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

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

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

the cryptographic algorithms specified by FCS_CKM.1/RSA and FCS_CKM.1/ECC.

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

OT.Sigy_SigF (Signature generation function for the legitimate signatory only) is provided by FIA_UAU.1 and FIA_UID.1 that ensure that no signature generation function can be invoked before the signatory is identified and authenticated.

The security functions specified by FDP_ACC.1/PERSONALISATION SFP, FDP_ACC.1/SIGNATURE-CREATION SFP, FDP_ACF.1/PERSONALISATION SFP, FDP_ACF.1/SIGNATURE-CREATION SFP, FMT_MTD.1 and FMT_SMR.1 ensure that the signature process is restricted to the signatory.

The security functions specified by FIA_ATD.1, FMT_MOF.1, FMT_MSA.2, and FMT_MSA.3 ensure that the access to the signature generation functions remain under the sole control of the signatory, as well as FMT_MSA.1/SIGNATORY provides that the control of corresponding security attributes is under signatory's control.

The security functions specified by FDP_SDI.2 and FPT_TRP.1/TOE ensure the integrity of stored data both during communication and while stored.

The security functions specified by FDP_RIP.1 and FIA_AFL.1 provide protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication.

The assurance measures specified by AGD_OPE.1 by requesting analysis of misuse of the TOE implementation, and AVA_VAN.5 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

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

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

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

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

7.3.2.2 TOE Environment Security Requirements Sufficiency

OE.CGA_QCert (Generation of qualified certificates) addresses the requirement of qualified certificates. The functions specified by FCS_CKM.2/CGA provide the cryptographic key distribution method. The functions specified by FCS_CKM.3/CGA ensure that the CGA imports the SVD using a secure channel and a secure key access method.

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

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

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

8 TOE summary specification

This section makes a basic description of how the TOE meets each SFR.

8.1 Cryptographic support (FCS)

8.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1/RSA

Generation of asymmetric keys belongs to GENERATE ASYMMETRIC KEY PAIR ISO/IEC 7816-8 command. All key referenced operations in this function came from an algorithm identifier that has different values for each kind of key and key size. Valid algorithm identifiers are defined in the operating system configuration and are only allowed the values that can made keys --in case of RSA generation – of length 2048, 3072, 4096 bits.

The command parses the algorithm identifier and transforms it to understandable values for the corresponding function of the crypto subsystem that generates the new key with size and type given from that algorithm identifier.

FCS_CKM.1.1/ECC

Generation of asymmetric keys belongs to GENERATE ASYMMETRIC KEY PAIR ISO/IEC 7816-8 command. All key referenced operations in this function came from an algorithm identifier that has different indexes which point to different sets of ECC curve parameters which in turn define the key size. Valid algorithm identifiers are defined in the operating system configuration and are only allowed the values that can made keys --in case of ECC generation – of length 192, 224, 256, 384, 521 bits.

This command parses the algorithm identifier and transforms it to understandable values for the corresponding function of the crypto subsystem that generates the new key with size and ECC curve parameters given from that algorithm identifier.

8.1.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1

If a key is generated is not possible to regenerate it if before this key has not been deleted. After a key is completely deleted then it is possible to regenerate a key with the same reference.

To delete a key there is the proprietary command *DELETE KEY* that searches the key and deletes it from the file system which in turns deletes it from the EEPROM as specified in the user guidance of the NXP P5CC081.

8.1.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/CORRESP/RSA

The SCD/SVD correspondence is guaranteed by the RSA algorithm.

FCS_COP.1.1/CORRESP/ECC

The SCD/SVD correspondence is guaranteed by the ECC public key system. The TSF supports ECC over GF(p).

FCS_COP.1.1/SIGNING/RSA

The PSO COMPUTE DIGITAL SIGNATURE ISO/IEC 7816-8 command calls the corresponding functions of the crypto subsystem which ultimately calls functions of the NXP certified Crypto Library. These functions meet the PKCS#1 v.2.1 standard.

