Security Target 'CardOS V5.0 with Application for QES V1.0', Rev. 2.00, Edition 03/2013

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....6
2 About this Document....7
2.1 References....7
2.1.1 General References....7
2.1.2 Common Evaluation Evidence....8
2.2 Tables....9
2.3 Acronyms....9
2.4 Terms and Definitions....10
2.4.1 Security Evaluation Terms....11
2.4.2 Technical terms....11
3 Security Target Introduction (ASE_INT)....15
3.1 ST Reference....15
3.2 TOE Reference....15
3.3 TOE overview....16
3.4 TOE description....17
4 Conformance Claims (ASE_CCL)....25
4.1 CC Conformance Claim....25
4.2 PP Claim, Package Claim....25
4.3 Conformance Rationale....26
4.3.1 PP Claims Rationale....26
5 Security Problem Definition (ASE_SPD)....27
5.1 General....27
5.1.1 Assets and objects....27
5.1.2 User and subjects acting for users....27
5.1.3 Threat agents....27
5.2 Threats....27
5.2.1 T.SCD_Divulg (Storing, copying, and releasing of the signature-creation data)....27
5.2.2 T.SCD_Derive (Derive the signature-creation data)....28
5.2.3 T.Hack_Phys (Physical attacks through the TOE interfaces)....28
5.2.4 T.SVD_Forgery (Forgery of the signature-verification data)....28
5.2.5 T.SigF_Misuse (Misuse of the signature-creation function of the TOE)....28
5.2.6 T.DTBS_Forgery (Forgery of the DTBS/R)....28
5.2.7 T.Sig_Forgery (Forgery of the digital signature)....28
5.2.8 T.Hash_Misuse (Misuse of the hash generation function of the TOE)....28
5.3 Organizational Security Policies....28
5.3.1 P.CSP_QCert (Qualified certificate)....28
5.3.2 P.QSign (Qualified electronic signatures)....29
5.3.3 P.Sigy_SSCD (TOE as secure signature-creation device)....29
5.3.4 P.Sig_Non-Repud (Non-repudiation of signatures)....29
5.4 Assumptions....29
5.4.1 A.CGA (Trustworthy certification-generation application)....29
5.4.2 A.SCA (Trustworthy signature-creation application)....29
5.4.3 A.Env_Admin (Environment for administrator)....29
5.4.4 A.Env_Mass_Signature (Environment for a mass signature TOE)....29
6 Security Objectives (ASE_OBJ)....30
6.1 General....30
6.2 Security Objectives for the TOE....30
6.2.1 OT.Lifecycle_Security (Lifecycle security)....30
6.2.2 OT.SCD/SVD_Gen (SCD/SVD generation)....30
6.2.3 OT.SCD_Unique (Uniqueness of the signature-creation data)....30
6.2.4 OT.SCD_SVD_Corresp (Correspondence between SVD and SCD)....30
6.2.5 OT.SCD_Secrecy (Secrecy of the signature-creation data)....30
6.2.6 OT.Sig_Secure (Cryptographic security of the digital signature)....30
6.2.7 OT.Sigy_SigF (Signature creation function for the legitimate signatory only)....31
6.2.8 OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE)....31
6.2.9 OT.EMSEC_Design (Provide physical-emanation security)....31
6.2.10 OT.Tamper_ID (Tamper detection)....31
6.2.11 OT.Tamper_Resistance (Tamper resistance)....31
6.3 Security Objectives for the Operational Environment....31

