Security Target 'CardOS V5.3 QES, V1.0', Rev. 1.61, Edition 07/2014

Atos IT Solutions and Services GmbH
Otto-Hahn-Ring 6

D-81739 Munich
Germany

Disclaimer of Liability

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly and any necessary corrections included in subsequent editions. Suggestions for improvement are welcome.

Contents

1 History and Indices

Revision History:

1.61	2014-07-23	Release Version

2 About this Document

2.1 References

2.1.1 General References

[BSI-AIS31-V3]

BSI, Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik

[BSI-AIS36-V4]

BSI, Anwendungshinweise und Interpretationen zum Schema, AIS36: Kompositionsevaluierung, Version 4, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik

[BSI-PP-0035]

BSI, Security IC Platform Protection Profile, Version 1.0, 15.06.2007, BSI-PP-0035

[BSI-TR-03111-V111-ECC]

BSI, Technical Guideline TR-03111, Elliptic Curve Cryptography, Version 1.11, 2009-04-17

[CC-3.1-P1]

Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model; Version 3.1 Revision 4 September 2012, CCMB-2012-09-001

[CC-3.1-P2]

Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements; Version 3.1 Revision 4 September 2012, CCMB-2012-09-002

[CC-3.1-P3]

Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements; Version 3.1 Revision 4 September 2012, CCMB-2012-09-003

[CEM-3.1]

Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012, CCMB-2012-09-004

[CWA-14890-1]

CWA 14890-1, March 2004, Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements

[DIR-EP-1993]

Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures

[Geeignete-Algorithmen]

Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), vom 18. 2. 2013, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen,

[NIST-FIPS-PUB-186-4]

NIST, Digital Signature Standard (DSS), Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, MD 20899-8900, July 2013

[NIST-FIPS-PUB-180-4]

Secure Hash Standard (SHS), Information Technology Laboratory, National Institute of Standards and

Technology Gaithersburg, MD 20899-8900, March 2012

[NIST-800-38A-2001]

NIST, Recommendation for Block Cipher Modes of Operation, National Institute of Standards and Technology Gaithersburg, MD 20899-8900, December 2001

[ISO-IEC-7816-part-3]

Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electrical interface and transmission protocols Reference number: ISO/IEC 7816-3:2006(E)

[ISO-IEC-7816-part-4]

Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange Reference number: ISO/IEC 7816-4:2005(E)

[ISO-IEC-7816-part-8]

Identification cards - Integrated circuit cards - Part 8: Commands for security operations Reference number: ISO/IEC 7816-8:2004(E)

[ISO-IEC-9797-1-2011]

ISO/IEC, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 2001-03

[RFC-5639-2010-03]

RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010

[SigG-QES-Germany]

Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), das durch Artikel 4 Absatz 111 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist

[SigV-QES-Germany]

Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), die durch Artikel 4 Absatz 112 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist

[SigG-QES-Austria]

Gesamte Rechtsvorschrift für Signaturgesetz, Fassung vom 02.08.2013

[SigV-QES-Austria]

Gesamte Rechtsvorschrift für Signaturverordnung 2008, Fassung vom 25.07.2013

2.1.2 Common Evaluation Evidence

Note: The references in this are common for all evaluated configurations.

[AIS-V53-CardOS-ADS-Descr]

AIS, ADS Description 'CardOS V5.3 QES, V1.0', Atos IT Solutions and Services GmbH

[AIS-V53-CardOS-Adm-Guid]

AIS, Administrator Guidance 'CardOS V5.3 QES, V1.0', Atos IT Solutions and Services GmbH

[AIS-V53-CardOS-PR-Notes]

AIS, CardOS V5.3 Chipcard Operating System, Packages & Release Notes, Atos IT Solutions and Services GmbH

[AIS-V53-CardOS-User-Guid]

AIS, User Guidance 'CardOS V5.3 QES, V1.0', Atos IT Solutions and Services GmbH

[AIS-V53-CardOS-Users-Manual]

AIS, CardOS V5.3 Chipcard Operating System, User's Manual, Atos IT Solutions and Services GmbH Edition 05/2014

[BSI-CC-PP-0035-2007]

BSI, Certification Report BSI-CC-PP-0035-2007 for Security IC Platform Protection Profile Version 1.0 from Atmel Secure Products, Infineon Technologies AG, NXP Semiconductors Germany GmbH, Renesas Technology Europe Ltd, STMicroelectronics

[BSI-CC-PP-0071]

BSI, Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application, prEN 14169-4:2012, Date: 2012-11, v1.0.1

[BSI-CC-PP-0071-2012]

BSI, BSI-CC-PP-0071-2012 for Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application, Version 1.0.1, V1.0, 12 December 2012

[BSI-MR-CC-PP-0059-2009-MA-01]

BSI, Assurance Continuity Maintenance Report, Protection profiles for secure signature creation device - Part 2: Device with key generation, Version 2.0.1 from CEN/ISSS - Information Society Standardization System, 21 February 2012

[BSI-CC-PP-0059-2009-MA-01]

BSI, Protection profiles for Secure signature creation device - Part 2: Device with key generation, prEN 14169-2:2012, Date: 2012-01, v2.0.1

[BSI-DSZ-CC-0782-2012-MA-01]

BSI, Assurance Continuity Maintenance Report, Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, ECv1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG, 5 September 2013

[Infineon-ST-Chip-B11-2013-08-13]

Infineon, Security Target Lite for maintenance process ACM M7892 B11, (comprises the Infineon Technologies Security Controller M7892 B11 with specific IC dedicated software and optional RSA v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries), Version: 1.4, Date: 2013-08-26

[Infineon-Chip-HW-Ref]

Infineon, M7892 Controller Family for Security Applications - Hardware Reference Manual Revision 1.3 2013-03-11 and Errata Sheet Revision 1.5 2013-09-18

2.2 Tables

2.3 Acronyms

ADS
: Application Digital Signature

APDU
: Application Protocol Data Unit

CC
: Common Criteria

CfPA
: Composite-fulfilled Platform Assumption

CGA
: Certificate generation application

CSF
: CardOS Sequence Format

CSP
: Certification service provider

CVCA
: Country Verifying Certification Authority

DF
: Dedicated File

DPA
: Differential Power Analysis

DTBH
: Data to be hashed

DTBS
: Data to be signed

DTBS/R
: Representation of DTBS

EAL
: Evaluation Assurance Level

EC
: Elliptic Curve

ECDSA
: Elliptic Curve Digital Signature Algorithm

EF
: Elementary File

IC
: Integrated Circuit

ICC
: IC Card

ICCSN
: ICC Serial Number

IP_SFR
: Irrelevant Platform SFR

IFD
: Interface Device

IT
: Information Technology

LCS
: Life Cycle Status

MAC
: Message Authentication Code

n.a.

n/a
: not applicable

PIN
: Personal Identification Number

PP
: Protection Profile

PTRNG
: physical true RNG (short: physical RNG)

PUK
: Personal Unblocking Key

QES
: Qualified Electronic Signature

RA
: Registration Authority

RAD
: Reference Authentication Data

RP_SFR
: Relevant Platform SFR

SCA
: Signature-Creation Application

SCD
: Signature-Creation Data

SCIC
: Smart Card IC

SCS
: Signature-Creation system

SDO
: Signed Data Object

SE
: Security Environment

SFP
: Security Function Policy

SFR
: Security Functional Requirement

SLE78CFX*P (M7892 B11)
: SLE78CFX2400P, SLE78CFX3000P or SLE78CFX4000P (design step B11)

SM
: Secure Messaging

SPA
: Simple Power Analysis

SS
: Security Service

SSCD
: Secure Signature Creation Device

SSC
: Send Sequence Counter

ST
: Security Target

SVAD
: Signatory VAD

SVD
: Signature Verification Data

TA
: Terminal Authentication

TC
: Trust Center

TOE
: Target of Evaluation

TSF
: TOE Security Functions

VAD
: Verification Authentication Data

2.4 Terms and Definitions

2.4.1 Security Evaluation Terms

Common Criteria
: CC: set of rules and procedures for evaluating the security properties of a product

Evaluation Assurance Level
: EAL: a set of assurance requirements for a product, its manufacturing process and its security evaluation specified by Common Criteria

Protection Profile
: PP: document specifying security requirements for a class of products that conforms in structure and content to rules specified by common criteria

Security Target
: ST: document specifying security requirements for a particular product that conforms in structure and content to rules specified by common criteria, which may be based on one or more Protection Profiles

Target of Evaluation
: TOE: abstract reference in a document, such as a Protection Profile, for a particular product that meets specific security requirements

TOE Security Functions
: TSF: functions implemented by the TOE to meet the requirements specified for it in a Protection Profile or Security Target

2.4.2 Technical terms

Notes:

1. Terms marked with asterisks (*) are added to contents of PP [BSI-CC-PP-0059-2009-MA-01].
2. References in [DIR-EP-1993] to a specific article and paragraph of this directive are of the form '(The Directive: n.m)'.

* Activated Application for QES
: The Signatory PIN is set.

* ADS Configuration
: Finalizing the TOE configuration with Application for QES for a signatory's use. For this purpose, the life cycle phase is temporarily changed from OPERATIONAL to ADMINISTRATION. Generally, the ADS Configuration comprises following tasks: 1. Exporting of the SVD 2. Optional creation or deletion of EFs / DFs, e.g. for storing of certificates 3. Importing of Transport PIN.

Advanced electronic signature
: Digital signature which meets specific requirements in The Directive (The Directive: 2.2) Note: according to The Directive a digital signature qualifies as an electronic signature if it: * is uniquely linked to the signatory; * is capable of identifying the signatory; * is created using means that the signatory can maintain under his sole control, and * is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Authentication data
: Information used to verify the claimed identity of a user

* Authentication Scheme
: Used to authenticate the card to a user and a user to the card.

* Basic Configuration
: The process of configuring the basic configuration of the TOE. Generally, the Basic Configuration comprises the following tasks: 1. Performing acceptance procedures (identification of card) 2. Installation of a personalization image (creation of the Master File, installation of objects and the import of a personalization authentication key for establishing a mutually authenticated Trusted Channel) 3. Loading and activation of packages (optional) 4. Configuration of MF 5. Creation and configuration of Application for QES 6. Generating signature key pair 7. Deletion of personalization authentication key 8. Secure delivery to the end user.

Certificate
: Digital signature used as electronic attestation binding an SVD to a person confirming the identity of that person as legitimate signer (The Directive: 2.9)

Certificate info

Information associated with a SCD/SVD pair that may be stored in a secure signature creation device. Note: Certificate info is either * a signer's public key certificate or, * one or more hash values of a signer's public key certificate together with an identifier of the hash function used to compute the hash values. Certificate info may be combined with information to allow the user to distinguish between several certificates.

Certificate generation application
: Collection of application components that receive the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate.

Certification service provider
: Entity that issues certificates or provides other services related to electronic signatures (The Directive: 2.11).

* Confirmation
: An assessment of technical components and products for legally valid electronic signatures; the assessment checks if the applicable regulatory requirements are fulfilled.

Data to be signed
: All electronic data to be signed including a user message and signature attributes.

Data to be signed or its unique representation
: Data received by a secure signature creation device as input in a single signature creation operation. Note: DTBS/R is either * a hash-value of the data to be signed (DTBS), or * an intermediate hash-value of a first part of the DTBS complemented with a remaining part of the DTBS, or * the DTBS.

* Deactivated Application for QES
: The Transport Protection cannot be disabled because the Transport PIN is not set.

* DF
: Dedicated File

* EF
: Elementary File

* Floor
: Mathematical operation which means: round down to the next integer.

Legitimate user
: User of a secure signature creation device who gains possession of it from an SSCD-provisioning service provider and who can be authenticated by the SSCD as its signatory.

* Mutually authenticated Trusted Channel
: Is a channel which is set up by means of the Authentication Scheme.

Notified body
: Organizational entity designated by a member state of the European Union as responsible for accreditation and supervision of the evaluation process for products conforming to this standard and for determining admissible algorithms and algorithm parameters (The Directive: 1.1b and 3.4)

Qualified certificate
: Public key certificate that meets the requirements laid down in Annex I and that is provided by a CSP that fulfills the requirements laid down in Annex II (The Directive: 2.10)

Qualified electronic signature
: Advanced electronic signature that has been created by an SSCD with a key certified with a qualified certificate (The Directive: 5.1)

Reference authentication data
: Data persistently stored by the TOE for authentication of a user as authorized for a particular role.

* Registration Authority
: The (local or remote) Registration Authority (RA) is an organizational entity which acts under the TC's security policy. The RA is often locally separated from a TC.

Secure signature creation device
: Personalized device that meets the requirements laid down in (The Directive: A.III) by being evaluated according to a security target conforming to the PP [BSI-PP0059-2009] (The Directive: 2.5 and 2.6).

Signatory
: Legitimate user of an SSCD associated with it in the certificate of the signature-verification and who is authorized by the SSCD to operate the Signature-creation function (The Directive: 2.3).

Signature attributes
: Additional information that is signed together with a user message.

Signature-creation application
: Application complementing an SSCD with a user interface with the purpose to create an electronic signature. Note: A signature-creation application is software consisting of a collection of application components configured to: * present the data to be signed (DTBS) for review by the signatory, * obtain prior to the signature process a decision by the signatory, * if the signatory indicates by specific unambiguous input or action its intent to sign send a DTBS/R to the TOE * process the electronic

signature generated by the SSCD as appropriate, e.g. as attachment to the DTBS.

Signature-creation data
: Private cryptographic key stored in the SSCD under exclusive control by the signatory to create an electronic signature (The Directive: 2.4).

Signature-creation system
: Complete system that creates an electronic signature consists of the SCA and the SSCD.

Signature-verification data
: Public cryptographic key that can be used to verify an electronic signature (The Directive 2.7).

SSCD-provisioning service
: Service to prepare and provide an SSCD to a subscriber and to support the signatory with certification of generated keys and administrative functions of the SSCD

* StartKey
: Is a key stored in the User EEPROM. It is needed for the protection of card commands and is changed from the secret factory value to a known value with a command sequence provided by the developer.

* Terminal
: A terminal is the hardware and software combination which interacts with the card (and thus the end user) in the Operational Phase of the card.

* Transport PIN
: For the activation and first setting of the PIN and (optional) PUK of the Signatory. The Transport-PIN is used to activate the signature function. After entering the correct Transport-PIN the Signatory has to set his/her individual PIN and (optional) PUK values. Thereafter the PIN and (optional)PUK will be unblocked (thus activated) by the TOE.

* Transport Protected Application for QES
: The Transport PIN is set and the Signatory PIN is not set.

* Trust Center
: The Trust Center (TC) is an organizational entity which may comprise of the entities Initialization Service, Personalization Service, Certification Authority acting as Certification Service Provider and Registration Authority, all acting under the TC's security policy.

User
: Entity (human user or external IT entity) outside the TOE that interacts with the TOE.

User Message
: Data determined by the signatory as the correct input for signing.

Verification authentication data
: Data provided as input to a secure signature creation device for authentication by cognition or by data derived from a user's biometric characteristics.

3 Security Target Introduction (ASE_INT)

3.1 ST Reference

Title

Security Target 'CardOS V5.3 QES, V1.0'

Author

Atos IT Solutions and Services GmbH

Revision Number

1.61

General Status

Release

CC Version

3.1, Revision 4

Certification ID

BSI-DSZ-CC-921

The TOE is based on the Infineon Chip SLE78CFX*P (M7892 B11) as ICC platform, which requires a composite evaluation.

This ST provides

- the introduction (ASE_INT), in this chapter,
- the conformance claims in 4 Conformance Claims (ASE_CCL),
- the security problem definition in 5 Security Problem Definition (ASE_SPD),
- the security objectives in 6 Security Objectives (ASE_OBJ)
- the extended components definition in 7 Extended Component Definition (ASE_ECD),
- the security and assurance requirements in 8 IT Security Requirements (ASE_REQ),
- the rationale in 9 Rationale, and
- the TOE summary specification (TSS) in 10 TOE summary specification (ASE_TSS).

3.2 TOE Reference

The TOE 'CardOS V5.3 QES, V1.0' [1] is based on the Infineon chip SLE78CFX*P (M7892 B11) as ICC platform. The hardware and the software of the TOE is determined by the components listed within Table 1: Components of the TOE.

SLE78CFX*P (M7892 B11) is an abbreviation and denotes 3 contact based chips (design step B11) which differ only in flash size:

- SLE78CFX2400P with 240kByte flash
- SLE78CFX3000P with 300kByte flash
- SLE78CFX4000P with 404kByte flash

The Infineon chip SLE78CFX*P (M7892 B11) is certified, see [Infineon-ST-Chip-B11-2013-08-13] and [BSI-DSZ-CC-0782-2012-MA-01].

The TOE (Application for QES) is configured in two steps:

1. A Trust Center (TC) creates Application for QES including generation of a key pair but it is deactivated because the Transport Protection cannot be disabled (the Transport PIN is not set). After the Trust

1 Note: The TOE is part of a electronic identity document and may contain further applications besides the 'CardOS V5.3 QES, V1.0' (SSCD application).

Center finishes this step the TOE is in phase OPERATIONAL.
2. Using a mutually authenticated Trusted Channel a (local) Registration Authority
   a) exports the SVD
   b) optionally creates EFs / DFs below DF_QES including updating them, e.g. with certificates
   c) imports the Transport PIN.

Notes:

1. Before the Transport PIN is imported the Application for QES is deactivated.
2. After importing the Transport PIN the Application for QES is prepared for activation by the Signatory.
3. After the Transport Protection of the Application for QES is disabled by the Signatory, the PIN of the Signatory is set and thus the Application for QES is activated and the Signatory is enabled to perform SSCD activities.
4. The optional EFs may be used to store certificates, e.g. the (qualified) certificate belonging to the SCD/SVD pair and a second certificate belonging to the Certification Authority which generates the (qualified) certificate belonging to the SCD/SVD pair.
5. The (local) Registration Authority is able to perform the optional step 2.b more than one time. That means the (local) Registration Authority is able to create further EFs / DFs below DF_QES or it is able to update all created EFs / DFs below DF_QES (again).

3.3 TOE overview

1. **TOE type**

The underlying platform of the TOE is a Smart Card Integrated Circuit (SCIC), which can be used as wafer, module, smart card ("card" for short) or another IC package. The SCIC already contains the OS "CardOS V5.3" when delivered. The TOE as defined by this Composite Security Target consists of the SCIC and the Application for QES. It is to be used as a Secure Signature Creation Device (SSCD). The SCIC is a SLE78CFX*P (M7892 B11) from Infineon.

When the TOE is delivered, it is not yet embedded in a card.

2. **Usage and major security features of the TOE**

The TOE allows to generate cryptographically strong signatures over previously externally or internally calculated hash values including last round hashing. The TOE generates the signature key pair (SCD/SVD). The TOE is able to protect the secrecy of the internally generated and stored Signature Creation Data (SCD, i.e. secret key) and restricts its usage to the authorized Signatory only. This restriction on usage is done via the well known PIN authentication mechanism.

The Trust Center does not configure the TOE 'CardOS V5.3 QES, V1.0' completely. It only performs the first configuration step. This Basic Configuration includes the import of symmetric key data individual to the card (depends on ICCSN) used by an Authentication Scheme and generation of the signature key pair. After this step the Application of QES is deactivated since the value of the Transport PIN is not yet imported and thus the Transport Protection cannot be disabled. At this point the card is delivered in a secure way to the end user.

A (local or remote) RA performs the second configuration step after the card holder applies for the Application for QES. This ADS Configuration includes exporting of the SVD, importing of the Transport PIN and optionally the creation / updating of EFs and DFs below DF_QES. The optional EFs may be used to store certificates, e.g. the (qualified) certificate belonging to the key pair and a second certificate belonging to the Certification Authority which generates the (qualified) certificate belonging to the key pair. After this step the Application of QES is prepared for activation by the Signatory.

To secure the second configuration step, the TOE 'CardOS V5.3 QES, V1.0' which was configured using Basic Configuration provides an Authentication Scheme for the (local or remote) RA which consists of a mutual authentication between the TOE and the (local or remote) Registration Authority. Additionally the Authentication Scheme results in sessions keys used by a Trusted Channel securing the ADS Configuration from modification and disclosure.

The ADS Configuration always has to be executed using the means of a secure mutually authenticated Trusted Channel. This configuration step is executed at the (local) RA office or by a RA remotely using the Internet (e.g. from the home PC of the end user). The authentication of a (local or remote) RA office is done using the Authentication Scheme.

It is possible to configure the TOE 'CardOS V5.3 QES, V1.0' as follows:

- the signature-creation function uses the ECDSA or the RSA algorithm for creating signatures
- a PUK for unblocking the PIN is available or not
- the retry counter of the PIN depends on the length of the PIN or not.

3. **Required non-TOE hardware/software/firmware**

The SCIC on which the TOE bases conforms to ISO 7816 and needs the usual IT environment for such smart cards, i.e. a SCA on the host connected with a smart card terminal.

4. **Optional Non-TOE software**

The SCIC product containing the Application for QES also may contain further applications, besides the 'CardOS V5.3 QES, V1.0' (SSCD application).

3.4 TOE description

The TOE is a secure signature creation device (SSCD) according to the Protection Profile [BSI-CC-PP-0059-2009-MA-01] for a Secure Signature Creation Device with key generation issued by the European Committee for Standardization, Information Society Standardization System (CEN/ISSS) as update of the Electronic Signatures (E-SIGN) CEN/ISSS workshop agreement (CWA) 14169:2002, Annex C on the protection profile secure signature creation devices, "EAL 4+".

The Protection Profile [BSI-CC-PP-0059-2009-MA-01] is a Protection Profile according to Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [DIR-EP-1993].

The following list outlines the TOE deliverables:

- the underlying hardware (SLE78CFX*P (M7892 B11) from Infineon) with OS "CardOS V5.3" used to implement the secure signature creation device (SSCD) and
- the configured software (the configuration script files which represents the installation of Application for QES)
- the pertaining guidance documentation
  'ADS Description V5.3' [AIS-V53-CardOS-ADS-Descr]
  'User Guidance CardOS V5.3' [AIS-V53-CardOS-User-Guid],
  'Administrator Guidance CardOS V5.3' [AIS-V53-CardOS-Adm-Guid],
  'CardOS V5.3 User's Manual' [AIS-V53-CardOS-Users-Manual] and
  'CardOS V5.3 Packages & Release Notes' [AIS-V53-CardOS-PR-Notes].

The TOE developer delivers the SCIC, the configuration script files for configuration and pertaining documentation. The Trust Center configures the TOE using the scripts for *Basic Configuration* and the (local) Registration Authority configures the TOE using the scripts for *ADS Configuration*.

The TOE utilizes the evaluation of the underlying platform, which includes the Infineon chip SLE78CFX*P (M7892 B11), the IC Dedicated Software and the libraries EC v1.02.013, SHA-2 v1.01, RSA-library 1.02.013 and Toolbox v1.02.013 libraries. The security functionality TDES and AES supported by the Infineon chip SLE78CFX*P (M7892 B11) are utilized by the TOE, too.

The SW image is built by a so called "Mask Building" process which needs

- CardOS V5.3 sources
- certified libraries of SLE78CFX*P (M7892 B11) (as needed by CardOS V5.3 sources) and
- the tool "Post Locater" (provided by Infineon)

The CardOS V5.3 sources are compiled and linked with the binary libraries. The result is a "generic" mask

which is used by the tool "Post Locater" to generate different hex files according to the different sizes of SLE78CFX*P (M7892 B11). These hex files are delivered to Infineon. The flash loader is deactivated when the Infineon chip leaves the production site.

The Infineon chip SLE78CFX*P (M7892 B11) is certified, cf [BSI-DSZ-CC-0782-2012-MA-01] for SLE78CFX*P (M7892 B11) from Infineon Technologies AG. The silicon of SLE78CFX*P (M7892 B11) is produced in Dresden, Germany only.