Following the ISO/IEC 7816-8 guidelines the PSO COMPUTE DIGITAL SIGNATURE command receives, among others, two parameters from the Security Environment:

1. The cryptographic mechanism reference which allows the user to select from one of the signature schemes, with its related parameters, defined in the PKCS#1 v2.1 standard, either the RSASSA-PSS or the RSASSA-PKCS1-v1_5.
2. The reference of a private key (the Signatory's SCD) previously generated inside the TOE which is used by the command to find the SCD user data in the file system. The private key is represented in either of the two possible formats defined in PKCS#1 and with one of the possible sizes that stated in this CC element. This is guaranteed by FCS_CKM.1.1/RSA.

FCS_COP.1.1/SIGNING/ECC

The PSO COMPUTE DIGITAL SIGNATURE ISO/IEC 7816-8 command calls the corresponding functions of the crypto subsystem which ultimately calls the ECC sign function of the NXP certified Crypto Library. This function meets the ISO/IEC 14888 Part3 standard.

Following the ISO/IEC 7816-8 guidelines the PSO COMPUTE DIGITAL SIGNATURE command receives the reference of a private key (the Signatory's SCD) previously generated inside the TOE. This key reference is used by the command to find the SCD user data in the file system. The size of the key is one of that stated in this CC element as the FCS_CKM.1.1/ECC guarantees.

8.2 User data protection (FDP)

8.2.1 Subset access control (FDP_ACC.1) and Security attribute based access control (FDP_ACF.1)

FDP_ACC.1.1/Initialisation SFP

FDP_ACF.1.1/Initialisation SFP

FDP_ACF.1.2/Initialisation SFP

FDP_ACF.1.3/Initialisation SFP

FDP_ACF.1.4/Initialisation SFP

The signatory of the TOE is identified and authenticated through his PIN.

The authorization and authentication subsystem defines an access mode (see section 1.4.1) for all

the DFs called AUT_ACL_ACCESS_DF_CREATE_KEY. This access mode refers to the generation and storing of a key pair inside this DF. For every DF are defined the necessary conditions to meet in order the AUT_ACL_ACCESS_DF_CREATE_KEY access can be performed or not.

Only when the PIN is entered and validated, and the necessary conditions of the AUT_ACL_ACCESS_DF_CREATE_KEY access mode of the current DF are fulfilled, the signatory is allowed to generate the SCD/SVD pair.

FDP_ACC.1.1/SVD Transfer SFP

FDP_ACF.1.1/SVD Transfer SFP

FDP_ACF.1.2/SVD Transfer SFP

FDP_ACF.1.3/SVD Transfer SFP

FDP_ACF.1.4/SVD Transfer SFP

The signatory is the user identified as 'user1' in the TOE who is identified and authenticated as such through his PIN.

Only the signatory is allowed to export SVD.

FDP_ACC.1.1/Personalisation SFP

FDP_ACF.1.1/Personalisation SFP

FDP_ACF.1.2/Personalisation SFP

FDP_ACF.1.3/Personalisation SFP

FDP_ACF.1.4/Personalisation SFP

The administrator is the user identified as 'user0' in the TOE who is identified and authenticated as such through his PIN.

In the initialisation phase of the life-cycle, the administrator is 'user0' implicitly although no PIN exists yet.

Only the administrator is allowed to create the RAD.

FDP_ACC.1.1/Signature-creation SFP

FDP_ACF.1.1/Signature-creation SFP

FDP_ACF.1.2/Signature-creation SFP

FDP_ACF.1.3/Signature-creation SFP

FDP_ACF.1.4/Signature-creation SFP

The signatory is the user identified as 'user1' in the TOE who is identified and authenticated as such through his PIN.