6.3.1 OE.SVD_Auth (Authenticity of the SVD) **31**
6.3.2 OE.CGA_QCert (Generation of qualified certificates) **31**
6.3.3 OE.SSCD_Prov_Service (Authentic SSCD provided by SSCD provisioning service) **31**
6.3.4 OE.HID_VAD (Protection of the VAD) **31**
6.3.5 OE.DTBS_Intend (SCA sends data intended to be signed) **32**
6.3.6 OE.DTBS_Protect (SCA protects the data intended to be signed) **32**
6.3.7 OE.Signatory (Security obligation of the signatory) **32**
6.3.8 OE.Attester (Security obligation of the attester for signatures with 4EP) **32**
6.3.9 OE.Env_Admin (Administrator works in trusted environment) **32**
6.3.10 OE.Env_Mass_Signature (Mass signatures are generated in trusted environment only) **32**
6.4 Security Objectives Rationale **32**
6.4.1 Security Objectives Coverage **33**
6.4.2 Security Objectives Sufficiency **33**
6.4.2.1 Policies and Security Objective Sufficiency **34**
6.4.2.2 Threats and Security Objective Sufficiency **36**
6.4.2.3 Assumptions and Security Objective Sufficiency **37**
7 Extended Component Definition (ASE_ECD) **38**
7.1 FPT_EMSEC.1 TOE Emanation **38**
8 IT Security Requirements (ASE_REQ) **40**
8.1 General **40**
8.2 TOE Security Functional Requirements **40**
8.2.1 Use of requirement specifications **40**
8.2.2 Part ONE (general SFRs) **40**
8.2.2.1 Cryptographic support (FCS) **40**
8.2.2.1.1 FCS_CKM.1/RSA Cryptographic key generation 40
8.2.2.1.2 FCS_COP.1/RSA Cryptographic operation 41
8.2.2.1.3 FCS_COP.1/SHA-2 Cryptographic operation 41
8.2.2.2 User data protection (FDP) **42**
8.2.2.2.1 FDP_ACC.1/SCD/SVD_Generation_SFP Subset access control 42
8.2.2.2.2 FDP_ACF.1/SCD/SVD_Generation_SFP Security attribute based access control 42
8.2.2.2.3 FDP_ACC.1/SVD_Transfer_SFP Subset access control 43
8.2.2.2.4 FDP_ACF.1/SVD_Transfer_SFP Security attribute based access control 43
8.2.2.2.5 FDP_RIP.1 Subset residual information protection 43
8.2.2.2.6 FDP_SDI.2/Persistent Stored data integrity monitoring and action 44
8.2.2.2.7 FDP_SDI.2/DTBS Stored data integrity monitoring and action 44
8.2.2.3 Identification and authentication (FIA) **44**
8.2.2.3.1 FIA_UID.1 Timing of identification 44
8.2.2.3.2 FIA_UAU.1 Timing of authentication 45
8.2.2.3.3 FIA_AFL.1/Transport_PIN Authentication failure handling 45
8.2.2.3.4 FIA_AFL.1/PUK Authentication failure handling 45
8.2.2.4 Security management (FMT) **46**
8.2.2.4.1 FMT_MSA.1/Admin Management of security attributes 46
8.2.2.4.2 FMT_MSA.4 Security attribute value inheritance 46
8.2.2.4.3 FMT_MTD.1/Admin Management of TSF data 46
8.2.2.5 Protection of the TSF (FPT) **47**
8.2.2.5.1 FPT_EMSEC.1 TOE Emanation 47
8.2.2.5.2 FPT_FLS.1 Failure with preservation of secure state 47
8.2.2.5.3 FPT_PHP.1 Passive detection of physical attack 47
8.2.2.5.4 FPT_PHP.3 Resistance to physical attack 47
8.2.2.5.5 FPT_TST.1 TSF testing 48
8.2.3 Part TWO (SFRs according to signatures without four eyes principle) **48**
8.2.3.1 User data protection (FDP) **48**
8.2.3.1.1 FDP_ACC.1/Signature-creation_SFP Subset access control 49
8.2.3.1.2 FDP_ACF.1/Signature-creation_SFP Security attribute based access control 49
8.2.3.2 Security management (FMT) **49**
8.2.3.2.1 FMT_MSA.1/Signatory Management of security attributes 49
8.2.3.2.2 FMT_MSA.3 Static attribute initialization 50
8.2.3.2.3 FMT_SMF.1 Security management functions (signatures without 4EP) 50
8.2.3.2.4 FMT_SMR.1 Security roles for signature without 4EP 50
8.2.3.2.5 FMT_MOF.1 Management of security functions behavior without 4EP 51
8.2.3.2.6 FMT_MSA.2 Secure security attributes without 4EP 51
8.2.3.3 Identification and authentication (FIA) **51**