Table 1: Components of the TOE

No.	Type	Term	Version	Date	Form of delivery
1	Hardware (chip)	SLE78CFX*P (M7892 B11)	M7892 B11	-	IC package
2	Software	CardOS for 240kByte flash	"C903"	*	loaded in protected part of Flash EEPROM
3		CardOS for 300kByte flash	"C903"	*	
4		CardOS for 404kByte flash	"C903"	*	
5		EC-library	1.02.013	-	
		SHA-2-library	v1.01		
		RSA-library	1.02.013		
		Toolbox	1.02.013		
6	Configuration script for RSA based QES Base Packet	ConfigAppRSABase.csf	*	*	file
7	Configuration script for EC based QES Base Packet	ConfigAppECBase.csf	*	*	file
8	Configuration script for QES ADS Packet	ConfigAppADS.csf	*	*	file
9	Constants definitions for EC key pair with secp256r1	Defines_EC_secp256r1.csf	*	*	file
10	Constants definitions for EC key pair with secp384r1	Defines_EC_secp384r1.csf	*	*	file
11	Constants definitions for EC key pair with brainpoolP256r1	Defines_EC_brainpoolP256r1.csf	*	*	file
12	Constants definitions for EC key pair with brainpoolP384r1	Defines_EC_brainpoolP384r1.csf	*	*	file
13	Constants definitions for RSA key pair, length 2048 bits	Defines_RSA_2048.csf	*	*	file

No.	Type	Term	Version	Date	Form of delivery
14	Constants definitions for RSA key pair, length 2560 bits	Defines_RSA_2560.csf	*	*	file
15	Constants definitions for RSA key pair, length 3072 bits	Defines_RSA_3072.csf	*	*	file
16	Constants definitions for RSA key pair, length 3584 bits	Defines_RSA_3584.csf	*	*	file
17	Constants definitions for RSA key pair, length 4096 bits	Defines_RSA_4096.csf	*	*	file
18	Documentation	[AIS-V53-CardOS-Users-Manual]	05/2014	-	PDF file
19		[AIS-V53-CardOS-PR-Notes]	*	-	PDF file
20		[AIS-V53-CardOS-Adm-Guid]	*	*	PDF file
21		[AIS-V53-CardOS-User-Guid]	*	*	PDF file
22		[AIS-V53-CardOS-ADS-Descr]	*	*	PDF file

Notes:

1. (*) The final version and date information of these files will be defined at the end of the evaluation and will be listed in the certification report and the ETR Summary.
2. Personalization files (CardOS Sequence Format CSF) determine how the Trust Center can set up the TOE. This can include different choices, e.g. for minimal PIN length or for signature key length.
3. Items (6) and (7) contain the Basic Configuration for Application for QES (RSA or EC based signature creation)
4. Item (8) contains the *ADS Configuration* to finalize the configuration provided by items (6) or (7).
5. The Trust Center is allowed to make changes or extensions in items (6), (7) and (8) which are marked by the developer. These changes or extensions concern: in case of EC which domain parameters of an EC curve shall be imported, in case of RSA which bit length shall be used, whether a PUK shall be available or not or which value shall be used for the retry counter of the Signatory PIN

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

1. to generate the signature creation data (SCD) and the corresponding signature verification data (SVD) and
2. to create a **single** electronic signature
   a) after allowing for the data to be signed (DTBS) to be displayed correctly where the display function is provided by the TOE environment
   b) using appropriate hash functions that are, according to a standard (see chapter 8.2.2 Table of cryptographic mechanisms used) agreed as suitable for electronic signatures
   c) after appropriate authentication of the Signatory by the TOE
   d) after transferring the DTBS, DTBS/R or the intermediate value + remainder of DTBS (last round hashing) by sending the appropriate APDU
   e) using an appropriate cryptographic signature function that employs appropriate cryptographic parameters and key lengths agreed as suitable according to a standard (see chapter 8.2.2 Table of cryptographic mechanisms used)

When the TOE is leaving the Trust Center the Application for QES is deactivated since the Transport PIN is not imported by the Trust Center during the *Basic Configuration*. In this state the TOE however provides an Authentication Scheme for setting up a secure mutually authenticated Trusted Channel for securing all data from modification and disclosure and providing the (local) RA a mechanism to authenticate itself to the TOE and vice versa the TOE to the (local) RA.

To perform the *ADS Configuration* the TOE provides following functions which are securely performed using the means of a mutually authenticated Trusted Channel:

1. export of the public key data of the generated key pair
2. optional creation including update of EFs / DFs below DF_QES, e.g. with the qualified certificate and the certificate of the Certification Authority which generates the qualified certificate. The RA is able to remove EFs, DFs below DF_QES, too.
3. import of the Transport PIN, from now on the Application for QES is is prepared for activation by the Signatory.

The ADS Configuration can be done at a (local) RA or at a (remote) RA using the Internet.

Note:

1. The (local) Registration Authority is able to perform the optional steps 1 + 2 more than one time. That means the (local) Registration Authority is able
   - to create further EFs / DFs below DF_QES
   - to update all created EFs / DFs below DF_QES (again)
   - to remove (all) EFs / DFs below DF_QES

   in further sessions.
2. The Trust Center or the (local) Registration Authority is not able to remove DF_QES or to create / remove objects within DF_QES or to update other objects than TPIN_QES (possible only once) within DF_QES.

The PIN of the Signatory has to be entered first before the signature-creation function can be used.

In case the PUK is absent:

- If the Signatory cannot remember his PIN, neither the Signatory nor the Trust Center are able to set a new PIN.
- If the PIN of the Signatory is blocked, it is not possible to unblock it.

In case the PUK is present:

- If the Signatory cannot remember his PIN, neither the Signatory nor the Trust Center are able to set a new PIN.
- If the PIN of the Signatory is blocked, the Signatory uses the PUK to unblock it.
- If the Signatory cannot remember his PUK, neither Signatory nor the Trust Center are able to set a new PUK.
- If the PUK of the Signatory is blocked or if it's use counter is zero, it is not possible to unblock it or to set the use counter to a new value.

Note:

1. If a PUK is present, the PUK has a finite use counter.

The TOE implements all IT security functionality which is necessary to ensure the secrecy of the SCD. To prevent the unauthorized usage of the SCD, the TOE provides user authentication and access control. The interface for the user authentication is provided by the trusted TOE environment. The TOE protects the SCD during the whole life cycle as to be solely used in the signature creation process by the legitimate Signatory.

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 uses authentication by knowledge. For authentication purposes, the TOE holds Reference Authentication Data (RAD) that will be used to check inputs of Verification Authentication Data (VAD). The human interface for user authentication (VAD input) is implemented in the trusted TOE environment.

Figure 1 shows the ST scope from the structural perspective. The TOE comprises the underlying hardware, the

operating system (OS), the SCD/SVD generation, SCD storage and use, hash-generation and Signature-creation functionality. The TOE limit is indicated by a shaded box with the label "TOE". An SCIC product containing the Application for QES may contain additional applications, besides the 'CardOS V5.3 QES, V1.0' (SSCD application), e.g. for electronic identity documents. The SCA and the CGA (and possibly other applications) are part of the immediate environment of the TOE.

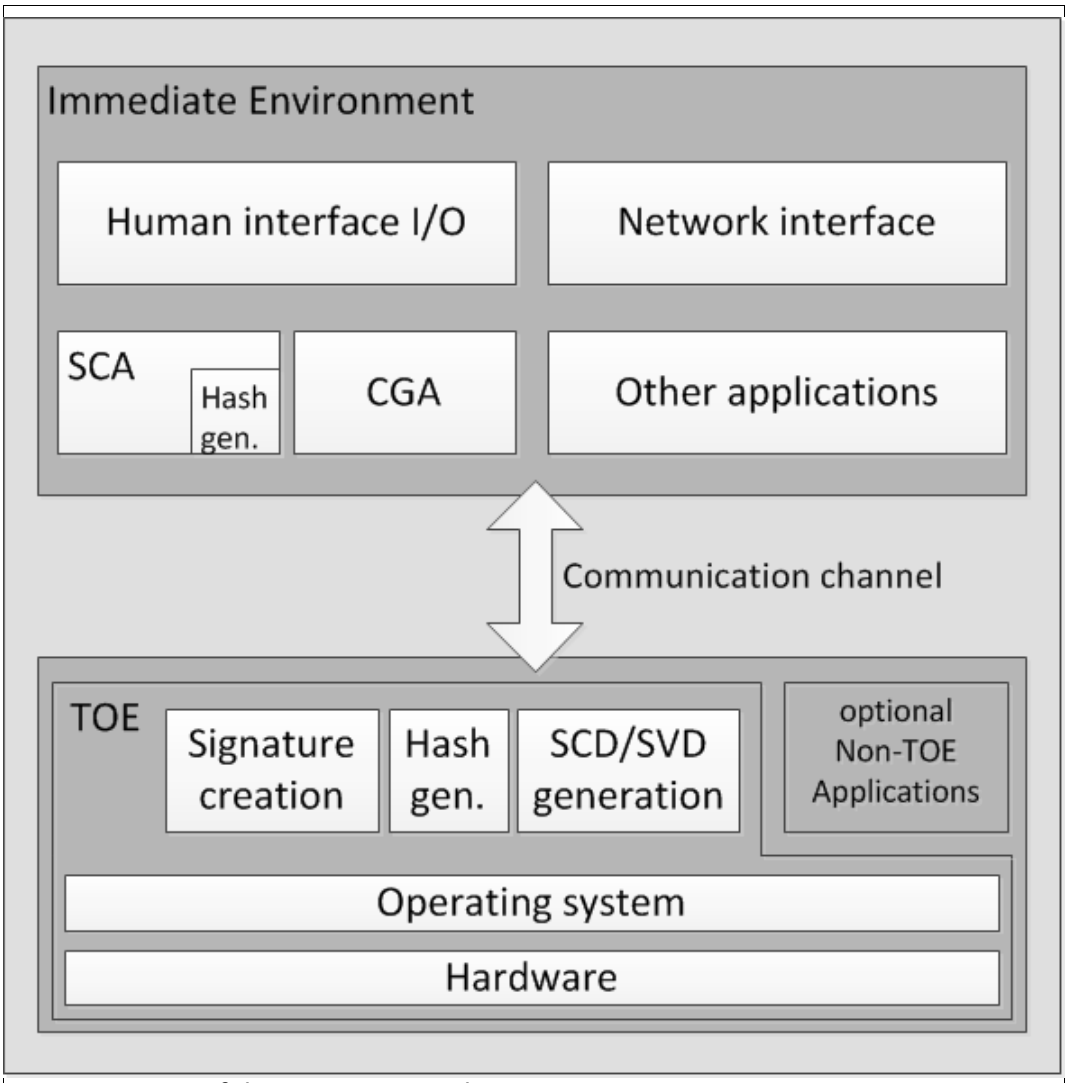

Figure 1: Scope of the SSCD, structural view

The contact based physical interface of the TOE is provided by a connection according to [ISO-IEC-7816-part-3]. This interface is used to transmit an APDU command to the TOE and receive the corresponding response APDU from the TOE as specified in [ISO-IEC-7816-part-4] and [ISO-IEC-7816-part-8].

3.4.1 PP's SSCD life cycle

The following figure is taken from PP, [BSI-CC-PP-0059-2009-MA-01], which "shows an example of the life cycle where an SCD/SVD pair is generated on the TOE before delivery to the signatory. The life cycle may allow generation of SCD or SCD/SVD key pairs after delivery to the signatory as well"

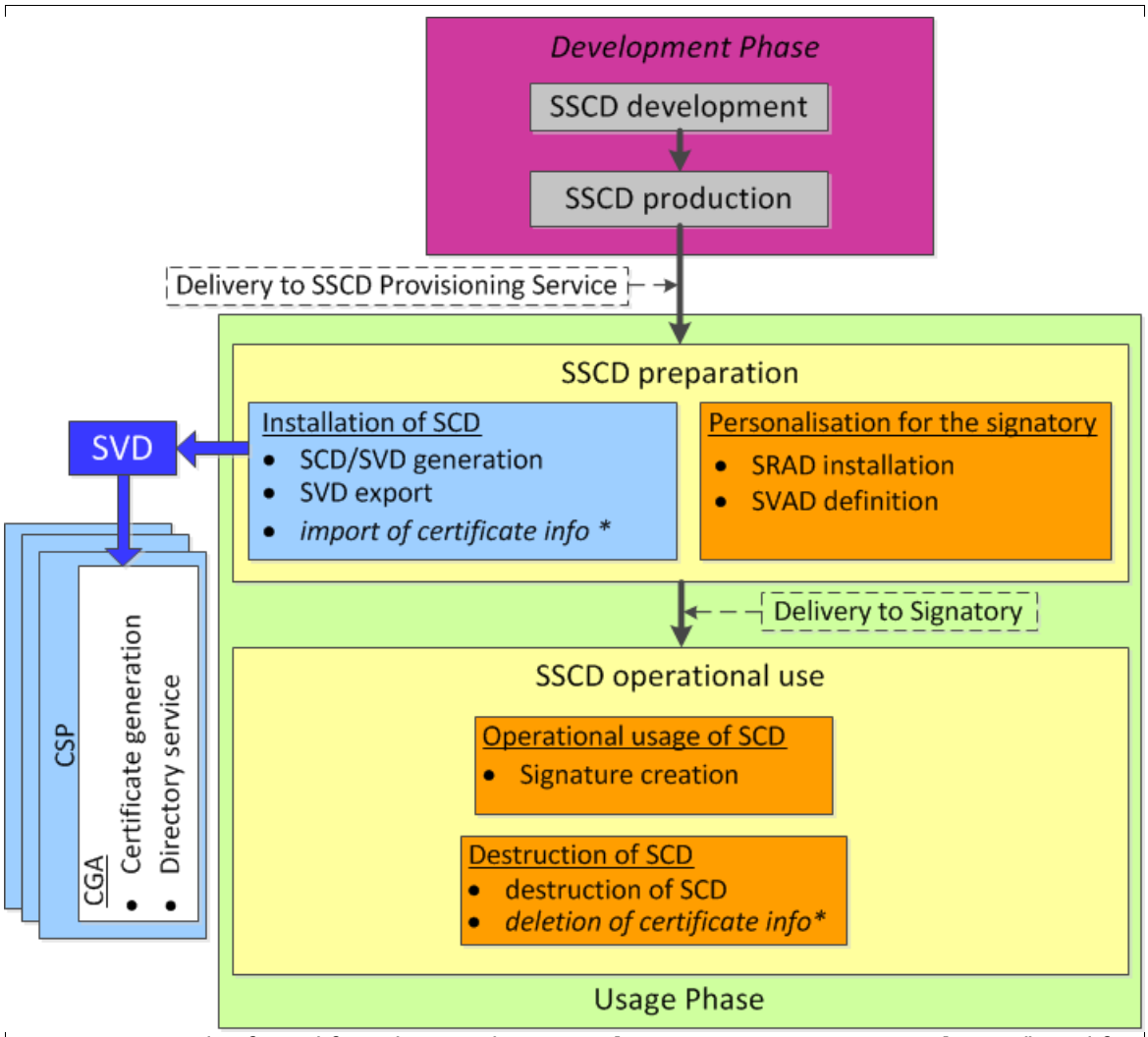

Figure 2: Example of TOE life cycle according to PP, [BSI-CC-PP-0059-2009-MA-01] 4.3.3 "TOE life cycle".

PP's example SSCD life cycle distinguishes two phases:

- Development Phase and
- Usage Phase.

The Development Phase distinguishes the following stages:

- SSCD Development and
- SSCD Production.

The Usage Phase distinguishes the following stages:

- SSCD Preparation, which includes installation of SCD (generation of SCD/SVD, export of SVD to CSP and import of certificate info*) and personalization for the Signatory (SRAD installation and SVAD definition)
- SSCD Operational Use, which includes operational usage of SCD (Signature creation) and destruction of SCD (destruction of SCD and deletion of certificate info*)

Note:

1. The asterisks '*' mark the optional import of certificate info during TOE preparation and certificate info deletion when SCD is destroyed.
2. The CSP generates the certificate using a CGA and provides a directory service.

3.4.2 Mapping of PP's SSCD life cycle onto TOE's life cycle

The TOE provides other notations for the life cycle than the example of the PP, cf [BSI-CC-PP-0059-2009-MA-01].

The following table maps this TOE's life cycle, [AIS-V53-CardOS-Users-Manual] "Card Life Cycle Phases", onto PP's SSCD example life cycle:

TOE life cycle phases	PP example life cycle phases
	Development Phase
MANUFACTURING	Usage Phase
PHYSINIT	
PHYSPERS	
ADMINISTRATION	
OPERATIONAL	
DEATH	-

Note:

1. "PHYSINIT" and "PHYSPERS" together describe the PHYSICAL PERSONALIZATION, cf. CardOS V5.3 User's Manual, [AIS-V53-CardOS-Users-Manual], lists in "Card Life Cycle Phases".

The preparation of this TOE does not include

- Export of SVD to CSP and import of certificate info
  The task "export of SVD to CSP and import of certificate info" is performed for this TOE after issuing the card to the end user at life phase OPERATIONAL by the (local) RA if the user applies for Application for QES.
- Personalization for the Signatory with SRAD installation and SVAD definition
  These tasks are performed for this TOE by the Signatory after the Application for QES is prepared for activation by importing the Transport PIN. If the Signatory enters successfully the Transport PIN, he is able to install his RAD.

MANUFACTURING is the phase after chip production and provides an implicit authentication of the administrator. It represents the portion of configuration which comprises performing acceptance procedures, the installation of a personalization image (secured by implicit authentication using the start key) and start-up in the CC terminology (first part of the Basic Configuration). The installation of the personalization image consists of:

1. the creation of the MF
2. the installation of objects and the import of a personalization authentication key for establishing a mutually authenticated Trusted Channel
3. switching the card to phase OPERATIONAL.

With switching to phase OPERATIONAL the TOE is delivered in the sense of CC.

Note:

1. After the card is switched the first time to phase OPERATIONAL it is only possible to switch it temporarily to phase ADMINISTRATION. After a reset the card always is in phase OPERATIONAL.
2. Installing the personalization image is a PHYSICAL PERSONALIZATION which runs through the life cycle phases PHYSINIT and PHYSPERS.
3. The card is only switched temporarily to phase ADMINISTRATION after the card has been switched to phase OPERATIONAL for the first time. In this sense ADMINISTRATION can be seen rather as a state

than as a life cycle phase of this TOE.

Phase OPERATIONAL represents the portion of configuration which comprises

- the second part of the Basic Configuration
- ADS Configuration.

At phase OPERATIONAL after finalizing the configuration the Signatory is able

1. to disable the Transport Protection
2. to set his RAD for the first time
3. to modify his RAD
4. to use the signature-creation function
5. to destroy the signature key pair.

Note:

1. The Signatory is able to perform task 1, 2 and 5 only one time.

The main functionality in phase OPERATIONAL is signature creation including all supporting functionality like SCD use and modifying RAD of the Signatory.

The TOE protects the SCD during the relevant life cycle phases. Only the legitimate Signatory can use the SCD for signature creation by means of user authentication and access control. The SVD corresponding to the Signatory's SCD will be included in the certificate of the Signatory by the certificate-service provider (CSP). The life cycle ends with the life cycle phase DEATH in which the SCD is permanently blocked.

Phases MANUFACTURING, PHYSINIT and PHYSPERS comprise

A. First part of Basic Configuration (at TC) with

1. Performing acceptance procedures

2. Installation of the personalization image which includes the import of a personalization symmetric authentication key and the switch of the card to phase OPERATIONAL.

Phase OPERATIONAL comprises

B. Second part of Basic Configuration (at TC) with

3. Performing Authentication Scheme with the personalization symmetric authentication key

4. Establishing a Trusted Path

5. Switching the card temporarily to phase ADMINISTRATION

6. Optional adjustment of the internal data field length

7. Loading and activation of packages (optional)

8. Creation and configuration of Application of QES (DF_QES)

9. Import of (ADS Configuration) symmetric authentication key for the Authentication Scheme

10. Generation of the signature key pair

11. Restriction of access rights for Application of QES (DF_QES)

12. Configuration of MF

13. Finalization of MF

14. Deletion of the personalization authentication key

15. Secure delivery to the end user.

(At this point the Application for QES is deactivated)

C. ADS Configuration (at local or remote Registration Authority)

16. Performing Authentication Scheme with the (ADS Configuration) symmetric authentication key

17. Establishing the Trusted Channel

18. Switching the card temporarily to phase ADMINISTRATION

19. Exporting SVD

20. Optional creation of EFs / DFs below Application of QES (e.g. for certificates)

21. Importing of Transport PIN

22. Optional creation of EFs / DFs below MF (e.g. for additional applications)

(At this point the Application for QES is prepared for activation)

D. Disabling of Transport Protection

23. Entering of the Transport PIN by the Signatory

24. Importing of the RAD by the Signatory

(At this point the Application for QES is activated)

E. Using the signature-creation function for

25. Signing documents

F. Optional destruction of the SCD

26. Optional destruction of the SCD on demand of the Signatory

Notes:

1. The stages (A), (B) and (C) are independent and comprises specific command sequences. These sequences must not be interrupted. However, it is possible to interrupt after completion of each stage, e.g. for organizational reasons. It is recommend though to carry out stages (A) and (B) without an interrupt.
2. The symmetric key imported at step (9) is individual to the card (it depends on card number (ICCSN)).
3. The Basic Configuration comprises steps (1) up to (14).
4. The ADS Configuration comprises steps (16) up to (21). The value of the Transport PIN itself has to be a well randomized (difficult to guess) value chosen by the Registration Authority.
5. Depending on configuration the RAD of the Signatory consists of a PIN or of a PIN and a PUK, see step 23.
6. The optional EFs may be used to store certificates, e.g. the (qualified) certificate belonging to the key pair and a second certificate belonging to the Certification Authority which generates the (qualified) certificate belonging to the key pair.
7. The Registration Authority is able to perform steps 16 - 20 more than one time. That means the Registration Authority is able to create further EFs / DFs below DF_QES or it is able to update (all) created EFs / DFs below DF_QES (again) or it is able to remove (all) EFs / DFs below DF_QES.
8. The Registration Authority is not able to remove DF_QES or to create / remove objects within DF_QES or to update other objects than TPIN_QES within DF_QES.
9. After the Basic Configuration is performed completely the personalization authentication key imported during first part of the Basic Configuration is no longer needed for any tasks concerning Application for QES. It has to be deleted.
10. Step 22 is out of scope of the TOE.

4 Conformance Claims (ASE_CCL)

The TOE is a composite product, as it is based on the Infineon Security Controller SLE78CFX*P (M7892 B11), which has been evaluated and certified as being conformant to the Common Criteria version 3.1 (R4), CC Part 2 (R4) extended, and CC Part 3 (R4) conformant (cf. [BSI-DSZ-CC-0782-2012-MA-01]).

As required by [BSI-AIS36-V4], compatibility between this Composite Security Target and the Platform Security Target [Infineon-ST-Chip-B11-2013-08-13] and of the Infineon chip SLE78CFX*P (M7892 B11) is claimed. In 10.2 Usage of Platform TSF by TOE TSF a detailed mapping shows how the Platform TSF are separated into

1. relevant Platform TSF being used by the composite ST, see Table 9: Relevant Platform SFRs used by Composite ST, and
2. irrelevant Platform TSF not being used by the composite ST, see Table 10: Irrelevant Platform SFRs not being used by Composite ST.

4.1 CC Conformance Claim

This ST claims conformance to the Common Criteria version 3.1 Release 4, cf. [CC-3.1-P1], [CC-3.1-P2], and [CC-3.1-P3].

This ST claims conformance to [CC-3.1-P2] extended due to the use of FPT_EMS.1 and FIA_API.1.