The authorization and authentication subsystem defines an access mode (see section 1.4.1) for the EF key files called AUT_ACL_ACCESS_KEY_READ. This access mode refers to the reading of the cryptographic key contained in the EF. For every EF are defined the necessary conditions to meet in order the AUT_ACL_ACCESS_KEY_READ access can be performed or not.

In addition, each cryptographic key has an attribute indicating the intended use of the key

(AUTHENTICATION_PURPOSE, SIGNATURE_PURPOSE, etc.).

We consider that an SCA is authorised when a trusted channel between this SCA and the TSF has been established following the “Key transport protocol for device authentication from CWA 14890-1: 2004” [12].

Only when the necessary conditions of the AUT_ACL_ACCESS_KEY_READ access mode of the referenced EF key file are fulfilled, the referenced key is intended for signature purpose, and the SCA is authorised, the signatory is allowed to create digital signatures for DTBS sent by the SCA.

8.2.2 Export of user data without security attributes (FDP_ETC.1)

FDP_ETC.1.1/SVD Transfer

The export of the SVD is initiated by the GENERATE ASYMMETRIC KEY PAIR ISO/IEC 7816-8 command with parameter P1='83', sent by an user to the TSF.

The SVD transfer SFP is enforced.

FDP_ETC.1.2/SVD Transfer

The SVD to export is encapsulated into an inter-industry template defined in ISO/IEC 7816-8 which contains only the public key parameters. Thus the user data is exported without the user data's associated security attributes.

8.2.3 Import of user data without security attributes (FDP_ITC.1)

FDP_ITC.1.1/DTBS

The PSO COMPUTE DIGITAL SIGNATURE ISO/IEC 7816-8 command can obtain the DTBS from outside the TSC either:

1) From its own command data field
2) From one or more previous PSO HASH ISO/IEC 7816-8 commands which have generated the DTBS data into a temporary non-persistent memory area of the TSC.

The Signature-creation SFP is enforced.

FDP_ITC.1.2/DTBS

Depending on the importing method, there are two situations:

1) The DTBS imported to the TSC is in the command data field of the PSO COMPUTE DIGITAL SIGNATURE ISO/IEC 7816-8 command as a hash-code.
2) The DTBS imported to the TSC is in the command data field of the intermediate PSO HASH ISO/IEC 7816-8 commands encapsulated into a BER-TLV data object with tag = '90'. For the final PSO HASH command the DTBS imported is in the command data field encapsulated into a BER-TLV data object with tag = '80'.

Thus no security attributes of the user data are imported to the TSC.

FDP_ITC.1.3/DTBS

The PSO COMPUTE DIGITAL SIGNATURE command can be executed only when a trusted channel has been established before. Thus the DTBS is imported by an authorised SCA.

8.2.4 Subset residual information protection (FDP_RIP.1)

FDP_RIP.1.1

When a resource, either a RAD or a SCD, located in the EEPROM is de-allocated the occupied area is filled with zeros.

When a resource, either a VAD or a SCD, located in the non-persistent memory is de-allocated the occupied area is filled with random data.

In both cases the previous information content of the resource is made unavailable after its de-allocation.

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

FDP_SDI.2.1/Persistent

Every object of the TSF file system, either an EF, DF, the system configuration areas, etc. have associated a CRC16 checksum. The CRC16 is computed after creating and updating an object. The CRC16 is verified before an object is read.

From this it follows that the SCD, RAD and SVD data persistently stored in the TOE is monitored for integrity errors.

FDP_SDI.2.2/Persistent

The detection of the data integrity errors occurs during a TSF command execution which depends on a certain user data to run properly. If that certain user data which the command depends is altered in some manner the command aborts its execution and an informative error is returned to the user and related to the context (e.g. “Reference data not usable”, “Execution error”)

For every object of the file system containing user data and to be used by an specific command the corresponding functions of the file subsystem are called to verify its integrity. These functions ultimately call the CRC16 module functions.