8.2.3.3.1 FIA_UAU.6/without_4EP Re-authenticating on Signature without 4EP....52
8.2.4 Part THREE (SFRs based on German QES)....52
8.2.4.1 Identification and authentication (FIA)....52
8.2.4.1.1 FIA_AFL.1/PIN Authentication failure handling....52
8.2.4.2 Security management (FMT)....52
8.2.4.2.1 FMT_MTD.1/Signatory Management of TSF data....52
8.2.4.2.2 FMT_MTD.1/Signatory_PIN_T Management of TSF data....53
8.2.5 Part FOUR (SFRs according to QES-Switzerland only)....53
8.2.5.1 Identification and authentication (FIA)....53
8.2.5.1.1 FIA_AFL.1/Swiss_PIN Authentication failure handling....53
8.2.5.2 Security management (FMT)....53
8.2.5.2.1 FMT_MTD.1/Swiss_Signatory_Modifying Management of TSF data....53
8.2.5.2.2 FMT_MTD.1/Swiss_Signatory_Unblocking Management of TSF data....54
8.2.5.2.3 FMT_MTD.1/Swiss_Admin Management of TSF data....54
8.2.5.2.4 FMT_MTD.1/Swiss_Admin_PIN_T Management of TSF data without 4EP....54
8.2.6 Part FIVE (SFRs according to QES-Two-PIN-Signatures)....55
8.2.6.1 User data protection (FDP)....55
8.2.6.1.1 FDP_ACC.1/4EP_Mass_Signature-creation_SFP Subset access control....55
8.2.6.1.2 FDP_ACF.1/4EP_Mass_Signature-creation_SFP Security attribute based access control....55
8.2.6.2 Identification and authentication (FIA)....56
8.2.6.2.1 FIA_UAU.6/with_4EP Re-authenticating on Signature with 4EP....56
8.2.6.3 Security management (FMT)....56
8.2.6.3.1 FMT_MSA.3/4EP_Mass_Signature Static attribute initialization for 4EP mass signature 56
8.2.6.3.2 FMT_SMF.1/with_4EP Security management functions for signatures with 4EP....57
8.2.6.3.3 FMT_SMR.1/with_4EP Security roles for Mass_Signature with 4EP....57
8.2.6.3.4 FMT_MTD.1/Attester Management of TSF data....57
8.2.6.3.5 FMT_MTD.1/Attester_PIN_T Management of TSF data....58
8.2.6.3.6 FMT_MOF.1/4EP_Mass_Signature Management of security functions behavior for 4EP_Mass_Signature....58
8.2.6.3.7 FMT_MSA.1/Signatory_Attester Management of security attributes....58
8.2.6.3.8 FMT_MSA.2/4EP_Mass_Signature Secure security attributes for 4EP_Mass_Signature...59
8.3 TOE Security Assurance Requirements....59
9 Rationale....61
9.1 Security Requirements Rationale....61
9.1.1 Security Requirement Coverage....61
9.1.2 TOE Security Requirements Sufficiency....63
9.1.2.1 Different possibilities to create signatures....68
9.1.2.2 Different reasons for authentication....69
9.2 Dependency Rationale for Security Functional Requirements....69
9.3 Rationale for EAL 4 Augmented....73
10 TOE summary specification (ASE_TSS)....74
10.1 TOE Security Services....74
10.1.1 SS1 User Identification and Authentication....74
10.1.2 SS2 Access Control....78
10.1.3 SS3 SCD/SVD Pair Generation....80
10.1.4 SS4 Signature Creation....81
10.1.4.1 Signature Creation with RSA....81
10.1.4.2 TOE IT environment generated hash values....81
10.1.4.3 TOE generated hash values....82
10.1.5 SS5 Protection....82
10.2 Usage of Platform TSF by TOE TSF....83
10.3 Assumptions of Platform for its Operational Environment....85

1 History and Indices

Revision History:

2.00	2013-03-27	Release Version

2 About this Document

2.1 References

2.1.1 General References

[AIS36]

Anwendungshinweise und Interpretationen zum Schema, AIS36: ETR-lite für zusammengesetzte EVGs, Version 1, 29.07.2002, Bundesamt für Sicherheit in der Informationstechnik

[CC-3.1-P1]

Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model; Version 3.1 Revision 3 July 2009, CCMB-2009-07-001

[CC-3.1-P2]

Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements; Version 3.1 Revision 3 July 2009, CCMB-2009-07-002

[CC-3.1-P3]

Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements; Version 3.1 Revision 3 July 2009, CCMB-2009-07-003

[CEM-3.1]

Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009, CCMB-2009-07-004

[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 30. Dezember 2011, Veröffentlicht am 18. Januar 2012 im Bundesanzeiger Nr. 10, Seite 243 Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

[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)

[QES-Germany-SigG]

Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001 (BGBl. I S.876 ff)

[QES-Germany-SigV]

Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) vom 16.November 2001 BGBl.I S.3074ff)

[QES-Swiss-SigGesetz]