This ST claims conformance to [CC-3.1-P3]; no extended assurance components have been defined.

For the evaluation the following methodology is used:

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, cf [CEM-3.1].

4.2 PP Claim, Package Claim

This Security Target claims strict conformance to the Protection Profile for Secure signature creation device - Part 2: Device with key generation, cf [BSI-CC-PP-0059-2009-MA-01].

The assurance level for the TOE is EAL4 augmented. Augmentation results from the selection of:

Assurance Class

Vulnerability assessment

Assurance components

AVA_VAN.5

Description

Advanced methodical vulnerability analysis

This ST claims the assurance package EAL4 augmented by AVA_VAN.5 as defined in [CC-3.1-P3] for product certification.

Notes:

1. The Protection Profile [BSI-CC-PP-0059-2009-MA-01] has been certified by the Bundesamt für Sicherheit in der Informationstechnik (BSI), cf [BSI-MR-CC-PP-0059-2009-MA-01].

4.3 Conformance Rationale

"Initialization" and "personalization" of the TOE as used by the PP ([BSI-CC-PP-0059-2009-MA-01]) to describe the setup of the TOE are refined in this ST to "configuration" of the TOE. These refinements are always clearly marked.

4.3.1 PP Claims Rationale

4.3.1.1 TOE Type

The PP describes the TOE type as follows (cf [BSI-CC-PP-0059-2009-MA-01] chapter "4.2 PP overview"):

- This Protection Profile describes core security requirements for a secure device that can generate a signing key (signature creation data, SCD) and operates to create electronic signatures with the generated key.
- After a SSCD has generated a signing key, the corresponding public key (signature verification data, SVD) has to be provided as input to a certificate generation application (CGA).

This ST (cf 3.3 TOE overview part (1) + (2)) describes the TOE type as follows:

- The TOE as defined by this Composite Security Target consists of the SCIC and of the Application for QES. It is to be used as a Secure Signature Creation Device (SSCD).
- The TOE allows to generate cryptographically strong signatures over previously externally or internally calculated hash values including last round hashing. The TOE generates the signature key pair (SCD/SVD). The TOE is able to protect the secrecy of the internally generated and stored Signature Creation Data (SCD, i.e. secret key) and restricts its usage to the authorized Signatory only. This restriction on usage is done via the well known PIN authentication mechanism.
- A (local) RA performs the second configuration step after the card holder applies for the Application for QES. This ADS Configuration includes exporting of the SVD, importing of the Transport PIN and optionally the creation / updating of of EFs and DFs below DF_QES. The optional EFs may be used to store certificates, e.g. the (qualified) certificate belonging to the key pair and a second certificate belonging to the Certification Authority which generates the (qualified) certificate belonging to the key pair. After this step the Application of QES is prepared for activation.

Both, the PP and this ST describe a TOE type which are able

- to generate a SCD and SVD
- to secure the SCD
- to create signatures with the SCD
- to export the SVD for generating a certificate

Conclusion:

- The TOE type of this ST is able to do the same as the TOE type of the PP
- The TOE type is consistent with the TOE type of the PP.

4.3.1.2 Security Problem Definition

The Security Problem Definition of the PP is completely taken over.

Security Problem Definition is extended by

- one user
- one asset
- two assumptions
- one security attribute type
- two security objectives for the operation environment

and a threat of the PP is extended by an attack against the new asset.

The new asset is:

> **Symmetric key data for the Authentication Scheme: used for mutual authentication of TOE and (local or remote) Registration Authority (RA-Terminal).**

The new security attribute type is:

> **SM-Connection** which can be associated to S.User with the values
>
> **established** or **not established**.

Security attribute type "SM-Connection" states whether a Trusted Channel is established or not using means of encryption/decryption and MAC keys.

4.3.1.2.1 Users and subject acting for users

The IT-Entity RA-Terminal is added to this ST:

> **RA-Terminal: Local or remote IT entity (trusted IT product) which is used to perform the administrative functions such as the transfer of public key data, optional creation of EFs / DFs and import of the Transport PIN via a Trusted Channel as performed in a local RA. In the TOE the subject S.RA-Terminal is acting in the role R.RA-Terminal for this user after successful authentication as RA-Terminal.**

This user reflects that this TOE is configured in more than one step:

1. The Basic Configuration is performed by an Administrator and the ADS Configuration is performed by an RA-Terminal.
2. After the Basic Configuration is performed the Application for QES is deactivated and the card is issued to the card holder.
3. If the card holder applies for Application for QES, the ADS Configuration is performed by the RA-Terminal and the Signatory creates afterward his RAD.

- The tasks performed during ADS Configuration by an RA-Terminal are not foreseen by the PP.
- In this TOE the Signatory creates his RAD. The PP states that the Administrator creates the RAD of the Signatory which requires a hand over of the RAD.

Conclusion

- Concerning creation of Signatory RAD this TOE is more secure.
- The users in this ST are a super set of the users in the PP.
- This ST are consistent with the statement of the PP.

4.3.1.2.2 Threats

The threat T.Hack_Phys (Physical attacks through the TOE interfaces)

> An attacker interacts physically with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD and DTBS.

is extended by an attack against the new asset "symmetric key data for the Authentication Scheme"

> An attacker interacts physically with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD and DTBS **and symmetric key data for the Authentication Scheme**.

The new asset "symmetric key data for the Authentication Scheme" is not linked to the other assets "SCD, SVD and DTBS".

Conclusion:

- Any attack against "SCD, SVD and DTBS" does not concern the "symmetric key data for the Authentication Scheme" and vice versa the attack against "symmetric key data for the Authentication Scheme" does not concern "SCD, SVD and DTBS".
- The threats in this ST is a super set of the threats in the PP.
- The threats in this ST are consistent with the Security Problem Definition in the PP.

4.3.1.2.3 Organizational security policies

The Organizational Security Policies of this TOE are identically to PP's OSPs.

4.3.1.2.4 Assumptions

The assumptions

A.Env_Admin (Environment for administrator)

> **Authentication of and configuration by the Administrator only takes place within a trusted environment**.

A.Env_RA (RA as a trusted environment)

> **Transfer of public key data, optional creation of EFs / DFs including updating them and import of the Transport PIN via a Trusted Channel are performed by the RA as a trusted environment.**

are added to to the assumptions defined in the PP.

These assumptions do not

1. mitigate a threat (or a part of a threat) meant to be addressed by security objectives for the TOE in the PP because the data, TOE interfaces or signature-creation function which are attacked by
   a) T.SCD_Divulg (Storing, copying, and releasing of the signature creation data)
   b) T.SCD_Derive (Derive the signature creation data)
   c) T.Hack_Phys (Physical attacks through the TOE interfaces)
   d) T.SVD_Forgery (Forgery of the signature-verification data)
   e) T.SigF_Misuse (Misuse of the signature-creation function of the TOE)
   f) T.DTBS_Forgery (Forgery of the DTBS/R)
   g) T.Sig_Forgery (Forgery of the digital signature)
   are created, stored, configured or transferred in the same way whether the authentication of and configuration by the Administrator or by the RA take place within a trusted environment or not.
2. fulfill an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the PP because the organizations (and applications used by them), the signature creation system, the requirements for an SSCD laid down in Annex III and the usage by the Signatory enforced by the SSCD itself which are described by
   a) P.CSP_QCert (Qualified certificate)
   b) P.QSign (Qualified electronic signatures)
   c) P.Sigy_SSCD (TOE as secure signature creation device)
   d) P.Sig_Non-Repud (Non-repudiation of signatures)
   are not affected, less, modified or the configuration is changed whether the authentication of and configuration by the Administrator or by the RA take place within a trusted environment or not.

Conclusion:

- The assumptions in this ST do not change the statement made by the assumptions in the PP.
- The assumptions in this ST are a super set of the assumptions in the PP.
- The assumptions in this ST are consistent with the assumptions in the PP.

4.3.1.2.5 Conclusion

- The Security Problem Definition in this ST does not change the statement made by the Security Problem Definition in the PP.
- The Security Problem Definition in this ST is a super set of Security Problem Definition in the PP.
- The Security Problem Definition is consistent with the Security Problem Definition in the PP.

4.3.1.3 Security Objectives for the Operation Environment

The security objectives for the operational environment

OE.Env_Admin (Administrator works in trusted environment)

> **The administrative functions of "Administrator" users are performed within a trusted environment**.

OE.Env_RA (RA as a trusted environment)

> **The administrative functions transfer of public key data, optional creation of EFs / DFs including updating them and import of the Transport PIN via a Trusted Channel performed by, or using, "RA-Terminal" users are performed as a trusted environment.**

are added to the objectives defined in the PP.

These security objectives do not

1. mitigate a threat (or a part of a threat) meant to be addressed by security objectives for the TOE in the PP because the data, TOE interfaces or signature-creation function which are attacked by
   a) T.SCD_Divulg (Storing, copying, and releasing of the signature creation data)
   b) T.SCD_Derive (Derive the signature creation data)
   c) T.Hack_Phys (Physical attacks through the TOE interfaces)
   d) T.SVD_Forgery (Forgery of the signature-verification data)
   e) T.SigF_Misuse (Misuse of the signature-creation function of the TOE)
   f) T.DTBS_Forgery (Forgery of the DTBS/R)
   g) T.Sig_Forgery (Forgery of the digital signature)
   are created, stored, configured or transferred in the same way whether the administrative functions of "Administrator" or of "RA" users are performed within a trusted environment or not.
2. fulfill an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the PP because the organizations (and applications used by them), the signature creation system, the requirements for an SSCD laid down in Annex III and the usage by the Signatory enforced by the SSCD itself which are described by
   a) P.CSP_QCert (Qualified certificate)
   b) P.QSign (Qualified electronic signatures)
   c) P.Sigy_SSCD (TOE as secure signature creation device)
   d) P.Sig_Non-Repud (Non-repudiation of signatures)
   are not affected, less, modified or the configuration is changed whether the administrative functions of "Administrator" or of "RA" users are performed within a trusted environment or not.

Conclusion:

- The Security objectives in this ST do not change the statement made by the Security Objectives for the TOE in the PP.
- The Security Objectives in this ST are a super set of the Security Objectives in the PP.
- The Security Objectives in this ST are consistent with the Security Objectives for the TOE in the PP.

4.3.1.4 Security Requirements

Not all configurations of this TOE are valid, see 8.2.3 Configurations. These configurations do not influence this section because the SRFs of the PP and the SFRs added to the contents of PP are considered is this section.

4.3.1.4.1 SFRs of the PP

All SFRs in the PP are taken over and the application notes are considered. The following SFRs are extended by appending a slash with informative data for mnemonic reasons:

SFR in the PP	SFR in this ST
FCS_CKM.1	FCS_CKM.1/EC
FCS_COP.1	FCS_COP.1/EC
FIA_AFL.1	FIA_AFL.1/FixedLenPINRC

The informative data of SFR "FMT_MTD.1/Admin" after the slash is replaced by "RAD" to FMT_MTD.1/RAD for mnemonic reason because this SFR is refined. In this ST the PIN is created by the Signatory instead of the Administrator.

These SFRs are clearly marked with a note, e.g.

> FCS_CKM.1/EC amounts to requirement "FCS_CKM.1" with the selection of ECC key generation.

Note:

1. "RAD" is chosen because a SFR with the informative data "Signatory" after the slash is already defined by the PP, cf FMT_MTD.1/Signatory.

The data persistently stored by the TOE is extended by adding the new asset symmetric key data for the Authentication Scheme.

- This changes only the quantity not the quality of SFR FDP_SDI.2/Persistent.

SFR FDP_ACF.1/SVD_Transfer_SFP is extended by the new SFP-relevant security attribute "SM-Connection" which associates user S.User with the security attribute "SM-Connection"

- This SFP-relevant security attribute depends on whether a Trusted Channel is established or not.
- This SFP-relevant security attribute makes the SFR more restrictive.

SFR FDP_RIP.1 is extended by adding the new asset "Symmetric key data for Authentication Scheme"

- The new asset is not linked to the other asset of FDP_RIP.1.
- This new asset changes only the quantity of previous information content of a resource to make unavailable upon the de-allocation of the resource not the quality of this SFR.

Conclusion:

- The added informative data to the SRFs in the ST does not change the statement of SFRs in the PP.
- The added data persistently stored by the TOE does not change the intend of the statement of SFRs in the PP only the set of data is greater.
- The added asset used by the TOE for the Authentication Scheme does not change the intend of the statement of SFRs in the PP only the set of data is greater.
- The added SFP-relevant security attribute by the TOE makes the statement of SFRs in the PP more restrictive.
- The statement of SFRs in the ST is consistent with the statement of SFRs in the PP.

4.3.1.4.2 SFRs added to content of the PP

Note:

1. If a security functional requirement is added to contents of PP [BSI-CC-PP-0059-2009-MA-01], this is described by a note which also states whether the SFR is "iterated" or "not iterated" from a PP SFR.

The following SFRs are added to this ST:

FCS_COP.1/SHA-2 (adds SHA-2 to this ST, not iterated)

FCS_CKM.1/AuthScheme (adds generation of session keys to this ST, not iterated)

FCS_CKM.4/AuthScheme (adds destroying of session keys to this ST, iterated)

FCS_CKM.1/RSA (adds generation of RSA to this ST, iterated)

FCS_COP.1/RSA (adds RSA signature generation to this ST, iterated)

FCS_COP.1/3DES-ENC (adds encrypting of commands to this ST, not iterated)

FCS_COP.1/3DES-MAC (adds MACing of commands to this ST, not iterated)

FCS_COP.1/AES-ENC (encrypting and decrypting of the commands, not iterated)

FCS_COP.1/AES-MAC (MACing of the commands, not iterated)

FDP_ACC.1/Config_DF_QES (adds additional tasks of the RA to this ST, not iterated)

FDP_ACF.1/Config_DF_QES (adds additional tasks of the RA to this ST, not iterated)

FTP_ITC.1/SM_ADS_Conf (adds a Trusted Channel to this ST, not iterated)

FIA_AFL.1/VarLenPINRC (adds failure handling of PIN with variable RC to this ST, iterated)

FIA_AFL.1/PUK (adds failure handling of PUK to this ST, iterated)

FIA_AFL.1/T-PIN (adds failure handling of the Transport PIN to this ST, iterated)

FIA_AFL.1/AuthAdmin (adds failure handling of the Admin at phase OPERATIONAL to this ST, not iterated)

FIA_AFL.1/SM (adds failure handling of an established Trusted Channel to this ST, not iterated)

FIA_API.1/AuthScheme (adds Proof of Identity of the TOE to this ST, not iterated)

FMT_MSA.1/RA-Terminal (adds restriction of the new security attribute "SM-Connection" to this ST, not iterated)

FMT_MTD.1/Ini-Data (adds restriction of the initial data to this ST, not iterated)

Note:

1. The new security attribute "SM-Connection" describes whether the Trusted Channel is established or not.

These SFRs introduce functionality to this ST which

- is not foreseen in the PP and therefore
- does not affect the functionality as described by the statement of SFRs of the PP.

Conclusion:

- The SRFs added to content of the PP in the ST do not change the statement of SFRs in the PP.
- The statement of SFRs in the ST is consistent with the statement of SFRs in the PP.

4.3.1.4.3 Conclusion

- The added informative data to the SRFs in this ST does not change the statement made by the Security Requirements in the PP.
- The SRFs added to content of the PP in the ST do not change the statement of SFRs in the PP.
- The Security Requirements in this ST is a super set of the Security Requirements in the PP.
- The Security Requirements in this ST are consistent with the statement of Security Requirements in the PP.

5 Security Problem Definition (ASE_SPD)

5.1 Assets, users and threat agents

The Common Criteria define assets as entities that the owner of the TOE presumably places value upon. The term "asset" is used to describe the threats in the operational environment of the TOE.

5.1.1 Assets and objects

1. SCD: private key used to perform a digital signature operation. The confidentiality, integrity and signatory's sole control over the use of the SCD must be maintained.
2. SVD: public key linked to the SCD and used to perform digital signature verification. The integrity of the SVD when it is exported must be maintained.
3. DTBS and DTBS/R: set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the digital signature must be maintained.
4. **Symmetric key data for the Authentication Scheme: used for mutual authentication of TOE and (local or remote) Registration Authority (RA-Terminal)**.

Notes:

1. "Symmetric key data for the Authentication Scheme: ..." is added to the contents of [BSI-CC-PP-0059-2009-MA-01].
2. Symmetric key data are individual to the card (depends on ICCSN).
3. As a additional result of the Authentication Scheme the Trust Center and the card share a secret which is used to set up a Trusted Channel by deriving session keys.

5.1.2 User and subjects acting for users

1. User:
   a) End user **who is a human user** of the TOE who can be identified as Administrator or Signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.
   b) **who is an IT entity and can be identified as "RA-Terminal". In the TOE the subject S.User may act as S.RA-Terminal in the role R.RA-Terminal**.
2. Administrator: User who is in charge to perform the TOE **configuration** or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as Administrator.
3. 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. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as Signatory.
4. **RA-Terminal: Local or remote IT entity (trusted IT product) which is used to perform the administrative functions such as transfer of public key data, optional creation of EFs / DFs and import of the Transport PIN via a Trusted Channel as performed in a local RA. In the TOE the subject S.RA-Terminal is acting in the role R.RA-Terminal for this user after successful authentication as RA-Terminal.**

Note:

1. "configuration" is a [REFINEMENT] of "initialisation, TOE personalisation".
2. For (1.a): "who is a human user" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01].
3. (1.b) is added to contents of PP [BSI-CC-PP-0059-2009-MA-01].
4. (4) is added to contents of PP [BSI-CC-PP-0059-2009-MA-01].

5.1.3 Threat agents

1. Attacker: Human or process acting on their behalf outside the TOE. The main goal of the attacker is to access the SCD or to falsify the digital signature. An attacker has got a high attack potential and knows no secret.

5.2 Threats

5.2.1 T.SCD_Divulg (Storing, copying, and releasing of the signature creation data)

An attacker stores or copies the SCD outside the TOE. An attacker can obtain the SCD during generation, storage and use for signature creation in the TOE.

5.2.2 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 exported outside the TOE, which is a threat against the secrecy of the SCD.

5.2.3 T.Hack_Phys (Physical attacks through the TOE interfaces)

An attacker interacts physically with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD and DTBS **and symmetric key data for the Authentication Scheme**.

Note:

1. "Symmetric key data for the Authentication Scheme" is added to the contents of [BSI-CC-PP-0059-2009-MA-01].

5.2.4 T.SVD_Forgery (Forgery of the signature-verification data)

An attacker presents a forged SVD to the CGA. This results in loss of SVD integrity in the certificate of the signatory.

5.2.5 T.SigF_Misuse (Misuse of the signature-creation function of the TOE)

An attacker misuses the signature-creation function of the TOE to create a digital signature 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.

5.2.6 T.DTBS_Forgery (Forgery of the DTBS/R)

An attacker modifies the DTBS/R sent by the SCA. Thus the DTBS/R used by the TOE for signing does not match the DTBS the signatory alone intended to sign.

5.2.7 T.Sig_Forgery (Forgery of the digital signature)

Without use of the SCD an attacker forges data with associated digital signature and the verification of the digital signature by the SVD does not detect the forgery. 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.

5.3 Organizational Security Policies

5.3.1 P.CSP_QCert (Qualified certificate)

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. the directive, article 2, clause 9, and Annex I) for the SVD generated by the SSCD. The certificates contain at least

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 as SSCD is evident with signatures through the certificate or other publicly available information.

5.3.2 P.QSign (Qualified electronic signatures)

The signatory uses a signature creation system to sign data with an advanced electronic signature (cf. the directive, article 1, clause 2), which is a qualified electronic signature if it is based on a valid qualified certificate (according to the directive Annex I) [2]. The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature created with a SCD implemented in the SSCD that the signatory maintain under their sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

5.3.3 P.Sigy_SSCD (TOE as secure signature creation device)

The TOE meets the requirements for an SSCD laid down in Annex III of the directive [DIR-EP-1993]. This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once.

5.3.4 P.Sig_Non-Repud (Non-repudiation of signatures)

The life cycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate.

5.4 Assumptions

5.4.1 A.CGA (Trustworthy certification-generation application)

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

5.4.2 A.SCA (Trustworthy signature-creation application)

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

5.4.3 A.Env_Admin (Environment for administrator)

Authentication of and configuration by the Administrator only takes place within a trusted environment.

Note: "A.Env_Admin" is added to the contents of [BSI-CC-PP-0059-2009-MA-01].

5.4.4 A.Env_RA (RA as a trusted environment)

Transfer of public key data, optional creation of EFs / DFs including updating them and import of the Transport PIN via a Trusted Channel are performed by the RA as trusted environment.

Note: "A.Env_RA" is added to the contents of [BSI-CC-PP-0059-2009-MA-01].

2 It is a non-qualified advanced electronic signature if it is based on a non-qualified certificate for the SVD.

6 Security Objectives (ASE_OBJ)

6.1 General

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 organizational security policies and assumptions.

6.2 Security Objectives for the TOE

6.2.1 OT.Lifecycle_Security (Lifecycle security)

The TOE shall detect flaws during the **configuration** and operational usage. The TOE shall securely destroy the SCD on demand of the signatory.

Application note 1: The TOE may contain more than one set of SCD. There is no need to destroy the SCD in case of repeated SCD generation. The signatory shall be able to destroy the SCD stored in the SSCD e.g. after the (qualified) certificate for the corresponding SVD has been expired.

Note:

1. "configuration" is a [REFINEMENT] of "initialization, personalization".
2. This TOE contains only one SCD (RSA or EC based).

6.2.2 OT.SCD/SVD_Auth_Gen (Authorized SCD/SVD generation)

The TOE shall provide security features to ensure that authorized users only may invoke the generation of the SCD and the SVD.

6.2.3 OT.SCD_Unique (Uniqueness of the signature creation data)

The TOE shall ensure the cryptographic quality of an SCD/SVD pair it creates as suitable for the advanced or qualified electronic signature. The SCD used for signature creation 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.

6.2.4 OT.SCD_SVD_Corresp (Correspondence between SVD and SCD)

The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE. This includes unambiguous reference of a created SVD/SCD pair for export of the SVD and in creating a digital signature creation with the SCD.

6.2.5 OT.SCD_Secrecy (Secrecy of the signature creation data)

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

Application note 2: The TOE shall keep the confidentiality of the SCD at all times, in particular during SCD/SVD generation, signature creation operation, storage and secure destruction.

CardOS V5.3 provides no means for exporting the SCD. During generation, signature creation operation, storage and secure destruction the SCD is secured by means of the chip design.

6.2.6 OT.Sig_Secure (Cryptographic security of the digital signature)

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

6.2.7 OT.Sigy_SigF (Signature-creation function for the legitimate signatory only)

The TOE provides the digital signature-creation function for the legitimate signatory only and protects the SCD against the use of others to create a digital signature. The TOE shall resist attacks with high attack potential.

6.2.8 OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE)

The TOE must not alter the DTBS/R. As by definition of the DTBS/R this may consist of the DTBS themselves, this objective does not conflict with a signature creation process where the TOE hashes the provided DTBS (in part or entirely) for signature creation.

6.2.9 OT.EMSEC_Design (Provide physical-emanation security)

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

Note:

1. This security objective holds also for new asset "Symmetric key data for the Authentication Scheme".

6.2.10 OT.Tamper_ID (Tamper detection)

The TOE provides system features that detect physical tampering of its components and uses those features to limit security breaches.

6.2.11 OT.Tamper_Resistance (Tamper resistance)

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

6.3 Security Objectives for the Operational Environment

6.3.1 OE.SVD_Auth (Authenticity of the SVD)

The operational environment shall ensure the integrity of the SVD sent to the CGA of the CSP. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

6.3.2 OE.CGA_QCert (Generation of qualified certificates)

The CGA shall generate a qualified certificate that includes (amongst others)

a) the name of the signatory controlling the TOE,
b) the SVD matching the SCD stored in the TOE and being under sole control of the signatory,
c) the advanced signature of the CSP.