FDP_SDI.2.1/DTBS

The DTBS-representation imported to the TOE (in our case a hash value) is temporarily stored in the security environment of the TSF, in a non-persistent memory area.

As in the case of the persistent user data, the security environment data has associated a CRC16 checksum. The CRC16 is computed after creating and updating the non-persistent memory area containing this security environment. The CRC16 is verified whenever the security environment is read.

From this it follows that the DTBS-representation temporarily stored by the TOE is monitored for

integrity errors.

FDP_SDI.2.2/DTBS

During the PSO COMPUTE DIGITAL SIGNATURE ISO/IEC 7816-8 command execution the system function for get the DTBS-representation is called. That function ultimately calls the CRC16 module functions.

In the above context if a DTBS-representation integrity error is detected the signature-creation process does not takes place and an informative error is returned to the user.

8.2.6 Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/SVD Transfer

FDP_UIT.1.2/SVD Transfer

FDP_UIT.1.1/TOE DTBS

FDP_UIT.1.2/TOE DTBS

For inter-TSF transfer of the user data, either the SVD or the DTBS-representation, a trusted channel must be established following the “Key transport protocol for device authentication from CWA 14890-1: 2004” [12]. This trusted channel provides authenticity and integrity of the user data thus protecting and detecting it against modifications, insertions and deletions.

8.3 Identification and authentication (FIA)

8.3.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1

An unsuccessful authentication attempt is detected when the comparison between RAD and VAD is incorrect.

The VERIFY ISO/IEC 7816-4 command performs the PIN verification, comparing RAD with VAD. If RAD and VAD doesn't match, an internal counter (previously initialized with value 3) is decreased by 1. Subsequent unsuccessful authentication attempts decrease the internal counter by 1. A successful authentication attempt sets the counter value back to value 3.

FIA_AFL.1.2

When the value of the internal retry counter reaches 0, an internal flag is set indicating that the PIN is blocked. Also, if retry counter value of the PIN is 0 the VERIFY ISO/IEC 7816-4 command is forbidden for that PIN.

8.3.2 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1

The data of RAD is stored in INTERNAL files.

8.3.3 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1

The identification of the user previous to authentication is forced by FIA_UID.1. The user identification is specified in the parameters P1/P2 of the VERIFY ISO/IEC 7816-4 command.

The authentication method forces a trusted channel. The VERIFY ISO/IEC 7816-4 command performs the authentication operation. To force a trusted channel, the INTERNAL file containing the RAD will have the “secure messaging” and “external authentication” authorization attributes set for the AUT_ACL_ACCESS_INT_VERIFY access mode (see section 1.4.1).

This trusted channel provides also the trusted path for the user.

FIA_UAU.1.2

The TSF-mediated actions on behalf of an user will force user authentication. “User authentication” authorization attribute is set to force user authentication.

8.3.4 Timing of identification (FIA_UID.1)

FIA_UID.1.1

The identification method forces a trusted channel. The VERIFY ISO/IEC 7816-4 command performs the identification operation. To force a trusted channel, the INTERNAL file containing the RAD will have the “secure messaging” and “external authentication” authorization attributes set for the AUT_ACL_ACCESS_INT_VERIFY access mode (see section 1.4.1).

FIA_UID.1.2

The TSF-mediated actions on behalf of an user will force user identification. “User authentication” authorization attribute is set to force user identification.

8.4 Security management (FMT)

8.4.1 Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1

The way to access the signature operation is using the PSO COMPUTE DIGITAL SIGNATURE ISO/IEC 7816-8 command. It verifies that the indicated file containing the SCD have the correct

permissions to be used by the signatory. The permissions given for each key file are set when the file is created through the GENERATE ASYMMETRIC KEY PAIR ISO/IEC 7816-8 command that creates the file with default permissions which are defined in system configuration. Those permissions allow one user (signatory) to use that key for signature.