Bundesamt für Kommunikation BAKOM, Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur, SR 943.032.1 / Anhang, Ausgabe 4: 8.7.2011

[RSA-PKCS1-v2.1]

RSA Laboratories, PKCS #1 v2.1: RSA Encryption Standard, RSA Laboratories, June 14th, 2002

2.1.2 Common Evaluation Evidence

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

[ADS-Descr-CardOS50]

ADS Description 'CardOS V5.0 with Application for QES V1.0', Atos IT Solutions and Services GmbH

[Administrator-Guidance-V50]

Administrator Guidance 'CardOS V5.0 with Application for QES V1.0', Atos IT Solutions and Services GmbH

[BSI-CC-PP-0035-2007]

Certification Report BSI-CC-PP-0035-2007 for Security Protection Profile V1.0.

[BSI-PP-0006-2002T]

Protection Profile Secure Signature-Creation Device Type 3, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0006-2002T, also short SSVG-PPs or CWA14169

[BSI-PP-0035]

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

[BSI-CF-PP0059-2009]

Certification Report BSI-CC-PP-0059-2009 for Protection Profiles for Secure Signature Creation Device - Part 2: Device with Key Generation, Version 1.03 from CEN/ISSS - Information Society Standardization System. 11 December 2009.

[BSI-PP0059-2009]

Protection profiles for Secure signature creation device - Part 2: Device with key generation, prEN 14169-1:2009

[CardOS50-PR-Notes]

CardOS V5.0 Chipcard Operating System, Packages & Release Notes, Atos IT Solutions and Services GmbH

[Chip-Data-Book]

M7892 Controller Family for Security Applications - Hardware Reference Manual Revision 1.2 2011-12-12 and Errata Sheet 2012-02-27

[CF-IFX-Chip-A21]

Certification Report BSI-DSZ-CC-0758-2012 for Infineon Security Controller M7892 A21 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG

[ST-IFX-Chip-B11-Maint]

Security Target Lite Maintenance 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 1.2, Date 2012-07-24, Infineon Technologies AG

[CF-IFX-Chip-B11-MaintRep]

Assurance Continuity Maintenance Report, BSI-DSZ-CC-0758-2012-MA-01, Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG

[User-Guidance-V50]

User Guidance 'CardOS V5.0 with Application for QES V1.0', Atos IT Solutions and Services GmbH

[Users-Manual-V50]

CardOS V5.0 Chipcard Operating System, User's Manual, Atos IT Solutions and Services GmbH

2.2 Tables

Table 1: Components of the TOE

Table 2: Security problem definition to security objectives mapping

Table 3: Security Attributes and related Status for the Subjects and Objects (in case of signatures without 4EP)

Table 4: Secure Values of the Combinations for Signatures without 4EP

Table 5: Security Attributes and related Status for the Subjects and Objects (in case of signatures with 4EP)

Table 6: Secure Values of the Combinations for 4EP_Mass_Signature

Table 7: Assurance Requirements: EAL4 augmented with AVA_VAN.5

Table 8: Functional Requirement to TOE security objective mapping

Table 9: Functional Requirements Dependencies

Table 10: Relevant Platform SFRs used by Composite ST

Table 11: Irrelevant Platform SFRs not being used by Composite ST

Table 12: Categorization of the assumptions of Platform for its Operational Environment

2.3 Acronyms

4EP
: Four Eyes Principle

ADS
: Application Digital Signature

APDU
: Application Protocol Data Unit

CC
: Common Criteria

CfPA
: Composite-fulfilled Platform Assumption

CGA
: Certification Generation Application

CSF
: CardOS Sequence Format

DPA
: Differential Power Analysis

DTBH
: Data to be hashed

DTBS
: Data to be signed

DTBS/R

Representation of DTBS

EAL
: Evaluation Assurance Level

IC
: Integrated Circuit

ICC
: IC Card

IP_SFR
: Irrelevant Platform SFR

IT
: Information Technology

MAC
: Message Authentication Code

PIN
: Personal Identification Number

PP
: Protection Profile

PUK
: Personal Unblocking Key

QES
: Qualified Electronic Signature

RAD
: Reference Authentication Data

RP_SFR
: Relevant Platform SFR

SCA
: Signature Creation Application

SCD
: Signature Creation Data

SCIC
: Smart Card IC

SDO
: Signed Data Object

SFP
: Security Function Policy

SFR
: Security Functional Requirement

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

SPA
: Simple Power Analysis

SS
: Security Service

SSCD
: Secure Signature Creation Device

ST
: Security Target

SVAD
: Signatory VAD

SVD
: Signature Verification Data

TOE
: Target of Evaluation

TRNG
: True Random Number Generator

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 products 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. **Bold** term indicates that this part is added to contents of PP [BSI-PP0059-2009].
2. References in [DIR-EP-1993] to a specific article and paragraph of this directive are of the form '(The Directive: n.m)'.