The CGA shall confirm with the generated qualified certificate that the SCD corresponding to the SVD is stored in a SSCD.

6.3.3 OE.SSCD_Prov_Service (Authentic SSCD provided by SSCD provisioning service)

The SSCD-provisioning service shall **configure** for the signatory an authentic copy of the TOE and deliver this copy as SSCD to the signatory.

Note:

1. "configure" is a [REFINEMENT] of "initialize and personalize".

6.3.4 OE.HID_VAD (Protection of the VAD)

If an external device provides the human interface for user authentication, this device shall ensure confidentiality and integrity of the VAD as needed by the authentication method employed from import through its human interface until import through the TOE interface. In particular, if the TOE requires a trusted channel for import of the VAD, the HID shall support usage of this trusted channel.

6.3.5 OE.DTBS_Intend (SCA sends data intended to be signed)

The signatory shall use a trustworthy SCA that

- generates the DTBS/R 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,
- sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE,
- attaches the signature produced by the TOE to the data or provides it separately.

Application note 3: The SCA should be able to support advanced electronic signatures. Currently, there exist three formats defined by ETSI recognized as meeting the requirements needed by advanced electronic signatures: CAdES, XAdES and PAdES. These three formats mandate to include the hash of the signer's public key certificate in the data to be signed. In order to support for the mobility of the signer, it is recommended to store the certificate info on the SSCD for use by SCA and identification of the corresponding SCD if more than one SCD is stored on the SSCD.

This TOE does not support CAdES, XAdES and PAdES. This TOE uses only one SCD.

6.3.6 OE.DTBS_Protect (SCA protects the data intended to be signed)

The operational environment shall ensure that the DTBS/R cannot be altered in transit between the SCA and the TOE. In particular, if the TOE requires a trusted channel for import of the DTBS/R, the SCA shall support usage of this trusted channel.

6.3.7 OE.Signatory (Security obligation of the signatory)

The signatory shall check that the SCD stored in the SSCD received from SSCD-provisioning service is in non-operational state. The signatory shall keep their VAD confidential.

6.3.8 OE.Env_Admin (Administrator works in trusted environment)

The administrative functions of "Administrator" users are performed within a trusted environment.

Note: "OE.Env_Admin" is added to the contents of [BSI-CC-PP-0059-2009-MA-01].

6.3.9 OE.Env_RA (RA as a trusted environment)

The administrative functions transfer of public key data, optional creation of EFs / DFs including updating them and import of the Transport PIN via a Trusted Channel performed by, or using, "RA-Terminal" users are performed as a trusted environment.

Note: "OE.Env_RA" is added to the contents of [BSI-CC-PP-0059-2009-MA-01].

6.4 Security Objectives Rationale

6.4.1 Security Objectives Coverage

Table 2: Security problem definition to security objectives mapping

	OT.lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OE.CGA_QCert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.DTBS_Intend	OE.HID_VAD	OE.Signatory	OE.DTBS_Protect	OE.ENV_Admin	OE.ENV_RA
T.SCD_Divulg					x															
T.SCD_Derive		x				x														
T.Hack_Phys					x				x	x	x									
T.SVD_Forgery				x									x							
T.SigF_Misuse	x						x	x							x	x	x	x		
T.DTBS_Forgery								x							x			x		
T.Sig_Forgery			x			x						x								
P.CSP_QCert	x			x								x								
P.QSign						x	x					x			x					
P.Sigy_SSCD	x	x	x		x	x	x	x	x		x			x						
P.Sig_Non-Repud	x		x	x	x	x	x	x	x	x	x	x	x	x	x		x	x		
A.CGA												x	x							
A.SCA															x					
A.Env_Admin																			x	

A.Env_RA																			x

6.4.2 Security Objectives Sufficiency

6.4.2.1 Countering of threats by security objectives

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 recital (18) of the directive. This threat is countered by OT.SCD_Secrecy, which assures the secrecy of the SCD used for signature creation.

T.SCD_Derive (*Derive the signature creation data*)

deals with attacks on the SCD via public known data produced by the TOE, which are the SVD and the signatures created with the SCD. OT.SCD/SVD_Auth_Gen counters this threat by implementing cryptographically secure generation of the SCD/SVD pair. OT.Sig_Secure ensures cryptographically secure electronic signatures.

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. OT.EMSEC_Design counters physical attacks through the TOE interfaces and observation of TOE emanations. OT.Tamper_ID and OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tampering attacks.

T.SVD_Forgery (*Forgery of the signature verification data*)

deals with the forgery of the SVD exported by the TOE to the CGA for certificate generation. T.SVD_Forgery is addressed by OT.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and OE.SVD_Auth that ensures the integrity of the SVD exported by the TOE to the CGA.

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 an electronic signature on data for which the signatory has not expressed the intent to sign, as required by paragraph 1(c) of Annex III. OT.Lifecycle_Security (Lifecycle security) requires the TOE to detect flaws during the **configuration** and operational usage including secure destruction of the SCD, which may be initiated by the signatory. OT.Sigy_SigF (Signature creation function for the legitimate signatory only) ensures that the TOE provides the signature creation function for the legitimate signatory only. OE.DTBS_Intend (Data intended to be signed) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign and OE.DTBS_Protect counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE. OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. If the SCA provides a human interface for user authentication, OE.HID_VAD (Protection of the VAD) provides confidentiality and integrity of the VAD as needed by the authentication method employed. OE.Signatory ensures that the signatory checks that an SCD stored in the SSCD when received from an SSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the signatory becomes control over the SSCD. OE.Signatory ensures also that the signatory keeps their VAD confidential.

Note:

1. "configuration" is a [REFINEMENT] of "initialization, personalization".

T.DTBS_Forgery (*Forgery of the DTBS/R*)

addresses the threat arising from modifications of the data sent as input to the TOE's signature creation

function that does not represent the DTBS as presented to the signatory and for which the signature has expressed its intent to sign. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.DTBS_Intend, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE, and by means of OE.DTBS_Protect, which ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE. The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by ensuring the integrity of the DTBS/R inside the TOE.

T.Sig_Forgery (*Forgery of the electronic signature*)

deals with non-detectable forgery of the electronic signature. OT.Sig_Secure, OT.SCD_Unique and OE.CGA_QCert address this threat in general. OT.Sig_Secure (Cryptographic security of the electronic signature) ensures by means of robust cryptographic techniques that the signed data and the electronic signature are securely linked together. OT.SCD_Unique and ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance. OE.CGA_QCert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision concerning a forged signature.

6.4.2.2 Enforcement of OSPs by security objectives

P.CSP_QCert (*CSP generates qualified certificates*)

establishes the CSP generating qualified certificate or non-qualified certificate linking the signatory and the SVD implemented in the SSCD under sole control of this signatory. P.CSP_QCert is addressed by

- OT.Lifecycle_Security, which requires the TOE to detect flaws during the **configuration** and operational usage,
- OT.SCD_SVD_Corresp, which requires to ensure the correspondence between the SVD and the SCD during their generation,
- OE.CGA_QCert for generation of qualified certificates or non-qualified certificates, which requires the CGA to certify the SVD matching the SCD implemented in the TOE under sole control of the signatory.

Note:

1. "configuration" is a [REFINEMENT] of "initialization, personalization".

P.QSign (*Qualified electronic signatures*)

provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate. OT.Sigy_SigF ensures signatory's sole control of the SCD by requiring the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others. OT.Sig_Secure ensures that the TOE creates electronic signatures, which cannot be forged without knowledge of the SCD through robust encryption techniques. OE.CGA_QCert addresses the requirement of qualified or non-qualified electronic certificates building a base for the electronic signature. OE.DTBS_Intend ensures that the SCA provides only those DTBS to the TOE, which the signatory intends to sign.

P.Sigy_SSCD (*TOE as secure signature creation device*)

requires the TOE to meet Annex III. This is ensured as follows:

- OT.SCD_Unique meets the paragraph 1(a) of Annex III, by the requirements that the SCD used for signature creation can practically occur only once;
- OT.SCD_Unique, OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(a) of Annex III by the requirements to ensure secrecy of the SCD. OT.EMSEC_Design and OT.Tamper_Resistance address specific objectives to ensure secrecy of the SCD against specific attacks;
- OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(b) of Annex III by the requirements to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE;
- OT.Sigy_SigF meets the requirement in paragraph 1(c) of Annex III by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others;

- OT.DTBS_Integrity_TOE meets the requirements in paragraph 2 of Annex III as the TOE must not alter the DTBS/R.

Paragraph 2 of Annex III, requires that an SSCD does not prevent the data to be signed from being presented to the signatory prior to the signature process is obviously fulfilled by the method of TOE usage: the SCA will present the DTBS to the signatory and send it to the SSCD for signing. The usage of SCD under sole control of the signatory is ensured by

- OT.Lifecycle_Security requiring the TOE to detect flaws during the **configuration** and operational usage,
- OT.SCD/SVD_Auth_Gen, which limits invocation of the generation of the SCD and the SVD to authorized users only, and
- OT.Sigy_SigF, which requires the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others.

OE.SSCD_Prov_Service ensures that the signatory obtains an authentic copy of the TOE, **configured** SSCD from an SSCD-provisioning service.

Note:

1. "configuration" is a [REFINEMENT] of "initialization, personalization".
2. "configured" is a [REFINEMENT] of "initialized and personalized".

P.Sig_Non-Repud (*Non-repudiation of signatures*)

deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in their certificate valid at the time of signature creation. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, which ensures the aspects of signatory's sole control over and responsibility for the electronic signatures created with the TOE.

OE.SSCD_Prov_Service ensures that the signatory obtains an authentic copy of the TOE, **configured** as SSCD from the SSCD-provisioning service.

OE.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. OE.SVD_Auth and OE.CGA_QCert require the environment to ensure authenticity of the SVD as being exported by the TOE and used under sole control of the signatory. OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE. OT.SCD_Unique provides that the signatory's SCD can practically occur just once.

OE.Signatory ensures that the signatory checks that the SCD, stored in the SSCD received from an SSCDprovisioning service is in non-operational state (i.e. the SCD cannot be used before the signatory becomes into sole control over the SSCD). OT.Sigy_SigF provides that only the signatory may use the TOE for signature creation. As prerequisite OE.Signatory ensures that the signatory keeps their VAD confidential. OE.DTBS_Intend, OE.DTBS_Protect and OT.DTBS_Integrity_TOE ensure that the TOE creates electronic signatures only for those DTBS/R, which the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig_Secure ensure that only this SCD may create a valid electronic signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE OT.Lifecycle_Security (*Lifecycle security*), OT.SCD_Secrecy (*Secrecy of the signature creation data*), OT.EMSEC_Design (*Provide physical emanations security*), OT.Tamper_ID (*Tamper detection*) and OT.Tamper_Resistance (*Tamper resistance*) protect the SCD against any compromise.

Note:

1. "configured" is a [REFINEMENT] of "initialized and personalized".

6.4.2.3 Upkeep of assumptions by security objectives

A.SCA (*Trustworthy signature creation application*)

establishes the trustworthiness of the SCA with respect to generation of DTBS/R. This is addressed by OE.DTBS_Intend (Data intended to be signed) which ensures that the SCA generates the DTBS/R of the data that have 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 certificate 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 (Authenticity of the SVD), which ensures the protection of the integrity of the received SVD and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

A.Env_Admin (*Environment for Administrator*)

establishes a trustworthy environment for the Administrator for setting up the configuration of the TOE after the Administrator is successfully authenticated. This is addressed by OE.Env_Admin (Administrator works in trusted environment) which ensures that authentication and configuration are only started by the Administrator within a trusted environment.

Note:

1. "A.Env_Admin" and "OE.Env_Admin" are added to the contents of [BSI-CC-PP-0059-2009-MA-01].

A.Env_RA (RA as a trusted environment)

establishes a trustworthy environment for transferring of public key data, optional creating of EFs / DFs including updating them and importing of the Transport PIN via a Trusted Channel, This is addressed by OE.Env_RA (RA as a trusted environment) which ensures that the administrative functions transfer of public key data, optional creation of EFs / DFs including updating them and import of the Transport PIN via a Trusted Channel performed by, or using, "RA-Terminal" users are performed as a trusted environment.

Note: "A.Env_RA" and "OE.Env_RA" are added to the contents of [BSI-CC-PP-0059-2009-MA-01].

7 Extended Component Definition (ASE_ECD)

7.1 Definition of the Family FPT_EMS

Note:

1. [5] references to "Protection Profile Secure Signature Creation Device Type 3, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0006-2002, also short SSCD-PP or CWA14169".

The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc.

This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation. The definition of the family FPT_EMS is taken from the Protection Profile Secure Signature Creation Device [5].

FPT_EMS TOE Emanation

Family behaviour:

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMS TOE Emanation	1

FPT_EMS.1 TOE Emanation has two constituents:

- FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
- FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions identified that shall be auditable if **FAU_GEN** (Security audit data generation) is included in a PP or ST using FPT_EMS.1.

7.1.1 FPT_EMS.1 *TOE Emanation*

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1

The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

FPT_EMS.1.2

The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

7.2 Definition of the Family FIA_API

Notes:

1. This chapter is a complete and unchanged copy of chapter "8.2 Definition of the family FIA_API" of PP [BSI-CC-PP-0071].
2. PP [BSI-CC-PP-0071] is certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) cf [BSI-CC-PP-0071-2012].
3. Definition of the Family FIA_API is added to contents of PP [BSI-CC-PP-0059-2009-MA-01].

To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

FIA_API Authentication Proof of Identity

Family behaviour

This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.

Component levelling:

FIA_API Authentication Proof of Identity	1

FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1

The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: authorized user or role].

8 IT Security Requirements (ASE_REQ)

8.1 General

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

Section 'Extended Component Definition' describes the definition of the Family FPT_EMS and the definition of the Family FIA_API. Section 'TOE Security Functional Requirements' provides the security functional requirements.

Operations not performed in Protection Profile [BSI-CC-PP-0059-2009-MA-01] are performed.

The TOE security assurance requirements statement is given in 'TOE Security Assurance Requirements' of this chapter.

8.2 TOE Security Functional Requirements

8.2.1 Use of requirement specifications

Common Criteria allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph 8.1 of part 1 of [CC-3.1-P1]. Each of these operations is used in [BSI-CC-PP-0059-2009-MA-01].

This Security Target performs the missing operations and considers the Application Notes given in [BSI-CC-PP-0059-2009-MA-01].

The following conventions have been applied to the set of operations that may be applied to functional requirements:

- selections are indicated by bold text and by footnotes which lists the deleted text,
- assignmenst are indicated by bold text and by footnotes which lists the deleted text,
- iterations are indicated by appending a slash with informative data following the component title (for example "/SHA-2") and
- refinements are indicated by bold text and by footnotes which identifies the refined text or by bold text and a leading [REFINEMENT] and in case of a longer section with a closing [END REFINEMENT].

If a security functional requirement is added to contents of PP [BSI-CC-PP-0059-2009-MA-01], this is described by a note which also states whether the SFR is "iterated" or "not iterated" from a PP SFR.

8.2.2 Table of cryptographic mechanisms used

This TOE is a composite product and uses for cryptographic mechanism listed in number 5 - 12 only mechanism provided by the underlying chip SLE78CFX*P (M7892 B11). The "Standard of Implementation" is a citation of the ST of the underlying chip SLE78CFX*P (M7892 B11) only, cf. [Infineon-ST-Chip-B11-2013-08-13].

The "Standard of Application" is

- in case of configurations applying for a Austrian Confirmation (SigG / SigV) [SigV-QES-Austria] chapter "Anhang"
- in case of configurations applying for a German Confirmation (SigG / SigV) [Geeignete-Algorithmen]

Table 3: Cryptographic mechanisms used

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits
1	Key Agreement	Symmetric Authentication Scheme	CWA-14890-1, chapter 8.7 + 8.8 improved by SHA-256	
		using TDES	see No. 5	168
		and Retail-MAC	see No. 7	
		and SHA-256	see No. 2	
		or using AES	see No. 6	128
		and CMAC	see No. 8	
		and SHA-256	see No. 2	
2	Cryptographic Primitive (see note 6)	SHA-{256, 384, 512}	NIST-FIPS-PUB-180-4 chapters 6.2, 6.4, 6.5	none
3	Authentication (see note 7)	Symmetric Authentication		
		using TDES	see No. 5	168
		and Challenge		64
4	Authentication (see note 7)	Symmetric Authentication		
		using AES	see No. 6	128
		and Challenge		64
5	Confidentiality (see note 1)	TDES	NIST, NIST Special Publication 800-67 Version 1.1	168
		in CBC mode	[NIST-800-38A-2001]	
6	Confidentiality (see note 8)	AES	FIPS PUB 197	128, 192 and 256
		in CBC mode	[NIST-800-38A-2001]	

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits
7	Integrity (see note 1)	TDES	NIST, NIST Special Publication 800-67 Version 1.1	168
		and Retail-MAC	[ISO-IEC-9797-1-2011]	
8	Integrity (see note 8)	AES	FIPS PUB 197	128, 192 and 256
		and CMAC	[ISO-IEC-9797-1-2011]	
9	Authenticity (see note 2)	RSA signature generation	PKCS1 v2.1 RFC3447, section 5.2.1 RSASP1	modulus length= 2048 - 4096
		padding with RSASSA-PSS and RSASSA-PKCS1 -v1_5		
		using SHA-{256,384,512}	see No. 2	
10	Key Generation (see note 3)	RSA key generation using "rsagen1"	PKCS1 v2.1 RFC3447, section 3.2(2)	modulus length= 2048 - 4096
11	Authenticity (see note 4)	ECDSA	ANSI X9.62 - 2005 section 7.3 and ISO/IEC 15946-2:2002 6.2.2. + 6.2.3	
		using curve "curve P-256" with SHA-256	NIST-FIPS-PUB-186-4 D.2.3 "Curve P-256"	256
		using curve "curve P-384" with SHA-384	NIST-FIPS-PUB-186-4 D.2.4 "Curve P-384"	384
		using brainpoolP256r1 with SHA-256	RFC-5639-2010-03 chapter 3.4	256
		using brainpoolP384r1 with SHA-384	RFC-5639-2010-03 chapter 3.6	384
12	Key Generation (see note 5)	ECDSA Key Generation	ANSI X9.62-2005 section 4.3 and ISO/IEC 15946-1:2002 section 6.1 (not 6.1.1)	
		using curve "curve P-256"	NIST-FIPS-PUB-186-4 D.2.3 "Curve P-256"	256
		using curve "curve P-384"	NIST-FIPS-PUB-186-4 D.2.4 "Curve P-384"	384
		using brainpoolP256r1	RFC-5639-2010-03 chapter 3.4	256
		using brainpoolP384r1	RFC-5639-2010-03 chapter 3.6	384

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits

Notes:

1. This TOE uses TDES provided by the underlying chip SLE78CFX*P (M7892 B11). For TDES operation see [Infineon-ST-Chip-B11-2013-08-13], 7.1.4.2 Triple-DES Operation.
2. This TOE uses the RSA crypto library v1.02.013 of the underlying chip SLE78CFX*P (M7892 B11). For the signature generation see [Infineon-ST-Chip-B11-2013-08-13], 7.1.4.4 Rivest-Shamir-Adleman (RSA) operation.
3. This TOE uses the RSA crypto library v1.02.013 of the underlying chip SLE78CFX*P (M7892 B11). For the cryptographic key generation algorithm "rsagen1" see [Infineon-ST-Chip-B11-2013-08-13], section 7.1.4.5 Rivest-Shamir-Adleman (RSA) key generation.
4. This TOE uses the EC crypto library v1.02.013 of the underlying chip SLE78CFX*P (M7892 B11). For the "Elliptic Curve Digital Signature Algorithm (ECDSA)" see [Infineon-ST-Chip-B11-2013-08-13], 7.1.4.7 Elliptic Curve DSA (ECDSA) operation.
5. This TOE uses the EC crypto library v1.02.013 of the underlying chip SLE78CFX*P (M7892 B11). For the cryptographic key generation algorithm "Elliptic Curve EC specified in ANSI X9.62-2005 and ISO/IEC 15946-1:2002" see [Infineon-ST-Chip-B11-2013-08-13], 7.1.4.8 Elliptic Curve (EC) key generation.
6. This TOE uses the SHA-2 crypto library v1.01 of the underlying chip SLE78CFX*P (M7892 B11). For the hash algorithms SHA-256 and SHA-512 see [Infineon-ST-Chip-B11-2013-08-13], 7.1.4.10 SHA-2 Operation. A SHA-384 value is computed by CardOS V5.3 from a SHA-512 value according to [NIST-FIPS-PUB-180-4] chapter 6.5.
7. For the challenge the random number generator of the underlying chip SLE78CFX*P (M7892 B11) is used. The chip provides a Physical True Random Number Generator (PTRNG) which meets the requirements of the functionality class PTG.2 of the [BSI-AIS31-V3].
8. This TOE uses the AES provided by the underlying chip SLE78CFX*P (M7892 B11). For AES operation see [Infineon-ST-Chip-B11-2013-08-13], 7.1.4.3 AES Operation.

8.2.3 Configurations

It is not possible to use all of the following Security Functional Requirements simultaneously, e.g. a TOE using the RSA algorithm for creating signature must not use simultaneously the ECDSA algorithm for creating signature and vice versa.

1. A configuration of the TOE shall use only one of the following SFRs:
   - FIA_AFL.1/VarLenPINRC
   - FIA_AFL.1/FixedLenPINRC
2. A configuration of the TOE shall use only one of the following groups of SFRs:
   - FCS_CKM.1/RSA, FCS_COP.1/RSA
   - FCS_CKM.1/EC, FCS_COP.1/EC
3. Depending on which SFR of (2) shall be used the domain parameters of an EC have to be imported or not. This concerns the following SFRs:
   - FMT_SMF.1
   - FMT_MTD.1/Ini-Data
4. Only if a configuration needs a PUK, the TOE shall use SFR
   - FIA_AFL.1/PUK
5. If a configuration does not need a PUK, the RAD of the Signatory consists only of a PIN. If a configuration needs a PUK, the RAD of the Signatory consists of PIN and PUK. This concerns the following SFRs
   - FIA_UID.1
   - FIA_UAU.1
   - FMT_SMF.1
   - FMT_MTD.1/RAD
   - FMT_MTD.1/Signatory

8.2.4 Cryptographic support (FCS)

8.2.4.1 FCS_CKM.1/EC *Cryptographic key generation*

Hierarchical to: No other components.

Dependencies:

- [FCS_CKM.2 Cryptographic key distribution, or
- FCS_COP.1 Cryptographic operation]
- FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/EC

The TSF shall generate an SCD/SVD pair in accordance with a specified cryptographic key generation algorithm **Elliptic Curve EC specified in ANSI X9.62-2005 and ISO/IEC 15946-1:2002** [3] and specified cryptographic key sizes **256 bits and 384 bits** [4] that meet the following:

1. **ECDSA Key Generation: 1. According to the appendix A4.3 in ANSI X9.62-2005 the cofactor h is not supported. 2. According to section 6.1 (not 6.1.1) in ISO/IEC 15946-1:2002**

using curves

1. **for 256 bits: P-256 ([NIST-FIPS-PUB-186-4], chapter D.2.3 "Curve P-256", aka secp256r1)**
2. **for 384 bits: P-384 ([NIST-FIPS-PUB-186-4], chapter D.2.4 "Curve P-384", aka secp384r1)**
3. **for 256 bits: brainpoolP256r1 ([RFC-5639-2010-03] chapter 3.4)**
4. **for 384 bits: brainpoolP384r1 ([RFC-5639-2010-03] chapter 3.6)**. [5]

Note:

1. FCS_CKM.1/EC amounts to requirement "FCS_CKM.1" with the selection of ECC key generation.
2. This TOE uses the EC crypto library v1.02.013 of the underlying chip SLE78CFX*P (M7892 B11).
3. For the cryptographic key generation algorithm "Elliptic Curve EC specified in ANSI X9.62-2005 and ISO/IEC 15946-1:2002" see [Infineon-ST-Chip-B11-2013-08-13], 7.1.4.8 Elliptic Curve (EC) key generation.
4. If a configuration of the TOE uses FCS_CKM.1/RSA, it must not use this SFR additionally.