8.4.2 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1/Administrator

SCD/SVD management attributes in this TOE means who has the right/permission to create a key under a determined DF. If the user is not allowed to create a key under a determined DF, is SCD/SVD management not authorised. Otherwise, it is authorised to generate the key.

The DFs are created with proper permissions only by the administrator.

FMT_MSA.1.1/Signatory

Only the signatory is allowed to create a SCD/SVD pair. In this creation process the 'SCD operational' attribute of the SCD is set implicitly to 'no'. Only when the signatory wants to perform the signature operation and the conditions of the Signature-creation SFP are met, the 'SCD operational' attribute of the SCD is set implicitly to 'yes'.

From the above it follows that only the signatory has the ability to modify the security attribute 'SCD operational'.

8.4.3 Secure security attributes (FMT_MSA.2)

FMT_MSA.2.1

In the initialisation, the administrator assigns the proper values for the security attributes, and during the operational use of the TOE they cannot change to insecure values.

8.4.4 Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1

When the Signatory creates a new key for signature the 'SCD operational' security attribute of the SCD is implicitly set to 'no' (see FMT_MSA.1.1/Signatory).

FMT_MSA.3.2

The administrator can give alternate initial values of the security attributes using the configuration subsystem (see section 1.4.1).

8.4.5 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1

The CREATE REFERENCE DATA ISO/IEC 7816-4 command allows to create a new RAD, when User creates a new RAD, an ACL (see section 1.4.1) is set for that RAD, that will allow only

Signatory to modify it.

In order to modify the RAD the ISO/IEC 7816-4 CHANGE REFERENCE DATA and RESET RETRY COUNTER commands are used. A VAD verification is made to verify the user and then it will check that user is Signatory to allow modify the RAD.

8.4.6 Security roles (FMT_SMR.1)

FMT_SMR.1.1

Roles of administrator and signatory are maintained by the authorization and authentication subsystem (see section 1.4.1) which is set in each file of TOE to restrict all operations over any file.

In the initialisation phase of the life-cycle, the administrator role is implicitly assigned to the current user.

FMT_SMR.1.2

Roles are implicit associated during the creation of the TOE when all operations are made as Administrator.

When card is initialised there is 'user1' that has the role of signatory and 'user0' will be the administrator.

8.5 Protection of the TSF (FPT)

8.5.1 TOE Emanation (FPT_EMSEC.1)

FPT_EMSEC.1.1

As stated in section 1.4, the cryptographic subsystem is built on the NXP Crypto Library.

The library algorithms used for signature-creation are resistant against Side Channel Attacks, including Simple Power Analysis (SPA), Differential Power Analysis (DPA), Differential Fault Analysis (DFA) and timing attacks [6].

When sensible data is copied or moved internally in RAM (private keys, session keys, etc.), the Operating System uses the secured memory copy algorithm from the NXP Crypto Library. This avoids leaking information.

Other critical functions of the operating system are implemented in a secure way to avoid the aforementioned attacks.

The chip HW is resistant against leakage attacks for user data [5].

FPT_EMSEC.1.2

This is provided by chip HW.

8.5.2 Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1

This is provided by chip HW.

See the Security Target of NXP Secure Smart Card Controllers P5CD016/021/041V1A and P5Cx081V1A, which are developed and provided by NXP Semiconductors.

8.5.3 Passive detection of physical attack (FPT_PHP.1)

FPT_PHP.1.1

FPT_PHP.1.2

The NXP P5CD016/021/041 and P5Cx081 Secure Smart Card Controller family provides mechanisms that notify the TSF of potential physical attacks.

The TSF responds to these notifications either by doing a reset or by entering an infinite loop, depending on the context and the type of notification.

8.5.4 Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1

This is provided by chip HW.

See the Security Target of NXP Secure Smart Card Controllers P5CD016/021/041V1A and P5Cx081V1A, which are developed and provided by NXP Semiconductors.