Administrator	User who performs TOE initialization, TOE personalization or other TOE administrative functions
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
Attester	User who secures the so-called 'unlimited mass signature' with four eyes principle setup of the TOE additionally with a second PIN (PIN_2) whose entry by the owner of PIN_2 is obligatory before mass signing is possible. The Signatory alone can thus never start the mass signing process by himself but always has to be accompanied by the attester (four eyes principle for more security).
Centralized model	Initialization and personalization take place only in the Trust Center, see also

	decentralized model.
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 CGA	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 CSP	Entity that issues certificates or provides other services related to electronic signatures (The Directive: 2.11).
Data to be signed DTBS	All electronic data to be signed including a user message and signature attributes.
Data to be signed or its unique representation DTBS/R	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.
Decentralized model	Initialization and the first two personalization phases take place in the Trust Center and the third personalization phase takes place in the Local Registration Authority. See also centralized model.
Initialization	The process of preparing a TOE for personalization. The initialization comprises of the three phases: Initialization phase 1: - performing acceptance procedures - card authentication / Initialization phase 2: - creation of master file - loading and activation of packages - creation of files and objects e.g. PIN / PUK object / Initialization phase 3: - generation of a SCD/SVD pair for the signatory
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.
Mass Signature	The generation of more than one signature at a time after suitable authentication, e.g. for an automated process, with or without four eyes principle.
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)
Personalization	The process of preparing a TOE for a signatory's use. The personalization comprises of the three phase: Personalization phase 1: - generating and importing of Transport-PIN - importing of reference authentication data (RAD) / Personalization phase 2: - reading out serial number - exporting SVD / Personalization phase 3: - importing of card holders's data - optional import of the certificate of the SVD - secure delivery to the end user
PUK letter	A letter from the Trust Center to the user that conveys the PUK value to the user. The PUK letter concept works only if the Trust Center does not block the PUK. In this case 1. the PUK is already usable when it arrives at the user and 2. can be used to unblock a blocked Transport-PIN (PIN_T).
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 RAD	Data persistently stored by the TOE for authentication of a user as authorized for a particular role
Secure signature-creation device SSCD	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 SCA	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 SCD	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 SCS	Complete system that creates an electronic signature consists of the SCA and the SSCD
Signature-verification data SVD	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.
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 VAD	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 V5.0 with Application for QES V1.0'

Author

Atos IT Solutions and Services GmbH

CC Version

3.1, Revision 3

Version Number

2.00

General Status

Release

Certification ID

BSI-DSZ-CC-0833

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, in this section,
- the conformance claims in section 4,
- the security problem definition in section 5,
- the security objectives in section 6,
- the extended components definition in section 7,
- the security and assurance requirements in section 8,
- the rationale in section 9, and
- the TOE summary specification (TSS) in section 10.

3.2 TOE Reference

The TOE 'CardOS V5.0 with Application for 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 sizes:

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

The Infineon chip SLE78CFX*P (M7892 B11) is certified, see [ST-IFX-Chip-B11-Maint] and [CF-IFX-Chip-B11-MaintRep] which is an addendum to [CF-IFX-Chip-A21].

The Application for QES can be setup (by the administrator) in two different models, which are named 'Centralized model' and 'Decentralized model'. Apart from that, different variants within the models are possible. The variants are determined through the use of the appropriate personalization scripts (cf. Table 1: Components of the TOE) or through other personalization processes that guarantee the same result.

1 Note: The TOE may be part of a product containing further applications besides the 'CardOS V5.0 with Application for QES V1.0' (SSCD application).

It is possible to personalize the TOE 'CardOS V5.0 with Application for QES V1.0' in three ways:

1. According to [QES-Germany-SigG] for **single** and **mass** signatures **without** four eyes principle (4EP), denoted in the following with **QES-Germany**,
2. According to [QES-Swiss-SigGesetz] for **single** and **mass** signatures **without** four eyes principle, denoted in the following with **QES-Switzerland**, and
3. Similar to [QES-Germany-SigG], for **mass** signatures **with** four eyes principle, denoted in the following with **QES-Two-PIN-Signatures**.