8.2.4.2 FCS_CKM.4 *Cryptographic key destruction*

Hierarchical to: No other components.

Dependencies:

- [FDP_ITC.1 Import of user data without security attributes,
- or FDP_ITC.2 Import of user data with security attributes,
- or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting the key with zeros** [6] that meets the following: **none** [7] .

8.2.4.3 FCS_COP.1/EC *Cryptographic operation*

Hierarchical to: No other components.

3 [assignment: cryptographic key generation algorithm]
4 [assignment: cryptographic key sizes]
5 [assignment: list of standards]
6 [assignment: cryptographic key destruction method]
7 [assignment: list of standards]

Dependencies:

- [FDP_ITC.1 Import of user data without security attributes, or
- FDP_ITC.2 Import of user data with security attributes, or
- FCS_CKM.1 Cryptographic key generation]
- FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/EC

The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm **Elliptic Curve Digital Signature Algorithm (ECDSA)** [8] and cryptographic key sizes **256 bits and 384 bits** [9] that meet the following:

1. **Signature Generation: 1. According to section 7.3 in ANSI X9.62 - 2005 Not implemented is step d) and e) thereof. The output of step e) has to be provided as input to our function by the caller. Deviation of step c) and f): The jumps to step a) were substituted by a return of the function with an error code, the jumps are emulated by another call to our function. 2. According to sections 6.2 (6.2.2. + 6.2.3) in ISO/IEC 15946-2:2002 Not implemented is section 6.2.1: The output of 5.4.2 has to be provided by the caller as input to the function.**

using curves

1. **for 256 bits: P-256 ([NIST-FIPS-PUB-186-4], chapter D.2.3 "Curve P-256", aka secp256r1)**
2. **for 384 bits: P-384 ([NIST-FIPS-PUB-186-4], chapter D.2.4 "Curve P-384", aka secp384r1)**
3. **for 256 bits: brainpoolP256r1 ([RFC-5639-2010-03] chapter 3.4)**
4. **for 384 bits: brainpoolP384r1 ([RFC-5639-2010-03] chapter 3.6)**. [10]

Note:

1. FCS_COP.1/EC amounts to requirement "FCS_COP.1" with the selection of ECDSA.
2. This TOE uses the EC crypto library v1.02.013 of the underlying chip SLE78CFX*P (M7892 B11).
3. For the "Elliptic Curve Digital Signature Algorithm (ECDSA)" see [Infineon-ST-Chip-B11-2013-08-13], 7.1.4.7 Elliptic Curve DSA (ECDSA) operation.
4. If a configuration of the TOE uses FCS_COP.1/RSA, it must not use this SFR additionally.

8.2.4.4 FCS_CKM.1/RSA *Cryptographic key generation*

Hierarchical to: No other components.

Dependencies:

- [FCS_CKM.2 Cryptographic key distribution, or
- FCS_COP.1 Cryptographic operation]
- FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/RSA

The TSF shall generate an SCD/SVD pair in accordance with a specified cryptographic key generation algorithm **rsagen1 (PKCS1 v2.1 RFC3447)** [11] and specified cryptographic key sizes **2048 - 4096 bits** [12] that meet the following:

PKCS1 v2.1 RFC3447, section 3.2(2). [13]

Note:

1. "FCS_CKM.1/RSA" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (iterated).
2. This TOE uses the RSA crypto library v1.02.013 of the underlying chip SLE78CFX*P (M7892 B11).

8 [assignment: cryptographic algorithm]
9 [assignment: cryptographic key sizes]
10 [assignment: list of standards]
11 [assignment: cryptographic key generation algorithm]
12 [assignment: cryptographic key sizes]
13 [assignment: list of standards]

3. For the cryptographic key generation algorithm "rsagen1" see [Infineon-ST-Chip-B11-2013-08-13], section 7.1.4.5 Rivest-Shamir-Adleman (RSA) key generation.
4. If a configuration of the TOE uses FCS_CKM.1/EC, it must not use this SFR additionally.

8.2.4.5 FCS_COP.1/RSA *Cryptographic operation*

Hierarchical to: No other components.

Dependencies:

- [FDP_ITC.1 Import of user data without security attributes, or
- FDP_ITC.2 Import of user data with security attributes, or
- FCS_CKM.1 Cryptographic key generation]
- FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/RSA

The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm **Rivest-Shamir-Adleman (RSA)** [14] and cryptographic key sizes **2048 - 4096 bits** [15] that meet the following:

1. **Signature Generation (with or without CRT): According to section 5.2.1 RSASP1 in PKCS1 v2.1 RFC3447 for u = 2, i.e., without any (r_i, d_i, t_i), i >2, therefore without 5.2.1.2.b (ii)&(v), without 5.2.1.1. 5.2.1.2.a, only supported up to n < 2 POWER 2048**. [16]

Note:

1. "FCS_COP.1/RSA" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (iterated).
2. This TOE uses the RSA crypto library v1.02.013 of the underlying chip SLE78CFX*P (M7892 B11).
3. For the "Rivest-Shamir-Adleman (RSA)" see [Infineon-ST-Chip-B11-2013-08-13], 7.1.4.4 Rivest-Shamir-Adleman (RSA) operation.
4. The padding is done according to RSASSA-PSS and RSASSA-PKCS1-v1_5.
5. If a configuration of the TOE uses FCS_CKM.1/EC, it must not use this SFR additionally.

8.2.4.6 FCS_COP.1/SHA-2 *Cryptographic operation - SHA-2 hash calculation*

Hierarchical to: No other components.

Dependencies:

- [FDP_ITC.1 Import of user data without security attributes, or
- FDP_ITC.2 Import of user data with security attributes, or
- FCS_CKM.1 Cryptographic key generation]
- FCS_CKM.4 Cryptographic key destruction

Notes:

1. [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] are not fulfilled but justified:
   A hash function does not use cryptographic keys, hence FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1 are not relevant.
2. FCS_CKM.4 Cryptographic key destruction is not fulfilled but justified:
   A hash function does not use cryptographic keys, hence FCS_CKM.4 is not relevant.

FCS_COP.1.1/SHA-2

The TSF shall perform **hash-value calculation of user chosen data** [17] in accordance with the specified cryptographic algorithms **SHA-256**, **SHA-384** and **SHA-512** [18] and cryptographic key sizes **none** [19] that meet the following:

14 [assignment: cryptographic algorithm]
15 [assignment: cryptographic key sizes]
16 [assignment: list of standards]
17 [assignment: list of cryptographic operations]
18 [assignment: cryptographic algorithm]
19 [assignment: cryptographic key sizes]

1. **[NIST-FIPS-PUB-180-4] with chapters 6.2 "SHA-256", 6.4 "SHA-512" and 6.5 "SHA-384"** [20]

Notes:

1. "FCS_COP.1/SHA-2" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (not iterated).
2. "FCS_COP.1/SHA-2" is used for key derivation cf FCS_CKM.1/AuthScheme Part Two.
3. "FCS_COP.1/SHA-2" is used for internally calculated hash values which are used afterward for the signature creation including last round hash values.
4. For the "hash-value calculation of user chosen data" in case of SHA-256 and SHA-512 see [Infineon-ST-Chip-B11-2013-08-13], 7.1.4.10 SHA-2 Operation.
5. A SHA-384 value is computed by CardOS V5.3 from a SHA-512 value according to [NIST-FIPS-PUB-180-4] chapter 6.5.

8.2.4.7 FCS_CKM.1/AuthScheme *Cryptographic key generation - using the Authentication Scheme*

Hierarchical to: No other components.

Dependencies:

- [FCS_CKM.2 Cryptographic key distribution, or
- FCS_COP.1 Cryptographic operation]
- FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/AuthScheme

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm

that consists of Part One + Part Two or of Part One + Part Three:

1. **Part One uses a "Symmetric Authentication Scheme" which**
   1. **authenticates the RA-Terminal at phase OPERATIONAL to the TOE**
   2. **authenticates the TOE to the RA-Terminal at phase OPERATIONAL**
   3. **results additionally in a secret that is shared by the RA-Terminal and the TOE consisting of K.IFD = 64 byte random number of the terminal and K.ICC = 64 byte random number of the chip**.
2. **Part Two creates TDES session keys as follows:**
   K.IFD = 64 byte random number of the terminal, K.ICC = 64 byte random number of the chip, SSC = send sequence number.
   K= K.IFD XOR K.ICC
   HASH1= SHA-256(K concatenate 00000001)
   SK.ENC = ODDPARITY(First 24 Byte of HASH1)
   HASH2= SHA-256(K concatenate 00000002)
   SK.MAC = ODDPARITY(First 24 Byte of HASH2)
   SSC.MAC = Last 8 Byte of HASH2
   With SK.ENC three keys (=TDES) for encryption/decryption are generated:
   Bytes 1 - 8 = ENC.Ka, bytes 9 - 16 = ENC.Kb, bytes 17 - 24 = ENC.Kc.
   With SK.MAC three keys (=TDES) for MACing are generated:
   Bytes 1 - 8 = MAC.Ka, bytes 8 - 16 = MAC.Kb, bytes 17 - 24 = MAC.Kc.
3. **Part Three creates AES session keys as follows:**
   K.IFD = 64 byte random number of the terminal, K.ICC = 64 byte random number of the chip, SSC = send sequence number.
   K= K.IFD XOR K.ICC
   HASH1= SHA-256(K concatenate 00000001)
   SK.ENC = First 16 Byte of HASH1
   HASH2= SHA-256(K concatenate 00000002)
   SK.MAC = First 16 Byte of HASH2
   SSC.MAC = Last 16 Byte of HASH2. [21]

and specified cryptographic key sizes **168 bits (for TDES) or 128 bits (for AES)** [22] that

20 [assignment: list of standards]
21 [assignment: cryptographic key generation algorithm]
22 [assignment: cryptographic key sizes]

meet the following:

1. **For Part One**
   [CWA-14890-1], chapter "8.7 Symmetric authentication scheme"
2. **For Part Two**
   The algorithm is the same as listed in [CWA-14890-1], chapter 8.8 "Compute session keys from key seed K.IFD/ICC" except for (a) the use of SHA-256 instead of SHA-1, (b) mapping SK.ENC and SK.MAC to three sub-keys, (c) generation of SSC
3. **For Part Three**
   [BSI-TR-03111-V111-ECC], chapter "4.3.3 Key Derivation Functions" and sub-chapter "4.3.3.2 Key Derivation for AES" except for (a) the use of SHA-256 instead of SHA-1, (b) mapping to SK.ENC and to SK.MAC, (c) generation of SSC. [23]

Notes:

1. "FCS_CKM.1/AuthScheme" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (not iterated).
2. The symmetric key data used by "Part One" is stored by the Administrator at the phase ADMINISTRATION using FMT_MTD.1/Ini-Data.
3. ODDPARITY computes the error detecting parity bits.

8.2.4.8 FCS_CKM.4/AuthScheme *Cryptographic key destruction - session key for the Trusted Channel*

Hierarchical to: No other components. Dependencies:

- [FDP_ITC.1 Import of user data without security attributes, or
- FDP_ITC.2 Import of user data with security attributes, or
- FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1/AuthScheme

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting the derived keys with zeros** [24] that meets the following: **none** [25].

Notes:

1. "FCS_CKM.4/AuthScheme" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (iterated).

8.2.4.9 FCS_COP.1/3DES-ENC *Cryptographic operation - En-/decrypting with 3DES*

Hierarchical to: No other components.

Dependencies:

- [FDP_ITC.1 Import of user data without security attributes, or
- FDP_ITC.2 Import of user data with security attributes, or
- FCS_CKM.1 Cryptographic key generation]
- FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/3DES-ENC

The TSF shall perform **encrypting and decrypting** [26] in accordance with a specified cryptographic algorithm **Triple Data Encryption Standard (3DES) in CBC mode** [27] and cryptographic key size **3 x 56 bits** [28] that meet the following:

1. **(for CBC): [NIST-800-38A-2001], chapter 6.2 THE CIPHER BLOCK CHAINING MODE.**
2. **National Institute of Standards and Technology (NIST), Technology**

23 [assignment: list of standards]
24 [assignment: cryptographic key destruction method]
25 [assignment: list of standards]
26 [assignment: list of cryptographic operations]
27 [assignment: cryptographic algorithm]
28 [assignment: cryptographic key sizes]

Administration, U.S. Department of Data Encryption Standard (DES), NIST Special Publication 800-67, Version 1.1. [29]

Note:

1. "FCS_COP.1/3DES-ENC" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (not iterated).
2. This TOE uses the Triple-DES provided by the underlying chip SLE78CFX*P (M7892 B11).
3. For the "Triple-DES encrypting and decrypting" see [Infineon-ST-Chip-B11-2013-08-13], 7.1.4.2 Triple-DES Operation.
4. The keys of TDES (ENC.Ka, ENC.Kb and ENC.Kc) are filled using FCS_CKM.1/AuthScheme Part Two.

8.2.4.10 FCS_COP.1/3DES-MAC *Cryptographic operation - MACing with 3DES*

Hierarchical to: No other components.

Dependencies:

- [FDP_ITC.1 Import of user data without security attributes, or
- FDP_ITC.2 Import of user data with security attributes, or
- FCS_CKM.1 Cryptographic key generation]
- FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/3DES-MAC

The TSF shall perform **message authentication code** [30] in accordance with a specified cryptographic algorithm **Triple Data Encryption Standard (3DES) in Retail-MAC mode** [31] and cryptographic key size **3 x 56 bits** [32] that meet the following:

1. **for Retail-MAC: [ISO-IEC-9797-1-2011], algorithm 3 and padding method 2**.
2. **for TDES: National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Data Encryption Standard (DES), NIST Special Publication 800-67, Version 1.1**. [33]

Note:

1. "FCS_COP.1/3DES-MAC" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (not iterated).
2. This TOE uses the Triple-DES provided by the underlying chip SLE78CFX*P (M7892 B11).
3. For the "Triple-DES in CBC mode encrypting and decrypting" see [Infineon-ST-Chip-B11-2013-08-13], 7.1.4.2 Triple-DES Operation.
4. The keys of TDES (MAC.Ka, MAC.Kb and MAC.Kc) are filled using FCS_CKM.1/AuthScheme Part Two.

8.2.4.11 FCS_COP.1/AES-ENC *Cryptographic operation - En-/decrypting with AES*

Hierarchical to: No other components.

Dependencies:

- [FDP_ITC.1 Import of user data without security attributes, or
- FDP_ITC.2 Import of user data with security attributes, or
- FCS_CKM.1 Cryptographic key generation]
- FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/AES-ENC

The TSF shall perform **encrypting and decrypting** [34] in accordance with a specified cryptographic algorithm **Advanced Encryption Standard (AES) in CBC mode** [35] and cryptographic key size **128 bits, 192 bits and 256 bits** [36] that meet the following:

29 [assignment: list of standards]
30 [assignment: list of cryptographic operations]
31 [assignment: cryptographic algorithm]
32 [assignment: cryptographic key sizes]
33 [assignment: list of standards]
34 [assignment: list of cryptographic operations]
35 [assignment: cryptographic algorithm]
36 [assignment: cryptographic key sizes]

1. **(for CBC): [NIST-800-38A-2001], chapter 6.2 THE CIPHER BLOCK CHAINING MODE.**
2. **for AES: U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES), FIPS PUB 197**. [37]

Note:

1. "FCS_COP.1/AES-ENC" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (not iterated).
2. This TOE uses the AES provided by the underlying chip SLE78CFX*P (M7892 B11).
3. For the "Advanced Encryption Standard (AES)" see [Infineon-ST-Chip-B11-2013-08-13], 7.1.4.3 AES Operation.

8.2.4.12 FCS_COP.1/AES-MAC *Cryptographic operation - MACing with AES*

Hierarchical to: No other components.

Dependencies:

- [FDP_ITC.1 Import of user data without security attributes, or
- FDP_ITC.2 Import of user data with security attributes, or
- FCS_CKM.1 Cryptographic key generation]
- FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/AES-MAC

The TSF shall perform **message authentication code** [38] in accordance with a specified cryptographic algorithm **Advanced Encryption Standard (AES) in CMAC mode** [39] and cryptographic key size **128 bits, 192 bits and 256 bits** [40] that meet the following:

1. **for CMAC: [ISO-IEC-9797-1-2011], algorithm 1 and padding method 2**.
2. **for AES: U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES), FIPS PUB 197**. [41]

Note:

1. "FCS_COP.1/AES-MAC" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (not iterated).
2. This TOE uses the AES provided by the underlying chip SLE78CFX*P (M7892 B11).
3. For the "Advanced Encryption Standard (AES)" see [Infineon-ST-Chip-B11-2013-08-13], 7.1.4.3 AES Operation.

8.2.5 User data protection (FDP)

The security attributes and related status for the subjects and objects are:

37 [assignment: list of standards]
38 [assignment: list of cryptographic operations]
39 [assignment: cryptographic algorithm]
40 [assignment: cryptographic key sizes]
41 [assignment: list of standards]

Table 4: Security Attributes and related Status for the Subjects and Objects

Subject or object the security attribute is associated	with Security attribute type	Value of the security attribute
S.User	Role	R.Admin, R.Sigy, **R.RA-Terminal**
S.User	SCD/SVD Management	authorized, not authorized
S.User	**SM-Connection**	**established, not established**
SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value
SVD	(This ST does not define security attributes for SVD)	(This ST does not define security attributes for SVD)

Note:

1. Security attribute type "SM-Connection" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] and states whether a Trusted Channel is established or not using means of encryption/decryption and MAC keys.
2. "R.RA-Terminal" is added to contents of PP [BSI-PP0059-2009].

8.2.5.1 FDP_ACC.1/SCD/SVD_Generation_SFP *Subset access control*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/SCD/SVD_Generation_SFP

The TSF shall enforce the SCD/SVD_Generation_SFP on

1. subjects: S.User,
2. objects: SCD, SVD,
3. operations: generation of SCD/SVD pair.

8.2.5.2 FDP_ACF.1/SCD/SVD_Generation_SFP *Security attribute based access control*

Hierarchical to: No other components.

Dependencies:

- FDP_ACC.1 Subset access control
- FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/SCD/SVD_Generation_SFP

The TSF shall enforce the SCD/SVD_Generation_SFP to objects based on the following:

the user S.User is associated with the security attribute "SCD/SVD Management".

FDP_ACF.1.2/SCD/SVD_Generation_SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

S.User with the security attribute "SCD/SVD Management" set to "authorized" is allowed to generate SCD/SVD pair.

FDP_ACF.1.3/SCD/SVD_Generation_SFP

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4/SCD/SVD_Generation_SFP

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

S.User with the security attribute "SCD/SVD Management" set to "not authorized" is not allowed to generate SCD/SVD pair.

Note:

1. The key pair can be generated only once.

8.2.5.3 FDP_ACC.1/SVD_Transfer_SFP *Subset access control*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/SVD_Transfer_SFP

The TSF shall enforce the SVD_Transfer_SFP on

1. subjects: S.User,
2. objects: SVD
3. operations: export.

8.2.5.4 FDP_ACF.1/SVD_Transfer_SFP *Security attribute based access control*

Hierarchical to: No other components.

Dependencies:

- FDP_ACC.1 Subset access control
- FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/SVD_Transfer_SFP

The TSF shall enforce the SVD_Transfer_SFP to objects based on the following:

1. the S.User is associated with the security attribute Role
2. the SVD
3. **the user S.User is associated with the security attribute "SM-Connection"**. [42]

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:

R.RA-Terminal [43] is allowed to export SVD **if the security attribute "SM-Connection" is set to "established"**. [44]

FDP_ACF.1.3/SVD_Transfer_SFP

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

42 is a [REFINEMENT]
43 is a [REFINEMENT] of [selection: R.Admin, R.Sigy]
44 is a [REFINEMENT]

FDP_ACF.1.4/SVD_Transfer_SFP

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

R.RA-Terminal is not allowed to export SVD if the security attribute "SM-Connection" is set to "not established". [45]

Note:

1. The changes represent the need to export the public key via Trusted Channel SM only.

This ST does not require the TOE to protect the integrity and authenticity of the exported SVD public key but requires such protection by the operational environment. If the operational environment does not provide sufficient security measures for the CGA to ensure the authenticity of the public key the TOE shall implement additional security functions to support the export of public keys with integrity and data origin authentication. See EN 14169-4 "Protection Profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application" for additional requirements for use of an SSCD in an environment that cannot provide such protection.

8.2.5.5 FDP_ACC.1/Signature-creation_SFP *Subset access control*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/Signature-creation_SFP

The TSF shall enforce the Signature-creation_SFP on

1. subjects: S.User,
2. objects: DTBS/R, SCD,
3. operations: signature creation.

8.2.5.6 FDP_ACF.1/Signature-creation_SFP *Security attribute based access control*

Hierarchical to: No other components.

Dependencies:

- FDP_ACC.1 Subset access control
- FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/Signature-creation_SFP

The TSF shall enforce the Signature-creation_SFP to objects based on the following:

1. the user S.User is associated with the security attribute "Role" and
2. the SCD with the security attribute "SCD Operational".

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:

R.Sigy is allowed to create digital signatures for DTBS/R with SCD whose security attribute "SCD operational" is set to "yes".

FDP_ACF.1.3/Signature-creation_SFP

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4/Signature-creation_SFP

45 is a [REFINEMENT] of none

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

S.User is not allowed to create digital signatures for DTBS/R with SCD whose security attribute "SCD operational" is set to "no".

8.2.5.7 FDP_ACC.1/Config_DF_QES *Subset access control - configuration of DF_QES*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/Config_DF_QES

The TSF shall enforce the **DF_QES-Configuration_SFP** [46] on

1. subjects: **S.User**,
2. objects: **Signature-creation function**,
3. operations:
   configuration including
   1. **installation of Transport Protection for DF_QES by updating of TPIN_QES with a non confidential value**
   2. **creation and deletion of EFs and DFs below DF_QES**
   3. **updating of contents of EFs and DFs below DF_QES**. [47]

Notes:

1. "FDP_ACC.1/Config_DF_QES" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (not iterated).
2. "DF_QES-Configuration_SFP" is performed only at phase OPERATIONAL.
3. Operation (1) can be performed only once.
4. Operations (2) and (3) are optional and might be performed more than one time.
5. The RA is not able to remove DF_QES or to create / remove objects within DF_QES or to update other objects than TPIN_QES within DF_QES.
6. Standard EF names for storing certificates are EF_C_X509_CH_DS and EF_C_X509_CA_CSDS.
7. Explanation of EF file names and object names:

   DF_QES

   DF with Application for QES

   EF_C_X509_CH_DS

   EF for the (qualified) certificate belonging to the SCD/SVD pair

   EF_C_X509_CA_CSDS

   EF for the certificate of the Certification Authority which generates the (qualified) certificate belonging to the SCD/SVD pair

   TPIN_QES

   Object containing the VAD for the Transport PIN

8.2.5.8 FDP_ACF.1/Config_DF_QES *Security attribute based access control- configuration of DF_QES*

Hierarchical to: No other components.