8.5.5 TSF testing (FPT_TST.1)

FPT_TST.1.1

For each start-up process, the TOE makes tests to check the correct functionality of the TOE.

The tests done are related to the hardware main modules.

FPT_TST.1.2

The TSF data is verified for integrity during user normal operation of the TSF (see section 8.2.5).

FPT_TST.1.3

The TSFI provides the COMPUTE ROM HASH proprietary command to verify the integrity of the ROM code by applying to it the SHA-256 function and returning the result to the user.

8.6 Trusted path/channels (FTP)

8.6.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SVD Transfer

The TSF supports the “Key transport protocol for device authentication from CWA 14890-1: 2004” [12]. The CGA and the TSF can establish a trusted channel.

FTP_ITC.1.2/SVD Transfer

Once the trusted channel is established the remote trusted IT product can initiate communication via the trusted channel by sending the desired commands to the TSF via the TSFI.

FTP_ITC.1.3/SVD Transfer

For export the SVD the CGA must send the appropriate TSFI commands with appropriate parameters to the TSF via the trusted channel.

FTP_ITC.1.1/DTBS Import

The TSF supports the “Key transport protocol for device authentication from CWA 14890-1: 2004” [12]. The SCA and the TSF can establish a trusted channel.

FTP_ITC.1.2/DTBS Import

Once the trusted channel is established the SCA can initiate communication via the trusted channel by sending the desired commands to the TSF via the TSFI.

FTP_ITC.1.3/DTBS Import

For signing the DTBS-representation the SCA must send the appropriate TSFI commands with appropriate parameters to the TSF via the trusted channel.

8.6.2 Trusted path (FTP_TRP.1)

FTP_TRP.1.1/TOE

The TSF supports the “Key transport protocol for device authentication from CWA 14890-1: 2004” [12]. Once a trusted channel is established with the trusted application, the local user uses it as trusted path.

FTP_TRP.1.2/TOE

Once the trusted path is established the local user can send the desired TSFI commands to the TSF. Depending on the command the local user could be forced to identify and authenticate before.

FTP_TRP.1.3/TOE

By sending the VERIFY ISO/IEC 7816-4 command, and so the PIN, to the TSF the user can identify and authenticate.

The TSF uses the following mechanisms: Execution control list (ECL) for commands and the Access control list (ACL) for files to require the use of a trusted channel in order that the user can send his PIN.

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]** "*Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model*", Version 3.1, Revision 3, July 2009, CCMB- 2009-07-001
- **[3]** "*Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components"*, Version 3.1, Revision 3, July 2009, CCMB-2009-07-002
- **[4]** "*Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components*", Version 3.1, Revision 3, July 2009, CCMB-2009-07-003
- **[5]** NXP Semiconductors, "*NXP Secure Smart Card Controllers P5CD016/021/041V1A and P5Cx081V1A Security Target Lite*", Rev. 1.3, 21 September 2009
- **[6]** NXP Semiconductors, "C*rypto Library V2.7 on P5CD081V1A / P5CC081V1A / P5CN081V1A / P5CD041V1A / P5CD021V1A / P5CD016V1A Security Target*", Rev. 0.8, 28 April 2010
- **[7]** "*ISO/IEC 7816-3: Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*", Third edition 2006-11-01
- **[8]** "*ISO/IEC 7816-4: Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*", Second edition 2005-01-15
- **[9]** "*ISO/IEC 7816-8: Identification cards — Integrated circuit cards — Part 8: Commands for security operations*", Second edition 2004-06-01
- **[10]** "*ISO/IEC 7816-9: Identification cards — Integrated circuit cards — Part 9: Commands for card management*", Second edition 2004-06-01
- **[11]** "*CWA 14169: Secure signature-creation devices "EAL 4+" "*, March 2004
- **[12]** "*CWA 14890-1: Application Interface for smart cards used as Secure Signature Creation Devices – Part 1: Basic requirements*", March 2004