3.3 TOE overview

1. **TOE type**

   The TOE as defined by this Composite Security Target is a Smart Card Integrated Circuit (SCIC), which can be delivered as wafer, module, smart card or another IC package. It is to be used as a Secure Signature Creation Device (SSCD) [2]. The SCIC is based on an Infineon Chip.

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. It is possible to personalize the TOE in a way that the TOE can generate **single** or **mass** signatures **without** and **with** four eyes principle, see also chapter "TOE Reference" (1), (2) and (3). 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.

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.

3a. **Optional Non-TOE software**

   An SCIC product containing the TOE may contain further applications, besides the 'CardOS V5.0 with Application for QES V1.0' (SSCD application), e.g. for electronic identity documents.

4. **Confirmation according to German signature law**

   The developer applies for a confirmation according to German signature law [QES-Germany-SigG]

   for requirements of the parts ONE, TWO and THREE,

   see "Split-up of TOE's requirements" below.

5. **Split-up of TOE's requirements**

   This TOE can be personalized according to German signature law, [QES-Germany-SigG], and Swiss signature law, [QES-Swiss-SigGesetz].

   The requirements of chapter "TOE Security Functional Requirements" are divided into 5 parts:

		QES-Germany	QES-Switzerland	QES-Two-PIN-Signatures
Part ONE	general SFRs	x	x	x

2 Note: The TOE may be part of a product where the SCIC contains further applications, besides the 'CardOS V5.0 with Application for QES V1.0', e.g. for electronic identity documents.

		QES-Germany	QES-Switzerland	QES-Two-PIN-Signatures
Part TWO	SFRs according to signatures without four eyes principle	x	x	
Part THREE	SFRs based on German QES	x		x
Part FOUR	SFRs according to Swiss QES only		x	
Part FIVE	SFRs according to signatures with four eyes principle			x

This is done in order to achieve the following:

1. Parts ONE, TWO and THREE allow a personalization of the TOE for signatures without four eyes principle according to [QES-Germany-SigG],
   this personalization is denoted in the following with **QES-Germany**
2. Parts ONE, THREE and FIVE allow a personalization of the TOE for signatures with four eyes principle,
   this personalization is denoted in the following with **QES-Two-PIN-Signatures**
3. Parts ONE, TWO and FOUR allow a personalization of the TOE according to [QES-Swiss-SigGesetz],
   this personalization is denoted in the following with **QES-Switzerland**.

3.4 TOE description

The TOE is a secure signature-creation device (SSCD) according to the Protection Profile [BSI-PP0059-2009] 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-PP0059-2009] 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 configured software (OS "CardOS V5.0", the service package (patches), personalization script files and signature application)
- the underlying hardware (SLE78CFX*P (M7892 B11) from Infineon) used to implement the secure signature-creation device (SSCD) and
- the pertaining guidance documentation 'User Guidance CardOS V5.0' [User-Guidance-V50] and 'Administrator Guidance CardOS V5.0' [Administrator-Guidance-V50].

The TOE developer delivers the SCIC, the service package (patches), personalization script files for initialization/personalization and pertaining documentation. The Trust Center (CA or CSP or entities acting under the CA policy) initializes and personalizes the TOE.

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 RSA v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries.

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

- CardOS V5.0 sources
- certified libraries of SLE78CFX*P (M7892 B11) (as needed by CardOS V5.0 sources) and
- the tool "Postlocator" (provided by Infineon)

The CardOS V5.0 sources are compiled and linked with the binary libraries. The result is a "generic" mask which is used by the tool "Postlocator" 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 for the production site Dresden in Germany (production line indicator 'A' or 'B'), cf Certification Report [CF-IFX-Chip-B11-MaintRep] which is an addendum to [CF-IFX-Chip-A21] for SLE78CFX*P (M7892 B11) from Infineon Technologies AG.