Dependencies:

- FDP_ACC.1 Subset access control
- FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/Config_DF_QES

46 [assignment: access control SFP]
47 [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

The TSF shall enforce the **DF_QES-Configuration_SFP** [48] to objects based on the following:

1. **the user S.User is associated with the security attribute "Role"**
2. **the user S.User is associated with the security attribute "SM-Connection"**. [49]

FDP_ACF.1.2/Config_DF_QES

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

R.RA-Terminal is allowed to configure DF_QES if the security attribute "SM-Connection" is set to "established". [50]

FDP_ACF.1.3/Config_DF_QES

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none** [51].

FDP_ACF.1.4/Config_DF_QES

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

R.RA-Terminal is not allowed to configure DF_QES if the security attribute "SM-Connection" is set to "not established". [52]

Notes:

1. "FDP_ACF.1/Config_DF_QES" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (not iterated).

8.2.5.9 FDP_RIP.1 *Subset residual information protection*

Hierarchical to: No other components.

Dependencies: No dependencies.

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 **[REFINEMENT] and symmetric key data for Authentication Scheme**.

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

(1) SCD

(2) SVD (if persistently stored by the TOE)

[REFINEMENT]

(3) **symmetric key data for the Authentication Scheme**

[END REFINEMENT]

The DTBS/R temporarily stored by the TOE has the user data attribute "integrity checked stored data".

48 [assignment: access control SFP]
49 [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]
50 [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
51 [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]
52 [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

8.2.5.10 FDP_SDI.2/Persistent *Stored data integrity monitoring and action*

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

FDP_SDI.2.1/Persistent

The TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes: integrity checked stored data.

FDP_SDI.2.2/Persistent

Upon detection of a data integrity error, the TSF shall

1. prohibit the use of the altered data
2. inform the S.Sigy about integrity error.

8.2.5.11 FDP_SDI.2/DTBS *Stored data integrity monitoring and action*

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

FDP_SDI.2.1/DTBS

The TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes: integrity checked stored DTBS.

FDP_SDI.2.2/DTBS

Upon detection of a data integrity error, the TSF shall

1. prohibit the use of the altered data
2. inform the S.Sigy about integrity error.

8.2.6 Trusted Path/Channels (FTP)

8.2.6.1 FTP_ITC.1/SM_ADS_Conf *Inter-TSF trusted channel - for ADS Configuration + SVD export*

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/SM_ADS_Conf

The TSF shall provide a communication channel between itself and another 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/SM_ADS_Conf

The TSF shall permit **local and remote RA-Terminals** [53] to initiate communication via the trusted channel.

FTP_ITC.1.3/SM_ADS_Conf

The TSF shall initiate communication via the trusted channel for

53 [selection: the TSF, another trusted IT product]

1. **DF_QES-Configuration_SFP**
2. **SVD_Transfer_SFP**. [54]

Notes:

1. "FTP_ITC.1/SM_ADS_Conf" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (not iterated).
2. Remote RA-Terminals establish the Trusted Channel using the Internet.
3. The commands sent via the Trusted Channel are encrypted and MACed, see FCS_COP.1/3DES-ENC and FCS_COP.1/3DES-MAC or FCS_COP.1/AES-ENC and FCS_COP.1/AES-MAC.
4. It is possible to use an AES key and the derived keys are AES or TDES keys. It is possible to use a TDES key and the derived keys are AES or TDES keys.

8.2.7 Identification and authentication (FIA)

8.2.7.1 FIA_UID.1 *Timing of identification*

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1

The TSF shall allow

1. Self test according to FPT_TST.1
2. **Performing of the Authentication Scheme**
3. **Entering of the Transport PIN**
4. **Entering of the Signatory RAD** [55]

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.

Notes:

1. If the Transport PIN is not set, it is not possible to enter a Transport PIN successfully (Application for QES is deactivated) and it is not possible to block the Transport PIN with unsuccessful consecutive authentication attempts.
2. If the Transport PIN is not entered successfully or the Transport PIN is blocked, the Signatory cannot be identified or authenticated.
3. If the Transport PIN is entered successfully, it is not possible to enter a Transport PIN again.
4. If the Signatory PIN is not set, it is not possible to enter the Signatory PIN successfully and it is not possible to block the Signatory PIN with unsuccessful consecutive authentication attempts.
5. After performing successfully the Authentication Scheme the RA-Terminal is identified and authenticated.
6. The Trusted Channel is established after the RA-Terminal is identified and authenticated.
7. If a configuration does not need a PUK, the Signatory RAD consists of the Signatory PIN only.
8. If a configuration needs a PUK, the Signatory RAD consists of the Signatory PIN and of Signatory PUK.

8.2.7.2 FIA_UAU.1 *Timing of authentication*

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1

The TSF shall allow

54 [assignment: list of functions for which a trusted channel is required]
55 [assignment: list of TSF-mediated actions]

1. Self test according to FPT_TST.1,
2. Identification of the user by means of TSF required by FIA_UID.1.
3. **Performing of the Authentication Scheme**
4. **Entering of the Transport PIN**
5. **Entering of the Signatory RAD** [56]

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.

Notes:

1. If the Transport PIN is not set, it is not possible to enter a Transport PIN successfully (Application for QES is deactivated) and it is not possible to block the Transport PIN with unsuccessful consecutive authentication attempts.
2. If the Transport PIN is not entered successfully or the Transport PIN is blocked, the Signatory cannot be identified or authenticated.
3. If the Transport PIN is entered successfully, it is not possible to enter a Transport PIN again.
4. If the Signatory RAD is not set, it is not possible to enter the Signatory RAD successfully and it is not possible to block the Signatory PIN with unsuccessful consecutive authentication attempts.
5. After performing successfully the Authentication Scheme the RA-Terminal is identified and authenticated.
6. The Trusted Channel is established after the RA-Terminal is identified and authenticated.
7. If a configuration does not need a PUK, the Signatory RAD consists of the Signatory PIN only.
8. If a configuration needs a PUK, the Signatory RAD consists of the Signatory PIN and of Signatory PUK.

8.2.7.3 FIA_AFL.1/FixedLenPINRC *Authentication failure handling - with fixed length retry counter*

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 *Timing of authentication*

FIA_AFL.1.1/FixedLenPINRC

The TSF shall detect when **10** [57] unsuccessful authentication attempts occur related to consecutive failed authentication attempts.

FIA_AFL.1.2/FixedLenPINRC

When the defined number of unsuccessful authentication attempts has been met, the TSF shall block RAD **[REFINEMENT] of the PIN with fixed length retry counter**.

Notes:

1. FIA_AFL.1/FixedLenPINRC amounts to requirement "FIA_AFL.1" with the [REFINEMENT] with fixed length retry counter.
2. The minimal length of the PIN has to be 6.
3. A configuration which retry counter does not depend on PIN's length, shall use this SFR.
4. If a configuration of the TOE uses FIA_AFL.1/VarLenPINRC, it must not use this SFR additionally.
5. With "The TOE stores signatory reference authentication data to authenticate a user as its signatory", see PP [BSI-CC-PP-0059-2009-MA-01], this requirement concerns the PIN of the Signatory only.

56 [assignment: list of additional TSF mediated actions]
57 [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

8.2.7.4 FIA_AFL.1/VarLenPINRC *Authentication failure handling - with variable length retry counter*

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 *Timing of authentication*

FIA_AFL.1.1/VarLenPINRC

> The TSF shall detect when **an administrator configurable positive integer within 3 up to floor(MINLEN/2) (see note 2. below)** [58] unsuccessful authentication attempts occur related to consecutive failed authentication attempts.

FIA_AFL.1.2/VarLenPINRC

> When the defined number of unsuccessful authentication attempts has been met, the TSF shall block RAD **[Refinement] of the PIN with variable length retry counter**.

Notes:

1. FIA_AFL.1/VarLenPINRC is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (iterated).
2. The minimal length of the PIN has to be 6.
3. The Administrator configurable positive integer shall not exceed floor(MINLEN/2), where MINLEN denotes the minimal length of the PIN.
4. A configuration which retry counter depends on PIN's length, shall use this SFR.
5. If a configuration of the TOE uses FIA_AFL.1/FixedLenPINRC, it must not use this SFR additionally.

8.2.7.5 FIA_AFL.1/PUK *Authentication failure handling - for PUK*

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 *Timing of authentication*

FIA_AFL.1.1/PUK

> The TSF shall detect when **3** [59] unsuccessful authentication attempts occur related to consecutive failed authentication attempts.

FIA_AFL.1.2/PUK

> When the defined number of unsuccessful authentication attempts has been met, the TSF shall block RAD **[Refinement] of the PUK**.

Notes:

1. FIA_AFL.1/PUK is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (iterated).
2. If a configuration uses a PUK, the TOE shall use this SFR for PUK's authentication failure handling.

8.2.7.6 FIA_AFL.1/T-PIN *Authentication failure handling - Transport PIN*

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/T-PIN

> The TSF shall detect when **3** [60] unsuccessful authentication attempts occur related to

58 [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
59 [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
60 [selection: [assignment: positive integer number] an administrator configurable positive integer within[assignment: range of acceptable values]]

consecutive failed authentication attempts.

FIA_AFL.1.2/T-PIN

When the defined number of unsuccessful authentication attempts has been met, the TSF shall block RAD **[Refinement] of the Transport PIN**.

Note:

1. "FIA_AFL.1/T-PIN" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (iterated).

8.2.7.7 FIA_AFL.1/AuthAdmin *Authentication failure handling - of the RA-Terminal at phase OPERATIONAL*

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/AuthAdmin

The TSF shall detect when **5** [61] unsuccessful authentication attempts occur related to **consecutive failed authentication attempts** [62].

FIA_AFL.1.2/AuthAdmin

When the defined number of unsuccessful authentication attempts has been **met** [63], the TSF shall **delay the next authentication attempt at least 5 seconds** [64].

Notes:

1. "FIA_AFL.1/AuthAdmin" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (not iterated).
2. This SFR concerns the authentication of the RA-Terminal using the Authentication Scheme.

8.2.7.8 FIA_AFL.1/SM *Authentication failure handling - after establishing of the Trusted Channel*

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/SM

The TSF shall detect when **1** [65] unsuccessful authentication attempts occur related to

commands sent without means of

1. **Secure messaging with MACing based on Triple-DES or AES or**
2. **Secure messaging with encryption/decryption based on Triple-DES or AES**

or commands sent with means of

1. **Secure messaging with MACing based on Triple-DES or AES not using the correct key or**
2. **Secure messaging with encryption/decryption based on Triple-DES or AES not using the correct key**

61 [selection: [assignment: positive integer number] an administrator configurable positive integer within[assignment: range of acceptable values]]
62 [assignment: list of authentication events]
63 [selection: met, surpassed]
64 [assignment: list of actions]
65 [selection: [assignment: positive integer number], an administrator configurable positive integer within[assignment: range of acceptable values]]

to the TOE after the Trusted Channel is succcesfully established [66].

FIA_AFL.1.2/SM

When the defined number of unsuccessful authentication attempts has been **met** [67], the TSF shall

1. **terminate the Trusted Channel which is set up using the Authentication Scheme**
2. **set the security attribute SM-Connection to "not established"**
3. **terminate the authentication of user S.RA-Terminal** [68].

Notes:

1. "FIA_AFL.1/SM" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (not iterated).
2. After the RA-Terminal is authenticated at phase OPERATIONAL the Trusted Channel is established. As long as commands are sent encrypted and MACed via the Trusted Channel the RA-Terminal remains authenticated.
3. The commands sent via the Trusted Channel are encrypted and MACed, see FCS_COP.1/3DES-ENC and FCS_COP.1/3DES-MAC or FCS_COP.1/AES-ENC and FCS_COP.1/AES-MAC.

8.2.7.9 FIA_API.1/AuthScheme *Authentication Proof of Identity*

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/AuthScheme

The TSF shall provide a

Authentication Scheme according to [CWA-14890-1], chapter 8.7 Symmetric authentication scheme. [69]

to prove the identity of the **TOE** [70].

Note:

1. "FIA_API.1/AuthScheme" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (not iterated).
2. According to PP [BSI-CC-PP-0071], which replaces the assignment "authorized user or role" by "SSCD", "SSCD" is replaced here by the equivalent "TOE".

8.2.8 Security management (FMT)

8.2.8.1 FMT_SMR.1 *Security roles*

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1

The TSF shall maintain the roles **[Refinement] R.RA-Terminal** and R.Sigy

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Note:

66 [assignment: list of authentication events]
67 [selection: met, surpassed]
68 [assignment: list of actions]
69 [assignment: authentication mechanism]
70 [assignment: authorized user or role]

1. "R.RA-Terminal" is a [REFINEMENT] of "R.Admin".

8.2.8.2 FMT_SMF.1 *Security management functions*

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:

1. Creation and modification of RAD,
2. Enabling the signature-creation function,
3. Modification of the security attribute SCD/SVD Management, SCD operational and **[REFINEMENT] SM-Connection**
4. Change the default value of the security attribute SCD Identifier,
5. **Initial storing of symmetric key data for the Authentication Scheme and domain parameters of an elliptic curve used for generating of the SCD/SVD**. [71]

Note:

1. If a configuration of the TOE uses FCS_CKM.1/RSA, it does not need domain parameters of an elliptic curve for generating of the SCD/SVD.
2. If a configuration does not need a PUK, the Signatory RAD consists of the Signatory PIN only.
3. If a configuration needs a PUK, the Signatory RAD consists of the Signatory PIN and of Signatory PUK.

8.2.8.3 FMT_MOF.1 *Management of security functions behaviour*

Hierarchical to: No other components.

Dependencies:

- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions.

FMT_MOF.1.1

The TSF shall restrict the ability to enable the functions signature creation function to R.Sigy.

8.2.8.4 FMT_MSA.1/Admin *Management of security attributes - Admin at phase ADMINISTRATION*

Hierarchical to: No other components.

Dependencies:

- [FDP_ACC.1 Subset access control, or
- FDP_IFC.1 Subset information flow control]
- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/Admin

The TSF shall enforce the SCD/SVD_Generation_SFP to restrict the ability to **modify** [72] the security attribute SCD/SVD Management to R.Admin [REFINEMENT] **before finishing the Basic Configuration**.

71 [assignment: list of other security management functions to be provided by the TSF].
72 [assignment: other operations]

8.2.8.5 FMT_MSA.1/RA-Terminal *Management of security attributes - RA at phase OPERATIONAL*

Hierarchical to: No other components.

Dependencies:

- [FDP_ACC.1 Subset access control, or
- FDP_IFC.1 Subset information flow control]
- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/RA-Terminal

> The TSF shall enforce the **SVD_Transfer_SFP and the DF_QES-Configuration_SFP** [73] to restrict the ability to **modify** [74] the security attribute **SM-Connection** [75] to **R.RA-Terminal after issuing the card** [76].

Notes:

1. "FMT_MSA.1/RA-Terminal" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (not iterated).
2. After the card is issued the card is in phase OPERATIONAL.

8.2.8.6 FMT_MSA.1/Signatory *Management of security attributes*

Hierarchical to: No other components.

Dependencies:

- [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions

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 R.Sigy.

8.2.8.7 FMT_MSA.2 *Secure security attributes*

Hierarchical to: No other components.

Dependencies:

- [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
- FMT_MSA.1 Management of security attributes
- FMT_SMR.1 Security roles

FMT_MSA.2.1

> The TSF shall ensure that only secure values are accepted for SCD/SVD Management, SCD operational and **[REFINEMENT] SM-Connection**.
>
> **[REFINEMENT]**:
>
> **Security attribute "SM-Connection" can only have the values "established" or "not established". Both values are secure, depending on the situation.**
>
> **Security attribute "SCD operational" can only have the values "no" or "yes". Both values are secure, depending on the situation.**

73 [assignment: access control SFP(s), information flow control SFP(s)]
74 [selection: change_default, query, modify, delete, [assignment: other operations]]
75 [assignment: list of security attributes]
76 [assignment: the authorized identified roles]

Security attribute "SCD/SVD Management" can only have the values "authorized" or "not authorized". Both values are secure, depending on the situation.

The security attribute values are not secure by themselves but in combinations.

The secure values of the combinations are shown in the following table:

Table 5: Secure Values of the Combinations for Signatures

SCD/SVD Management	SM-Connection	SCD operational	Secure
authorized	established	yes	NO
authorized	established	no	NO
authorized	not established	yes	NO
authorized	not established	no	YES
not authorized	established	yes	NO
not authorized	established	no	YES
not authorized	not established	yes	YES
not authorized	not established	no	YES

.

The TSF will only accept the secure combinations listed above. The TSF ensure that a non-secure situation will not occur.

[END REFINEMENT]

8.2.8.8 FMT_MSA.3 *Static attribute initialisation*

Hierarchical to: No other components.

Dependencies:

- FMT_MSA.1 Management of security attributes
- FMT_SMR.1 Security roles

FMT_MSA.3.1

> The TSF shall enforce the SCD/SVD_Generation_SFP, SVD_Transfer_SFP, Signature-creation_SFP, **[REFINEMENT] DF_QES-Configuration_SFP,** to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

> The TSF shall allow the R.Admin to specify alternative initial values to override the default values when an object or information is created.

8.2.8.9 FMT_MSA.4 *Security attribute value inheritance*

Hierarchical to: No other components.

Dependencies:

- [FDP_ACC.1 Subset access control, or
- FDP_IFC.1 Subset information flow control]

FMT_MSA.4.1

> The TSF shall use the following rules to set the value of security attributes:
>
> 1. If **S.Admin** successfully generates an SCD/SVD pair without S.Sigy being authenticated, the security attribute "SCD operational" of the SCD shall be set to "no" as a single operation.

Note:

1. Rule (2) is deleted, because TOE does not support generating an SVD/SCD pair by the signatory alone.

8.2.8.10 FMT_MTD.1/RAD *Management of TSF data*

Hierarchical to: No other components.

Dependencies:

- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/RAD

> The TSF shall restrict the ability to create the RAD **[REFINEMENT] of the Signatory once** to **R.Sigy only after successfully authentication with the Transport PIN**.

Notes:

1. FMT_MTD.1/RAD amounts to requirement "FMT_MTD.1/Admin".
2. "R.Sigy only after successfully authentication with the Transport PIN" is a [REFINEMENT] of "R.Admin".
3. If a configuration does not need a PUK, the Signatory RAD consists of the Signatory PIN only.
4. If a configuration needs a PUK, the Signatory RAD consists of the Signatory PIN and of Signatory PUK.

8.2.8.11 FMT_MTD.1/Signatory *Management of TSF data*

Hierarchical to: No other components.

Dependencies:

- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/Signatory

The TSF shall restrict the ability to **modify** [77] the RAD **[REFINEMENT] of S.Sigy** to R.Sigy.

Notes:

1. If a configuration does not need a PUK, the Signatory RAD consists of the Signatory PIN only.
2. If a configuration needs a PUK, the Signatory RAD consists of the Signatory PIN and of Signatory PUK.

8.2.8.12 FMT_MTD.1/Ini-Data *Management of TSF data - Initial storing of data*

Hierarchical to: No other components.

Dependencies:

- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/Ini-Data

The TSF shall restrict the ability to **store** [78] the

1. **symmetric key data for the Symmetric Authentication Scheme**
2. **domain parameters of an elliptic curve used for generating of the SCD/SVD**. [79]

to **R.Admin [REFINEMENT] before issuing the card** [80].

Notes:

1. "FMT_MTD.1/Ini-Data" is added to contents of PP [BSI-CC-PP-0059-2009-MA-01] (iterated).
2. The symmetric key data for Authentication Scheme is generated outside of the TOE.
3. The symmetric key data is individual to the card (depends on card number ICCSN).
4. If a configuration of the TOE uses FCS_CKM.1/RSA, it does not need domain parameters of an elliptic curve for generating of the SCD/SVD.

8.2.9 Protection of the TSF (FPT)

8.2.9.1 FPT_EMS.1 *TOE Emanation*

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1

The TOE shall not emit **information about IC power consumption** [81] in excess of **unintelligible limits** [82] enabling access to RAD and SCD **[REFINEMENT] and symmetric key data for the Authentication Scheme**.

77 [assignment: other operations]
78 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
79 [assignment: list of TSF data]
80 [assignment: the authorized identified roles]
81 [assignment: types of emissions]
82 [assignment: specified limits]

FPT_EMS.1.2

The TSF shall ensure **S.User** [83] are unable to use the following interface **physical contacts of the underlying IC hardware** [84] to gain access to SCD and RAD **[REFINEMENT] and symmetric key data for the Authentication Scheme**.

Note:

1. The refinement is added because of "FMT_MTD.1/Ini-Data (1)".

8.2.9.2 FPT_FLS.1 *Failure with preservation of secure state*

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur:

1. self-test according to FPT_TST fails,
2. **Failures during cryptographic operations**
3. **Memory failures during TOE execution**
4. **Out of range failures of temperature, clock and voltage sensors**
5. **Failures during random number generation**. [85]

8.2.9.3 FPT_PHP.1 *Passive detection of physical attack*

Hierarchical to: No other components.

Dependencies: No dependencies.

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.

8.2.9.4 FPT_PHP.3 *Resistance to physical attack*

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1

The TSF shall resist **physical manipulation and physical probing** [86] to the **TSF** [87] by responding automatically such that the SFRs are always enforced.

8.2.9.5 FPT_TST.1 *TSF testing*

Hierarchical to: No other components.

83 [assignment: type of users]
84 [assignment: type of connection]
85 [assignment: list of other types of failures in the TSF]
86 [assignment: physical tampering scenarios]
87 [assignment: list of TSF devices/elements]

Dependencies: No dependencies.

FPT_TST.1.1

The TSF shall run a suite of self-tests **during initial start-up and at the conditions**

1. **Generation of the SCD/SVD key pair according to** "FCS_CKM.1/EC" or "FCS_CKM.1/RSA"
2. **Signature-creation according to** "FCS_COP.1/EC" or "FCS_COP.1/RSA"
3. **VAD verification**
4. **RAD modification** [88]

to demonstrate the correct operation of the TSF.

FPT_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of TSF data.

FPT_TST.1.3

The TSF shall provide authorized users with the capability to verify the integrity of TSF.

8.3 TOE Security Assurance Requirements

Table 6: Assurance Requirements: EAL4 augmented with AVA_VAN.5

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Architectural Design with domain separation and non-bypassability
	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

88 [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions[assignment: conditions under which self test should occur]]

Assurance Class	Assurance components
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

9 Rationale

9.1 Security Requirements Rationale

9.1.1 Security Requirement Coverage

Table 7: Functional Requirement to TOE security objective mapping

	OT.lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
FCS_CKM.1/EC	x		x	x	x						
FCS_CKM.4	x				x						
FCS_COP.1/EC	x					x					
FCS_CKM.1/RSA	x		x	x	x						
FCS_COP.1/RSA	x					x					
FCS_COP.1/SHA-2						x					
FCS_CKM.1/AuthScheme	x										
FCS_CKM.4/AuthScheme	x										
FCS_COP.1/3DES-ENC	x										
FCS_COP.1/3DES-MAC	x										
FCS_COP.1/AES-ENC	x										
FCS_COP.1/AES-MAC	x										
FDP_ACC.1/SCD/SVD_Generation_SFP	x	x									
FDP_ACC.1/SVD_Transfer_SFP	x										

FDP_ACC.1/Signature-creation_SFP	x						x				
FDP_ACF.1/SCD/SVD_Generation_SFP	x	x									
FDP_ACF.1/SVD_Transfer_SFP	x										
FDP_ACF.1/Signature-creation_SFP	x						x				
FDP_ACC.1/Config_DF_QES	x						x				
FDP_ACF.1/Config_DF_QES	x										
FDP_RIP.1					x		x				
FDP_SDI.2/Persistent				x	x	x					
FDP_SDI.2/DTBS							x	x			
FTP_ITC.1/SM_ADS_Conf	x										
FIA_UID.1		x					x				
FIA_UAU.1		x					x				
FIA_AFL.1/FixedLenPINRC							x				
FIA_AFL.1/VarLenPINRC							x				
FIA_AFL.1/PUK							x				
FIA_AFL.1/AuthAdmin	x										
FIA_AFL.1/T-PIN	x						x				
FIA_AFL.1/SM	x										
FIA_API.1/AuthScheme	x										
FMT_SMR.1	x						x				
FMT_SMF.1	x			x			x				
FMT_MOF.1	x						x				
FMT_MSA.1/Signatory	x						x				
FMT_MSA.1/Admin	x	x									

FMT_MSA.1/RA-Terminal	x										
FMT_MSA.2	x	x					x				
FMT_MSA.3	x	x					x				
FMT_MSA.4	x	x		x			x				
FMT_MTD.1/RAD	x						x				
FMT_MTD.1/Signatory	x						x				
FMT_MTD.1/Ini-Data	x										
FPT_EMS.1					x				x		
FPT_FLS.1					x						
FPT_PHP.1										x	
FPT_PHP.3					x						x
FPT_TST.1	x				x	x					

9.1.2 TOE Security Requirements Sufficiency

Note:

1. Statements concerning new security requirements added to contents of PP [BSI-CC-PP-0059-2009-MA-01] are marked **bold**.

9.1.2.1 OT.Lifecycle_Security (Lifecycle security)

is provided by the SFR for SCD/SVD generation

- FCS_CKM.1/EC and SCD usage FCS_COP.1/EC

or

- FCS_CKM.1/RSA **and SCD usage** FCS_COP.1/RSA

and SCD destruction FCS_CKM.4 ensure cryptographically secure life cycle of the SCD.

The SCD/SVD generation is controlled by TSF according to FDP_ACC.1/SCD/SVD_Generation_SFP and FDP_ACF.1/SCD/SVD_Generation_SFP. The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer_SFP and FDP_ACF.1/SVD_Transfer_SFP. The test functions FPT_TST.1 provides failure detection throughout the life cycle. **The final configuration of DF_QES is controlled by TSF according to** FDP_ACC.1/Config_DF_QES **and** FDP_ACF.1/Config_DF_QES. **Initial access by the end user (signatory) is ensured by** "FIA_AFL.1/T-PIN". **The authentication of the RA-Terminal at phase OPERATIONAL is ensured by** FIA_AFL.1/AuthAdmin.

The SCD usage is ensured by access control

FDP_ACC.1/Signature-creation_SFP and FDP_ACF.1/Signature-creation_SFP

which are based on the security attribute secure TSF management according to

FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/RA-Terminal, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/RAD, FMT_MTD.1/Signatory, FMT_SMF.1 and FMT_SMR.1.

The test functions FPT_TST.1 provides failure detection throughout the life cycle.

The usage of FDP_ACC.1/SVD_Transfer_SFP **and** FDP_ACC.1/Config_DF_QES **is ensured by setting up a Trusted Channel using**

- FCS_CKM.1/AuthScheme (Deriving session keys)
- FCS_CKM.4/AuthScheme (Destroying of derived session keys)
- FCS_COP.1/3DES-ENC (encrypting and decrypting of the commands)
- FCS_COP.1/3DES-MAC (MACing of the commands)
- FCS_COP.1/AES-ENC (encrypting and decrypting of the commands)
- FCS_COP.1/AES-MAC (MACing of the commands)
- FIA_API.1/AuthScheme (proving identity to the RA-Terminal)

which establish the Trusted Channel between the TOE and an RA-Terminal used by the

- SVD_Transfer_SFP
- **DF_QES-Configuration_SFP**

which are enabled by FTP_ITC.1/SM_ADS_Conf **for local RA-Terminal and remote RA-Terminal performing these SFPs using the Internet and the symmetric key data is stored by**

- FMT_MTD.1/Ini-Data

which store also the domain parameters of an elliptic curve used for generating of the SCD/SVD in case of a configuration using an elliptic curve for signature generation.

Note:

1. **Encryption, decryption and MACing is done either with TDES or AES**.

The Trusted Channel is secured by

- FIA_AFL.1/SM

which terminates the Trusted Channel.

The usage of the Authentication Scheme for the TOE is provided by FIA_API.1/AuthScheme.

The usage of

- FDP_ACC.1/SVD_Transfer_SFP **and** FDP_ACF.1/SVD_Transfer_SFP
- FDP_ACC.1/Config_DF_QES **and** FDP_ACF.1/Config_DF_QES

is based on the security attribute secure "SM-Connection" which is managed by

- FMT_MSA.1/RA-Terminal
- FIA_AFL.1/SM.

At the TC, the Administrator initially stores all symmetric key data necessary for the Authentication Scheme which is provided by FMT_MTD.1/Ini-Data.

If the card holder applies for Application for QES, the RA can activate it (importing of certificates is optionally) using

- FDP_ACC.1/Config_DF_QES **and** FDP_ACF.1/Config_DF_QES.

which are based on the security attribute secure TSF management according to

- FMT_MSA.1/RA-Terminal.

9.1.2.2 OT.SCD/SVD_Auth_Gen (Authorized SCD/SVD generation)

addresses that generation of a SCD/SVD pair requires proper user authentication. The TSF specified by

FIA_UID.1 and FIA_UAU.1 provide user identification and user authentication prior to enabling access to authorized functions. The SFR FDP_ACC.1/SCD/SVD_Generation_SFP and FDP_ACF.1/SCD/SVD_Generation_SFP provide access control for the SCD/SVD generation. The security attributes of the authenticated user are provided by FMT_MSA.1/Admin, FMT_MSA.2 and FMT_MSA.3 for static attribute initialization. The SFR FMT_MSA.4 defines rules for inheritance of the security attribute "SCD operational" of the SCD.

9.1.2.3 OT.SCD_Unique (Uniqueness of the signature-creation data)

implements the requirement of practically unique SCD as laid down in (The Directive, A.III, paragraph 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1/EC **or** FCS_CKM.1/RSA.

9.1.2.4 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/EC **or** FCS_CKM.1/RSA 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. Moreover, the SCD Identifier allows the environment to identify the SCD and to link it with the appropriate SVD. The management functions identified by FMT_SMF.1 and by FMT_MSA.4 allow R.Admin to modify the default value of the security attribute SCD Identifier.

9.1.2.5 OT.SCD_Secrecy (Secrecy of signature-creation data)

is provided by the security functions specified by the following SFR. FCS_CKM.1/EC **or** FCS_CKM.1/RSA ensures the use of secure cryptographic algorithms for SCD/SVD generation. 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_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been used for signature creation and that destruction of SCD leaves no residual information.

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 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA).

SFR FPT_EMS.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD **[REFINEMENT] and symmetric key data for the Authentication Scheme and to resist physical manipulation and physical probing to the TSF**.

9.1.2.6 OT.Sig_Secure (Cryptographic security of the digital signature)

is provided by the cryptographic algorithms specified by FCS_COP.1/EC **and by** "FCS_COP.1/SHA-2". which ensures the cryptographic robustness of the signature algorithms. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE and FPT_TST.1 ensure self-tests ensuring correct signature creation. FCS_COP.1/SHA-2 **is used before** FCS_COP.1/EC

- **if DTBS is sent to the TOE or**
- **if an intermediate hash value with the remainder of DTBS is sent to the TOE (last round hash value).**

9.1.2.7 OT.Sigy_SigF (Signature-creation function for the legitimate signatory only)

is provided by an SFR for identification authentication and access control.

FIA_UAU.1 and FIA_UID.1 ensure that no signature generation function can be invoked before the signatory is identified and authenticated. The security functions specified by FMT_MTD.1/RAD, FMT_MTD.1/Signatory

manage the authentication function.

The Security Functional Requirement(s)

- "FIA_AFL.1/FixedLenPINRC"
  and
- "FIA_AFL.1/VarLenPINRC"
  and
- "FIA_AFL.1/PUK"
- **and**
- "FIA_AFL.1/T-PIN"

provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by FDP_SDI.2/DTBS ensures the integrity of stored DTBS and FDP_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature creation process).

Note:

1. The protection is defined by the standard which is required for a certain confirmation, see 8.2.2 Table of cryptographic mechanisms used

The PIN is set by the Signatory at phase OPERATIONAL using FMT_MTD.1/RAD.

The Transport PIN is stored using FDP_ACC.1/Config_DF_QES **and** FDP_ACF.1/Config_DF_QES.

The security functions specified by

- FDP_ACC.1/Signature-creation_SFP and FDP_ACF.1/Signature-creation_SFP

provide access control based on the security attributes managed according to the FMT_MSA.4 and

- SFR FMT_MTD.1/Signatory, FMT_MSA.2, FMT_MSA.3

The Security Functional Requirement(s)

- FMT_SMF.1 and FMT_SMR.1

list these management functions and the roles. These ensure that the signature process is restricted to the signatory.

- FMT_MOF.1 restricts the ability to enable the signature creation
- function to the signatory.
  FMT_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory.

9.1.2.8 OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE)

ensures that the DTBS/R is not altered by the TOE. The integrity functions specified by FDP_SDI.2/DTBS require that the DTBS/R has not been altered by the TOE.

9.1.2.9 OT.EMSEC_Design (Provide physical emanations security)

covers that no intelligible information is emanated. This is provided by FPT_EMS.1.1.

9.1.2.10 OT.Tamper_ID (Tamper detection)

is provided by FPT_PHP.1 by the means of passive detection of physical attacks.

9.1.2.11 OT.Tamper_Resistance (Tamper resistance)

is provided by FPT_PHP.3 to resist physical attacks.

9.2 Dependency Rationale for Security Functional Requirements

The following table provides an overview how the dependencies of the security functional requirements are solved. No dependencies are not satisfied.

Table 8: Functional Requirements Dependencies

Requirement	Dependencies	Fulfilled
FCS_CKM.1/EC	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/EC, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/EC, FCS_CKM.1/RSA
FCS_COP.1/EC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/EC, FCS_CKM.4
FCS_CKM.1/RSA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/RSA, FCS_CKM.4
FCS_COP.1/RSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/RSA, FCS_CKM.4
FCS_COP.1/SHA-2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	are not fulfilled but justified: see note (1) below
FCS_CKM.1/AuthScheme	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_CKM.4/AuthScheme, FCS_COP.1/3DES-ENC, FCS_COP.1/3DES-MAC, FCS_COP.1/AES-ENC, FCS_COP.1/AES-MAC
FCS_CKM.4/AuthScheme	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/AuthScheme
FCS_COP.1/3DES-ENC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/AuthScheme, FCS_CKM.4/AuthScheme
FCS_COP.1/3DES-MAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/AuthScheme, FCS_CKM.4/AuthScheme
FCS_COP.1/AES-ENC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/AuthScheme, FCS_CKM.4/AuthScheme
FCS_COP.1/AES-MAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/AuthScheme, FCS_CKM.4/AuthScheme
FDP_ACC.1/SCD/SVD_Generation_SFP	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation_SFP
FDP_ACC.1/Signature-creation_SFP	FDP_ACF.1	FDP_ACF.1/Signature-creation_SFP
FDP_ACC.1/SVD_Transfer_SFP	FDP_ACF.1	FDP_ACF.1/SVD_Transfer_SFP
FDP_ACF.1/SCD/SVD_Genera	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generatio

Requirement	Dependencies	Fulfilled
tion_SFP		n_SFP, FMT_MSA.3
FDP_ACF.1/Signature-creation_SFP	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature-creation_SFP, FMT_MSA.3
FDP_ACF.1/SVD_Transfer_SFP	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer_SFP, FMT_MSA.3
FDP_ACC.1/Config_DF_QES	FDP_ACF.1	FDP_ACF.1/Config_DF_QES
FDP_ACF.1/Config_DF_QES	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Config_DF_QES, FMT_MSA.3
FDP_RIP.1	No dependencies	n.a.
FDP_SDI.2/Persistent	No dependencies	n.a.
FDP_SDI.2/DTBS	No dependencies	n.a.
FTP_ITC.1/SM_ADS_Conf	No dependencies	n.a.
FIA_AFL.1/FixedLenPINRC	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/VarLenPINRC	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/PUK	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/AuthAdmin	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/T-PIN	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/SM	FIA_UAU.1	FIA_UAU.1
FIA_API.1/AuthScheme	No dependencies	n.a.
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD/SVD_Generation_SFP, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/RA-Terminal	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/Config_DF_QES, FDP_ACC.1/SVD_Transfer_SFP, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/Signature-creation_SFP, FMT_SMR.1,

Requirement	Dependencies	Fulfilled
		FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	FDP_ACC.1/SCD/SVD_Generation_SFP, FDP_ACC.1/Signature-creation_SFP, FDP_ACC.1/SVD_Transfer_SFP, FDP_ACC.1/Config_DF_QES, FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/RA-Terminal, FMT_MSA.1/Signatory
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Admin, FMT_MSA.1/RA-Terminal, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.4	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/SCD/SVD_Generation_SFP, FDP_ACC.1/Signature-creation_SFP
FMT_MTD.1/RAD	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1,
FMT_MTD.1/Signatory	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Ini-Data	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.
FPT_EMS.1	No dependencies	n.a.

Notes:

1. Justification of "FCS_COP.1/SHA-2" can be found in "FCS_COP.1/SHA-2 *Cryptographic operation - SHA-2 hash calculation*".

9.3 Rationale for EAL 4 Augmented

The assurance level for this protection profile is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. The TOE described in this protection profile is just such a product. Augmentation results from the selection of:

AVA_VAN.5 Advanced methodical vulnerability analysis

The TOE is intended to function in a variety of signature-creation systems for qualified electronic signatures. Due to the nature of its intended application, the TOE may be issued to users and may not be directly under the control of trained and dedicated Administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.

The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 Architectural Design with domain separation and non-bypassability
- ADV_FSP.4 Complete functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation of the TSF
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ATE_DPT.1 Testing: basic design

All of these dependencies are met or exceeded in the EAL4 assurance package.

10 TOE summary specification (ASE_TSS)

10.1 TOE Security Services

This chapter provides a description of the TOE's Security Services, which show how the TOE meets each SFR of "TOE Security Functional Requirements".

10.1.1 User Identification and Authentication

This Security Service is responsible for the identification and authentication of

- the RA-Terminal and the Signatory (FMT_SMR.1)

This implies that the TOE allows identification of the user before the authentication takes place (FIA_UAU.1). The TOE allows the execution of following TSF-mediated actions before the user is identified (FIA_UID.1), authenticated and associated with one of the roles:

- Self test according to FPT_TST.1

It is important that an attacker can not guess the RAD values by measuring or probing physical observables like TOE power consumption or electromagnetic radiation (FPT_EMS.1). Further protection functionality is covered by chapter "Protection" below.

The TOE is able to identify and authenticate users by

1. Performing of the Authentication Scheme
2. Entering of the Transport PIN
3. Entering of the Signatory RAD

cf FIA_UAU.1 and FIA_UID.1 but only the sequence as listed is possible.

Notes:

1. If the configuration does not need a PUK, the Signatory RAD consists of the Signatory PIN.
2. If the configuration needs a PUK, the Signatory RAD consists of the Signatory PIN and of Signatory PUK.

The security attributes used for policies are stated in Table 4: Security Attributes and related Status for the Subjects and Objects. Generally, the access control policy is assigned to user roles.

If the Authentication Scheme is not performed the Transport PIN and the Signatory PIN are not set. That means,

- it is not possible to enter successfully the Transport PIN
- it is not possible to enter successfully the Signatory PIN
- it is not possible to block both PINs with unsuccessful consecutive authentication attempts.

The Application for QES is deactivated.

If the Authentication Scheme is performed, the Transport PIN is set. That means,

- it is possible to enter successfully the Transport PIN
- it is possible to block the Transport PIN with unsuccessful consecutive authentication attempts
- it is not possible to enter successfully the Signatory PIN
- it is not possible to block the Signatory PIN with unsuccessful consecutive authentication attempts.

The Application for QES is prepared for activation.

If the Transport PIN is entered successfully and the Signatory PIN is set,

- it is possible to enter the Signatory PIN successfully
- it is possible to block the Signatory PIN with unsuccessful consecutive authentication attempts.

If a configuration needs a PUK,

- the conditions for the Signatory PIN also hold for the Signatory PUK.

The Application for QES is activated.

10.1.1.1 Authentication Scheme

The Authentication Scheme is used at phase OPERATIONAL to

- authenticate the RA-Terminal to the card and
- authenticate the TOE to the RA-Terminal

The Authentication Scheme used can be found in [CWA-14890-1], chapter "8.7 Symmetric authentication scheme. By reading the ICCSN first the RA-Terminal is able to retrieve the symmetric key data individual to the card for a specific card. By this symmetric key data individual to the card the RA-Terminal is able to authenticate himself to the card. The authentication of the RA-Terminal is ensured by FIA_AFL.1/AuthAdmin. Vice versa the card is able to authenticate itself to the RA-Terminal using FIA_API.1/AuthScheme. As a additional result of the Authentication Scheme the RA-Terminal and the card share a secret which consists of two 64 byte random numbers:

- K.IFD = random number of the terminal and
- K.ICC = random number of the chip.

This secret is used to set up SM by deriving session keys using FCS_CKM.1/AuthScheme. The session keys are destructed by FCS_CKM.4/AuthScheme after the Trusted Channel is no longer used. The Trusted Channel uses

- FCS_COP.1/3DES-ENC (encrypting and decrypting of the commands)
- FCS_COP.1/3DES-MAC (MACing of the commands)
  or
- FCS_COP.1/AES-ENC (encrypting and decrypting of the commands)
- FCS_COP.1/AES-MAC (MACing of the commands)

to avoid disclosure or modification.

The (ADS Configuration) symmetric key data used by the Authentication Scheme is stored by the Administrator at phase ADMINISTRATION using FMT_MTD.1/Ini-Data. This symmetric key data is individual to the card, it depends on the ICCSN.

Note:

1. If the Authentication Scheme is performed successfully for a specific card, the RA-Terminal is sure that this card is configured at phase OPERATIONAL by an Administrator. From this point of view the Authentication Scheme also is an acceptance procedure.

10.1.1.2 Phase OPERATIONAL: Administrator Identification and Authentication

Notes:

1. The StartKey secures the card within the life cycle phase MANUFACTURING.
   The Administrator is implicitly identified within the life cycle phase MANUFACTURING. Before the Administrator is able to start his work, the command sequence received by the TOE software developer has to be performed, since the initial StartKey (more exactly: the initial StartKey value of variable StartKey) is not known to the Administrator. The command sequence changes the secret StartKey (initial StartKey) to a default value ("default" in the sense of "the same value for each TC") which is known to the Administrator. It is mandatory that the Administrator change this default value to a value only known to him.
2. At this point the Administrator uses a personalization image to
   a) create the MF
   b) install objects and to import of a personalization authentication key for establishing a mutually authenticated Trusted Channel
   c) switch the card to phase OPERATIONAL.
   With switching to phase OPERATIONAL the TOE is delivered in the sense of CC.

After the card is switched to phase OPERATIONAL for the first time it is not possible to switch back to phase ADMINITRATION permanently. If a card is switch to phase ADMINISTRATION, it switches back to phase OPERATIONAL automatically after a reset.

At phase OPERATIONAL the Administrator performs

- second part of the Basic Configuration
- ADS Configuration.

The second part of Basic Configuration needs

- an authentication of the Administrator and vice versa the authentication of card to the Administrator using the personalization authentication key imported during first part of Basic Configuration
- establishing a Trusted Path

and then the Administrator

- switches the card to phase ADMINISTRATION
- installs all objects for Application for QES
- imports the (ADS Configuration) symmetric authentication key for the Authentication Scheme
- generates the key pair using SCD/SVD_Generation_SFP.

Note:

1. After the Basic Configuration is performed completely the personalization authentication key imported during first part of the Basic Configuration is no longer needed for any tasks concerning Application for QES. It has to be deleted.

The "SCD/SVD_Generation_SFP" is based on the security attribute "SCD/SVD Management" which is managed by

- FMT_MSA.2
- FMT_MSA.3
- FMT_MSA.1/Admin.

The generation of SCD/SVD pair is ensured by FDP_ACC.1/SCD/SVD_Generation_SFP and FDP_ACF.1/SCD/SVD_Generation_SFP.

The Administrator stores symmetric key data for the Authentication Scheme using

- FMT_MTD.1/Ini-Data

which stores also the domain parameters of an elliptic curve used for generating of the SCD/SVD in case of a configuration using an elliptic curve for signature generation.

At this time point the Application for QES is deactivated because object TPIN_QES is not usable (is in phase PROTECTED CREATION containing no value).

Note:

1. After a reset the card switches automatically back to phase OPERATIONAL.

10.1.1.3 Phase OPERATIONAL: RA-Terminal Identification and Authentication

This Security Service is responsible for identification and authentication of the RA-Terminal at phase OPERATIONAL.

Only an authenticated S.RA-Terminal associated with security attribute "SM-Connection" set to "established" is allowed to perform the ADS Configuration using

- SVD_Transfer_SFP
- DF_QES-Configuration_SFP.

The RA-Terminal is identified and authenticated after the Authentication Scheme is successfully performed, see 10.1.1.1 Authentication Scheme, which results additionally in session keys for establishing a Trusted Channel to avoid disclosure or modification of the ADS Configuration.

The Authentication Scheme and Trusted Channel have to be performed/established regardless of whether the ADS Configuration is performed using the Internet from the home PC of the end user or on-site at the RA.

The "DF_QES-Configuration_SFP" and "SVD_Transfer_SFP" are based on the security attribute "SM-Connection" which is managed by

- FMT_MSA.2
- FMT_MSA.3
- FMT_MSA.1/RA-Terminal.

The configuration of DF_QES is ensured by FDP_ACC.1/Config_DF_QES and FDP_ACF.1/Config_DF_QES. The export of the SVD is ensured by FDP_ACC.1/SVD_Transfer_SFP and FDP_ACF.1/SVD_Transfer_SFP.

After the Trusted Channel between the TOE and the RA-Terminal is establish successfully, the RA-Terminal performs

- the DF_QES-Configuration_SFP
- the SVD_Transfer_SFP

which are enabled by FTP_ITC.1/SM_ADS_Conf for local RA-Terminals on-site at RA and remote RA-Terminals performing these SFPs using the Internet.

The Trusted Channel is secured by

- FIA_AFL.1/SM

which terminates the association between the RA-Terminal and the Trusted Channel after a command is received not using the means of the Trusted Channel.

FDP_RIP.1 prevents misuse of any resources containing the symmetric key data used for the Authentication Scheme.

After the ADS Configuration is performed the Application for QES is transport protected because DF_QES-Configuration_SFP imports the value of the Transport PIN into object TPIN_QES with the result that the Transport PIN is usable from now on and the Signatory can set his RAD after he enters successfully the Transport PIN.

Notes:

1. After a reset the card switches automatically back to phase OPERATIONAL.
2. The RA-Terminal is able to perform ADS Configuration more than one time with the exception that the RA-Terminal cannot import a new Transport PIN. That means the RA-Terminal is able to create further EFs / DFs below DF_QES or it is able to update (all) created EFs / DFs below DF_QES (again) or he is able to remove (all) EFs / DFs below DF_QES.
3. The RA-Terminal is not able to remove DF_QES or to create / remove objects within DF_QES or to update other objects than TPIN_QES within DF_QES.

10.1.1.4 Signatory Identification and Authentication

Within the life cycle phase OPERATIONAL, the signatory is successfully authenticated after transmitting the correct VAD to the TOE, e.g. the user has to transmit the correct PIN to be associated with the role Signatory. The following type of VAD/RAD is defined for the TOE:

- PIN to authenticate the user as Signatory
- in case the configuration needs a PUK: PUK to unblock the Signatory PIN.