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	C901	*	loaded in protected part of Flash EEPROM
3		CardOS for 300kByte flash	C901	*	
4		CardOS for 404kByte flash	C901	*	
5		RSA-library	1.02.013	-	
		Toolbox	1.02.013		
		SHA-2-library	1.01		
6	Personalization script for QES Germany centralized model	PersAppSigG.csf	*	*	file
7	Pers. script for QES Germany centr. model without PUK	PersAppSigG_withoutPUK.csf	*	*	file
8	Pers. script for QES Germany decentralized model, file system only (by Trust Center)	Pre-PersAppSigG.csf	*	*	file
9	Pers. script for QES Germany decentralized model, end user data + certificate (by RA)	Post-PersAppSigG.csf	*	*	file
10	Pers. script for QES Germany decentr. model, file model only (by TC), without PUK	Pre-PersAppSigG_withoutPUK.csf	*	*	file
11	Pers. script for QES Germany decentr. model, end user data + certificate (by RA), without PUK	Post-PersAppSigG_withoutPUK.csf	*	*	file
12	Pers. script for QES similar to QES Germany decentr. model, file system only (by	Mass_Pre-PersAppSigG.csf	*	*	file

No.	Type	Term	Version	Date	Form of delivery
	TC), for 4EP mass signature				
13	Pers. script for QES similar to QES Germany decentr. model, end user data + certificate (by RA), for 4EP mass signature	Mass_Post-PersAppSigG.csf	*	*	file
14	Constants definitions for RSA key pair, length 1976 bits, centr. and decentr. model	Defines_1976.csf	*	*	file
15	Constants definitions for RSA key pair, length 2048 bits, centr. and decentr. model	Defines_2048.csf	*	*	file
16	Constants definitions for RSA key pair, length 2560 bits, centr. and decentr. model	Defines_2560.csf	*	*	file
17	Constants definitions for RSA key pair, length 3072 bits, centr. and decentr. model	Defines_3072.csf	*	*	file
18	Constants definitions for RSA key pair, length 3584 bits, centr. and decentr. model	Defines_3584.csf	*	*	file
19	Constants definitions for RSA key pair, length 4096 bits, centr. and decentr. model	Defines_4096.csf	*	*	file
20	Service Package	V50_ServicePack_Package.csf	*	*	file
21	Documentation	[Users-Manual-V50]	*	*	paper or PDF file
22		[CardOS50-PR-Notes]	*	*	paper or PDF file
23		[Administrator-Guidance-V50]	*	*	paper or PDF file
24		[User-Guidance-V50]	*	*	paper or PDF file
25		[ADS-Descr-CardOS50]	*	*	paper or 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.
2. Personalization files (CardOS Sequence Format CSF) determine how the Trust Center can setup the TOE. This can include different choices, e.g. for minimal PIN length or for PUK handling.
3. It is possible to setup the TOE so that at least the requirements for Qualified Electronic Signatures (QES) in Germany or Switzerland can be fulfilled.
4. It is possible to setup the TOE so that either single signatures or mass signatures with or without four eyes principle can be generated.
5. Items (6) through (11) and (14) through (20) also may be used for Swiss personalization.
6. The Service Package (patches), item 20, contains amendments to CardOS V5.0.

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 [Geeignete-Algorithmen], agreed as suitable for electronic signatures
   c) after appropriate authentication of the signatory by the TOE
   d) using an appropriate cryptographic signature function that employs appropriate cryptographic parameters and key lengths agreed as suitable according to [Geeignete-Algorithmen].
3. to create **limited** numbers of electronic signatures in a row **without** four eyes principle for an automated process
   a) after the signatory allows to start the process
   b) using appropriate hash functions that are, according to [Geeignete-Algorithmen], agreed as suitable for electronic signatures
   c) after appropriate authentication of the signatory by the TOE
   d) using an appropriate cryptographic signature function that employs appropriate cryptographic parameters and key lengths agreed as suitable according to [Geeignete-Algorithmen]
   e) and stops signing if number of signatures exceeds limit or authorization of the signatory is withdrawn.
4. to create **unlimited** numbers of electronic signatures in a row **without** four eyes principle for an automated process
   a) after the signatory allows to start the process
   b) using appropriate hash functions that are, according to [Geeignete-Algorithmen], agreed as suitable for electronic signatures
   c) after appropriate authentication of the signatory by the TOE
   d) using an appropriate cryptographic signature function that employs appropriate cryptographic parameters and key lengths agreed as suitable according to [Geeignete-Algorithmen]
   e) and stops signing if authentication of the signatory is withdrawn.
5. to create **unlimited** numbers of electronic signatures in a row **with** four eyes principle for an automated process
   a) after the signatory and the attester allow to start the process
   b) using appropriate hash functions that are, according to [Geeignete-Algorithmen], agreed as suitable for electronic signatures
   c) after appropriate authentication of both the signatory and the attester by the TOE
   d) using an appropriate cryptographic signature function that employs appropriate cryptographic parameters and key lengths agreed as suitable according to [Geeignete-Algorithmen]
   e) and stops signing if authorization of the signatory or authorization of the attester is withdrawn.