The number of unsuccessful consecutive authentication attempts by the user is limited. Thereafter this Security Service will block the RAD according to

- FIA_AFL.1/FixedLenPINRC if the retry counter shall not depend on the PIN's length (fixed RC)
- FIA_AFL.1/VarLenPINRC if the retry counter shall depend on the PIN's length (variable RC)
- FIA_AFL.1/PUK if the configuration needs a PUK.

The ability to create initially (FMT_MTD.1/RAD) and to modify (FMT_MTD.1/Signatory) the PIN of Signatory is restricted to the Signatory.

To modify PIN the Signatory has to provide

- the correct PIN to change resp. modify PIN or PIN length (in a specific interval which is set by the S.Admin by setting minimum and maximum length) (FMT_MTD.1/Signatory)

The individual PIN value is set by the Signatory (FMT_SMF.1 (1) + FMT_MTD.1/RAD).

If the configuration needs a PUK,

- FMT_MTD.1/RAD, FMT_MTD.1/Signatory and FMT_SMF.1 (1) also holds for the PUK.

Creation of the Signatory PIN has to be done immediately after the Transport PIN (T-PIN) is successfully entered. The Transport PIN is stored by the S.RA-Terminal (FDP_ACC.1/Config_DF_QES). The Transport PIN is secured by FIA_AFL.1/T-PIN which blocks the Transport PIN after too many unsuccessful consecutive authentication attempts by the user. In this case the TOE cannot be used anymore.

Note:

1. The value of the Transport PIN is not confidential.

The PIN is secured initially by the life cycle status (LCS) of it's object: it should be in phase PROTECTED CREATION containing no value. The SCA checks if the PIN is not set before. If so, the Transport Protection is already enabled. With the first setting of PIN the life cycle status is changed to OPERATIONAL ACTIVATED but the signatory is not authenticated (he cannot use the Signature-creation SFP after setting the PIN). If the Transport Protection is already disabled, the SCA informs the Signatory that

1. the card is not transport secured
2. he shall not use the card
3. he shall inform the Trust Center which hands out the card.

The SCA is a trustworthy application (A.SCA).

To set the PIN the Transport Protection has to be unlocked by entering the Transport PIN (T-PIN). The Transport PIN is delivered securely to the Signatory, e.g. by sending a Transport PIN letter or by displayed it during ADS Configuration.

Secure delivery to the end user

The Signatory enters his PIN only if

- the data he intends to sign (DTBS) is displayed correctly by the TOE environment.

If the data is not displayed correctly, the Signatory does not sign the data.

Signature-creation functionality of the TOE:

> The successful authentication with the PIN changes the value of the attribute "SCD operational" from "no" to "yes".

It is important that an attacker can not guess the RAD values by measuring or probing physical observables like TOE power consumption or electromagnetic radiation (FPT_EMS.1). Further protection functionality is covered by chapter "Protection" below.

If the configuration needs a PUK,

- conditions for creating / modifying the Signatory PIN holds also for the Signatory PUK
- a blocked PIN can be unblocked with the PUK (if the PUK is not blocked or if the use counter of the PUK is greater than zero)
- a blocked PUK cannot be unblocked or set
- if PUK's use counter is zero, it is not possible to unblock it or to set the use counter to a new value.

Note:

1. If a PUK is present, the PUK has a finite use counter.

10.1.2 Access Control provided by the Signature-creation_SFP

This Security Service is responsible for the signature creation.

Only a authenticated Signatory is allowed to generate a signature (RSA or EC based).

The security attributes used for this policy are stated in Table 4: Security Attributes and related Status for the Subjects and Objects. Generally, the access control policy is assigned to user roles. The identification, authentication and association of users to roles is realized by chapter 10.1.1 User Identification and Authentication; the description for the Signatory is contained in sub-chapter 10.1.1.4 Signatory Identification and Authentication.

This Security Service controls access to the signature-creation functionality of the TOE:

> The TOE allows generation of a signature if and only if (FDP_ACC.1/Signature-creation_SFP, FDP_ACF.1/Signature-creation_SFP and FMT_MOF.1 Management of security functions behaviour):
>
> 1. the security attribute "SCD operational" is set to "yes" (FMT_MSA.2 Secure security attributes).
> 2. the signature request is sent by an authorized Signatory, see also chapter 10.1.1.4 Signatory Identification and Authentication.

Before each single call of the SFP (i.e. before each creation of signature) the Signatory has to enter his PIN.

After the generation of the SCD/SVD key pair, the security attribute "SCD operational" is set to "no" (FMT_MSA.1/Admin, FMT_MSA.3 and FMT_MSA.4). Thereafter only the Signatory is allowed to modify the security attribute "SCD operational" (FMT_MSA.1/Signatory and FMT_SMF.1 (3)) depending on:

> The security attribute "SCD operational" can be set to "yes" by the TOE (FMT_MSA.1/Signatory and FMT_SMF.1 (3)) after the Signatory has successfully authenticated himself with the Transport PIN and unblocked his PIN, see also chapter 10.1.1.4 Signatory Identification and Authentication.

If the Transport Protection is already enabled, it is not possible to set the security attribute "SCD operational" to "yes" because the Signatory is not able to authenticate himself as Signatory.

10.1.3 Access Control provided by the SCD/SVD_Generation_SFP

This Security Service is responsible for the correct generation of the SCD/SVD key pair which is used by the Signatory to create signatures.

Only an authenticated S.Admin is allowed to generate a key pair (FDP_ACC.1/SCD/SVD_Generation_SFP and FDP_ACF.1/SCD/SVD_Generation_SFP).

The security attributes used for this policy are stated in Table 4: Security Attributes and related Status for the Subjects and Objects. Generally, the access control policy is assigned to user roles. The identification, authentication and association of users to roles is realized by chapter 10.1.1 User Identification and Authentication; the description for the Administrator is contained in sub-chapter 10.1.1.2 Phase OPERATIONAL: Administrator Identification and Authentication.

The generation is done with secure values for SCD/SVD parameters so that the key pairs fulfill the corresponding requirements of the standard as listed in [Infineon-ST-Chip-B11-2013-08-13] (ANSI X9.62-2005 and ISO/IEC 15946-1:2002) for EC key pairs (FMT_MSA.2 and FCS_CKM.1/EC). The TOE uses the Physical True RNG (PTRNG) of the underlying hardware for the generation of the SCD/SVD key pair. The generation is furthermore protected against electromagnetic emanation, simple power analysis (SPA) and timing attacks (FPT_EMS.1), see also chapter "Protection" below.

If a configuration uses RSA for the signature-creation function

- This holds also for FCS_CKM.1/RSA and standard as listed in [Infineon-ST-Chip-B11-2013-08-13] (PKCS1

v2.1 RFC3447) for RSA key pairs.

The generation of SCD/SVD pair is ensured by FDP_ACC.1/SCD/SVD_Generation_SFP and FDP_ACF.1/SCD/SVD_Generation_SFP. After generation of the SCD/SVD pair, no information of used resources is available (FDP_RIP.1) and the Signatory is informed if stored data is altered (FDP_SDI.2/Persistent).

The SCD is identified by security attribute "SCD identifier". The security attribute "SCD identifier" may have arbitrary values (FMT_SMF.1). The Administrator can set/change security attribute "SCD identifier" to a desired value (FMT_SMF.1 (4)). The Administrator is thus able to override the default values when an object or information (here: SCD) is created (FMT_MSA.3).

In configuring DF_QES, S.Admin can set/change security attribute "SCD identifier" to a desired value (FMT_SMF.1 (4)) and thus is able to override the default values when an object or information (here: SCD) is created (FMT_MSA.3).

In case of signature generation with elliptic curves the Administrator stores the domain parameters of an elliptic curve used for generating of the SCD / SVD using

- FMT_MTD.1/Ini-Data (2).

Optional a key pair can be destructed by overwriting it with zeros (FCS_CKM.4) on demand of the Signatory at phase OPERATIONAL, e.g. after the (qualified) certificate for the corresponding SVD has been expired.

Note:

1. It must not be possible to generate key pairs based on an elliptic curve and on RSA in a single configuration.

10.1.4 Access Control provided by the SVD_Transfer_SFP

This Security Service is responsible for the transfer of the SVD and is performed by an RA-Terminal at phase OPERATIONAL.

Only an authenticated S.RA-Terminal associated with security attribute "SM-Connection" set to "established" is allowed to transfer public key data (FDP_ACC.1/SVD_Transfer_SFP and FDP_ACF.1/SVD_Transfer_SFP.

The security attributes used for this policy are stated in Table 4: Security Attributes and related Status for the Subjects and Objects. Generally, the access control policy is assigned to user roles. The identification, authentication and association of users to roles is realized by chapter 10.1.1 User Identification and Authentication; the description for the RA-Terminal is contained in sub-chapter 10.1.1.3 Phase OPERATIONAL: RA-Terminal Identification and Authentication.

The export of the SVD is ensured by FDP_ACC.1/SVD_Transfer_SFP and FDP_ACF.1/SVD_Transfer_SFP. An export becomes necessary after a generation of a key pair to generate a new qualified certificate which is afterward optionally stored on the card.

FMT_MSA.2 (Secure security attributes) ensures that security attribute "SM-Connection" is only used in secure combinations.

Generally this SFP is used when

- the RA-Terminal finishes the configuration of DF_QES

but it can be used more than one time.

10.1.5 Access Control provided by the DF_QES-Configuration_SFP

This Security Service is responsible for

- optionally creation / deletion of EFs and DFs
- optionally updating these files, e.g. with the (qualified) certificate and of the certificate of the Certification Authority

- importing of the value of the Transport PIN which transport protects Application for QES

and is performed by an RA-Terminal at phase OPERATIONAL.

Only an authenticated S.RA-Terminal associated with security attribute "SM-Connection" set to "established" is allowed to configure application for QES (FDP_ACC.1/Config_DF_QES and FDP_ACF.1/Config_DF_QES.

The security attributes used for this policy are stated in Table 4: Security Attributes and related Status for the Subjects and Objects. Generally, the access control policy is assigned to user roles. The identification, authentication and association of users to roles is realized by chapter 10.1.1 User Identification and Authentication; the description for the RA-Terminal is contained in sub-chapter 10.1.1.3 Phase OPERATIONAL: RA-Terminal Identification and Authentication.

The configuration of DF_QES is ensured by FDP_ACC.1/Config_DF_QES and FDP_ACF.1/Config_DF_QES.

FMT_MSA.2 (Secure security attributes) ensures that security attribute "SM-Connection" is only used in secure combinations.

Generally this SFP is used when

- the RA-Terminal finishes the configuration of DF_QES

but it can be used more than one time with exception of the import of the Transport PIN.

10.1.6 Signature Creation

This Security Service is responsible for signature creation (FCS_COP.1/EC) using the SCD of the signatory. Before a signature is generated by the TOE, the signatory has to be authenticated successfully, see 10.1.1.4 Signatory Identification and Authentication.

The signatory is informed if stored data is altered (FDP_SDI.2/Persistent and FDP_SDI.2/DTBS).

If a configuration uses RSA for the signature-creation function

- This holds also for FCS_COP.1/RSA instead of FCS_COP.1/EC.

Note:

1. It must not be possible to generate signatures based on an elliptic curve and on RSA in a single configuration.

10.1.6.1 Signature Creation with EC

Technically, this Security Service generates EC signatures for hash values using the SCD of the signatory (FCS_COP.1/EC). The signatures generated by this Security Service meet the following standards:

- ANSI X9.62 - 2005, section 7.3
  ISO/IEC 15946-2:2002, sections 6.2 (6.2.2. + 6.2.3)
  see [Infineon-ST-Chip-B11-2013-08-13], 7.1.4.7 Elliptic Curve DSA (ECDSA) operation.

because this TOE uses the EC crypto library of the underlying chip SLE78CFX*P (M7892 B11).

The Security Service supports EC key length of 256 and 384 bits (FCS_COP.1/EC).

10.1.6.2 Signature Creation with RSA

Technically, this Security Service generates EC signatures for hash values with PKCS1 block type 1 or PSS padding using the SCD of the signatory (FCS_COP.1/RSA). The signatures generated by this Security Service meet the following standards:

- RSASP1 in PKCS1 v2.1 RFC3447
  see [Infineon-ST-Chip-B11-2013-08-13], 7.1.4.4 Rivest-Shamir-Adleman (RSA) operation

because this TOE uses the RSA crypto library of the underlying chip SLE78CFX*P (M7892 B11). The padding is done according to RSASSA-PSS and RSASSA-PKCS1-v1_5.

The Security Service supports RSA key length of 2048 - 4096 bits (FCS_COP.1/RSA).

10.1.6.3 TOE IT environment generated hash values

The hash value used for the signature creation is calculated over the DTBS in the TOE IT environment and sent to the TOE under the control of the Signature-creation_SFP, see 10.1.2 Access Control provided by the Signature-creation_SFP.

The signature creation process is implemented in a way which does not disclose the SCD by measuring the IC power consumption of the TOE during the signature calculation (FPT_EMS.1). It is furthermore not possible to gain unauthorized access to the SCD using the physical contacts of the underlying hardware. The certificate [BSI-DSZ-CC-0782-2012-MA-01] of the chip SLE78CFX*P (M7892 B11) (Common Criteria level EAL 6+) covers the EC functionality and RSA functionality for signature creation.

10.1.6.4 TOE generated hash values

In case that DTBS instead of a hash value (DTBS/R) is sent to the TOE under the control of the Signature-creation SFP, see 10.1.2 Access Control provided by the Signature-creation_SFP, the TOE directly generates a hash value over the sent DTBS first (FCS_COP.1/SHA-2 + FMT_SMF.1) which is used afterward for the signature creation.

The signature creation process is implemented in a way which does not disclose the SCD by measuring the IC power consumption of the TOE during the signature calculation (FPT_EMS.1). It is furthermore not possible to gain unauthorized access to the SCD using the physical contacts of the underlying hardware. The certificate [BSI-DSZ-CC-0782-2012-MA-01] of the chip SLE78CFX*P (M7892 B11) (Common Criteria level EAL 6+) cover the EC functionality and RSA functionality for signature creation.

Note:

1. This TOE uses SHA-384 provided by CardOS V5.3.

10.1.6.5 Hash last round

In case that the hash value (DTBS/R) is only partly computed in the IT environment an intermediate hash value with the remainder of DTBS is sent to the TOE under the control of the Signature-creation SFP, see 10.1.2 Access Control provided by the Signature-creation_SFP. The TOE first computes the 'last round(s)' over the remainder of DTBS and the intermediate hash value (FCS_COP.1/SHA-2 + FMT_SMF.1). The final hash value is used afterward for the signature creation.

The signature creation process is implemented in a way which does not disclose the SCD by measuring the IC power consumption of the TOE during the signature calculation (FPT_EMS.1). It is furthermore not possible to gain unauthorized access to the SCD using the physical contacts of the underlying hardware. The certificate [BSI-DSZ-CC-0782-2012-MA-01] of the chip SLE78CFX*P (M7892 B11) (Common Criteria level EAL 6+) cover the EC functionality and RSA functionality for signature creation.

Notes:

1. This TOE uses SHA-384 provided by CardOS V5.3.
2. Last round hash values may be used if a signature for large data shall be generated because the IT environment is able to hash much faster than the card.

10.1.7 Protection

This Security Service is responsible for the protection of the TSF, TSF data and user data. The TOE runs a suite of tests to demonstrate the correct operation of the security assumptions provided by the IC platform that underlies the TSF. The following tests are performed during initial start-up (FPT_TST.1):

- The SLE78CFX*P (M7892 B11) provides a high security initialization software concept. The self test software (STS) is activated by the chip after a cold or warm reset (ISO-reset with I/O=1). It contains diagnostic routines for the chip, see [Infineon-Chip-HW-Ref], chapter 8.
- After erasure of RAM the state of the User EEPROM is tested and, if not yet initialized, this will be done.
- The User EEPROM heap is checked for consistency. If it is not valid, the TOE will preserve a secure state (life cycle DEATH).
- The backup buffer is checked and its data is restored to User EEPROM, if they were saved because of a command interruption.
- The integrity of stored TSF executable code is verified. If this check fails, the TOE will preserve a secure state (life cycle DEATH).
- The integrity of stored data (objects and files) is verified before their use.
- The hardware sensors, the symmetric coprocessor and the random number generator are tested. If one of the tests fails, the chip platform will perform a security reset.

The TOE will furthermore run tests during the generation of the SCD/SVD key pair (10.1.3 Access Control provided by the SCD/SVD_Generation_SFP) (FPT_TST.1.1 (1)) and during signature creation ("Signature Creation") (FPT_TST.1.1 (2)). For tests during signature creation the code of the Infineon Crypto Library (Crypto Library for SLE78CFX*P (M7892 B11)) is used. The correct operation of 10.1.3 Access Control provided by the SCD/SVD_Generation_SFP is demonstrated by performing the following checks:

- The TOE's life cycle phase is checked. Only S.Admin can perform SCD/SVD pair generation.
- Before a random number from the PTRNG is used for the generation of the SCD/SVD key pair the correct functioning of the random number generator is checked by reading out the status register of PTRNG.
- All command parameters are checked for consistency.
- Access rights are checked.

If a critical failure occurs during these tests, the TOE will preserve a secure state (FPT_FLS.1). This comprises the following types of failures:

- Failure of sensors
- Failure of Active Shield
- Failure of cryptographic operation, e.g. during signature creation
- Memory failures during TOE execution

The TOE will also run tests before command execution for VAD verification (FPT_TST.1.1 (3)), RAD modification (FPT_TST.1.1 (4)) and RAD unblocking (FPT_TST.1.1 (5)).

The TOE is furthermore able to detect physical or mechanical tampering attempts (FPT_PHP.1). This comprises tampering attempts before start-up and during operation. If the underlying IC hardware is attacked by physical or mechanical means, the TOE will respond automatically in form of a continuously generated reset and the TOE functionality will be blocked (FPT_PHP.3).

This Security Service actively destroys temporarily stored SCD, VAD and RAD immediately after their use - as soon as these data are dispensable (FDP_RIP.1).

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

- SCD
- SVD
- RAD
- Symmetric key data for the Authentication Scheme

If the integrity of SCD, SVD, RAD or symmetric key data for Authentication Scheme is violated, the TOE will prohibit the usage of the altered data and inform the signatory about the integrity error by means of an error code (FDP_SDI.2/Persistent).

The TOE protects itself against interference and logical tampering by the following measures:

Each application removes its own data from the used memory area at the latest after execution of a command.

- Clearance of sensitive data, as soon as possible (when they are dispensable)

- No parallel but only serial execution of commands
- Encapsulation of context data (security relevant status variables, etc.)
- Use of the chips MMU (Memory Management Unit)
- Separation of User ROM and Test ROM, where the chip's self test software is located, and to which entries are not possible (apart from cold or warm reset)

The TOE protects itself against bypass by not allowing any function in the TSF to proceed if a prior security enforcement function was not executed successfully. The TOE always checks that the appropriate user is successfully authenticated (cf. 10.1.1 User Identification and Authentication) for a certain action.

10.2 Usage of Platform TSF by TOE TSF

The relevant SFRs (RP_SFR) of the platform being used by the Composite ST are listed in the following table:

Table 9: Relevant Platform SFRs used by Composite ST

RP_SFR	Meaning	Used by TOE SFR
FRU_FLT.2	Limited Fault Tolerance	FPT_TST.1
FPT_FLS.1	Failure with Preservation of Secure State	FPT_FLS.1
FPT_PHP.3	Resistance to Physical Attack	FPT_PHP.3
FDP_ITT.1	Basic Internal Transfer Protection	FPT_EMS.1
FDP_IFC.1	Subset Information Flow Control	FPT_EMS.1
FPT_ITT.1	Basic Internal TSF Data Transfer Protection	FPT_EMS.1
FCS_RNG.1	Quality Metric for Random Numbers	FCS_CKM.1/EC (EC Key Pair generation) FCS_COP.1/RSA (RSA Key Pair generation) FCS_COP.1/EC (EC based Signature generation) FCS_CKM.1/AuthScheme (Exchange of random numbers by the TOE and the RA-Terminal) FPT_EMS.1 (blinding)
FPT_TST.2	Subset TOE Security Testing	FPT_TST.1 FPT_PHP.3 (active shield and sensors)
FCS_CKM.1/EC	Cryptographic key generation	FCS_CKM.1/EC
FCS_COP.1/ECDSA	Cryptographic Support (ECDSA)	FCS_COP.1/EC
FCS_CKM.1/RSA	Cryptographic Key Generation (RSA)	FCS_CKM.1/RSA
FCS_COP.1/RSA	Cryptographic Support (RSA)	FCS_COP.1/RSA

RP_SFR	Meaning	Used by TOE SFR
FCS_COP.1/DES	Cryptographic Support (3DES)	FCS_COP.1/3DES-ENC, FCS_COP.1/3DES-MAC
FCS_COP.1/AES	Cryptographic Support (AES)	FCS_COP.1/AES-ENC, FCS_COP.1/AES-MAC
FCS_COP.1/SHA	Cryptographic Support (SHA-2) | FCS_COP.1/SHA-2	
FDP_SDI.2	Stored Data Integrity Monitoring and Action | FDP_SDI.2/Persistent	
FDP_ACC.1	Subset Access Control	no conflicts with TSF
FDP_ACF.1	Security Attribute Based Access Control	no conflicts with TSF
FMT_MSA.3	Static Attribute Initialisation	no conflicts with TSF

The irrelevant SFRs (IP_SFR) of the platform not being used by the Composite ST are listed in the following table:

Table 10: Irrelevant Platform SFRs not being used by Composite ST

IP_SFR	Meaning	Comment
FDP_SDI.1	Stored Data Integrity Monitoring	Not used by TSF
FMT_LIM.1	Limited Capabilities	Not used by TSF
FMT_LIM.2	Limited Availability	Not used by TSF
FAU_SAS.1	Audit Storage	Not used by TSF
FMT_MSA.1	Management of Security Attributes	Not used by TSF
FMT_SMF.1	Specification of Management Functions	Not used by TSF
FCS_COP.1/ECDH	Cryptographic key generation	Not used by TSF

There is no conflict between the security problem definition, the security objectives and the security requirements of the current Composite Security Target and the Platform Security Target (security target of the controller SLE78CFX*P (M7892 B11)). All related details (operations on SFRs, definition of security objectives, threats etc.) can be found in both the documents.

10.3 Assumptions of Platform for its Operational Environment

Table 11: Categorization of the assumptions of Platform for its Operational Environment

Assumptions of the hardware platform related to its operational environment	Short Description	Categorization	Comment
inherited from [BSI-PP-0035]:			
A.Plat-Appl	Usage of Hardware Platform: The Security IC Embedded Software is designed so that requirements from the following documents are met: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as documented in the certification report.	automatically fulfilled (CfPA)	Will be automatically fulfilled by the technical design and the implementation
A.Resp-Appl	Treatment of User Data: All User Data is owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) is treated by the Security IC Embedded Software as defined for its specific application context.	automatically fulfilled (CfPA)	Can be mapped at least to the following security objectives for the Composite-TOE: OT.EMSEC_Design OT.SCD_Secrecy OT.Sigy_SigF OT.Tamper_Resistance
A.Process-Sec-IC	Protection during Packaging, Finishing and Configuration: It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy,	automatically fulfilled (CfPA)	Will automatically be fulfilled by application of the security assurance requirements of the families ALC_DVS and ALC_DEL

Assumptions of the hardware platform related to its operational environment	Short Description	Categorization	Comment
inherited from [BSI-PP-0035]:			
	modification, retention, theft or unauthorized use).		
dedicatedly defined in [Infineon-ST-Chip-B11-2013-08-13]			
A.Key-Function	Usage of Key-dependent Functions: Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak- Inherent and T.Leak- Forced).	automatically fulfilled (CfPA)	Can be mapped at least to the following security objectives for the Composite-TOE: OT.EMSEC_Design OT.SCD_Secrecy