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. During life cycle phase ADMINISTRATION the TOE will be prepared for the signatory's use by

1. generating a SCD/SVD pair
2. personalization for the signatory by means of the signatory's reference authentication data (RAD) in case of single, limited and unlimited mass signature **without** four eyes principle.
3. personalization for the signatory and attester by means of the signatory's and the attester's reference authentication data (RADs of signatory and attester) in case of unlimited mass signature **with** four eyes principle.

The SVD corresponding to the signatory's SCD will be included in the certificate of the signatory by the certificate service provider (CSP). The human interface for user authentication is implemented in the trusted TOE environment and used for the input of VAD for authentication by knowledge. The TOE holds RAD to check the provided VAD.

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 TOE may contain additional applications, besides the 'CardOS V5.0 with Application for 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. They communicate with the TOE in a trusted environment.

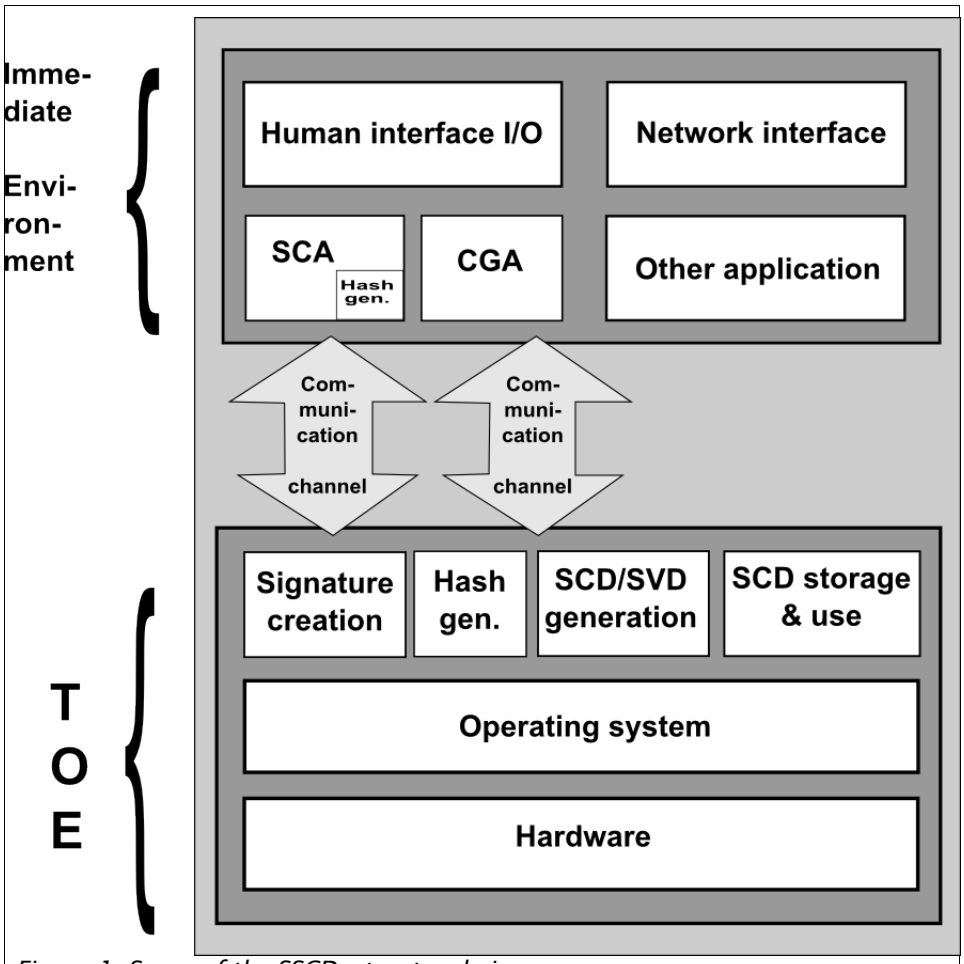

Figure 1: Scope of the SSCD, structural view

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].

The following figure is taken from PP, [BSI-PP0059-2009], from which this ST is derived.

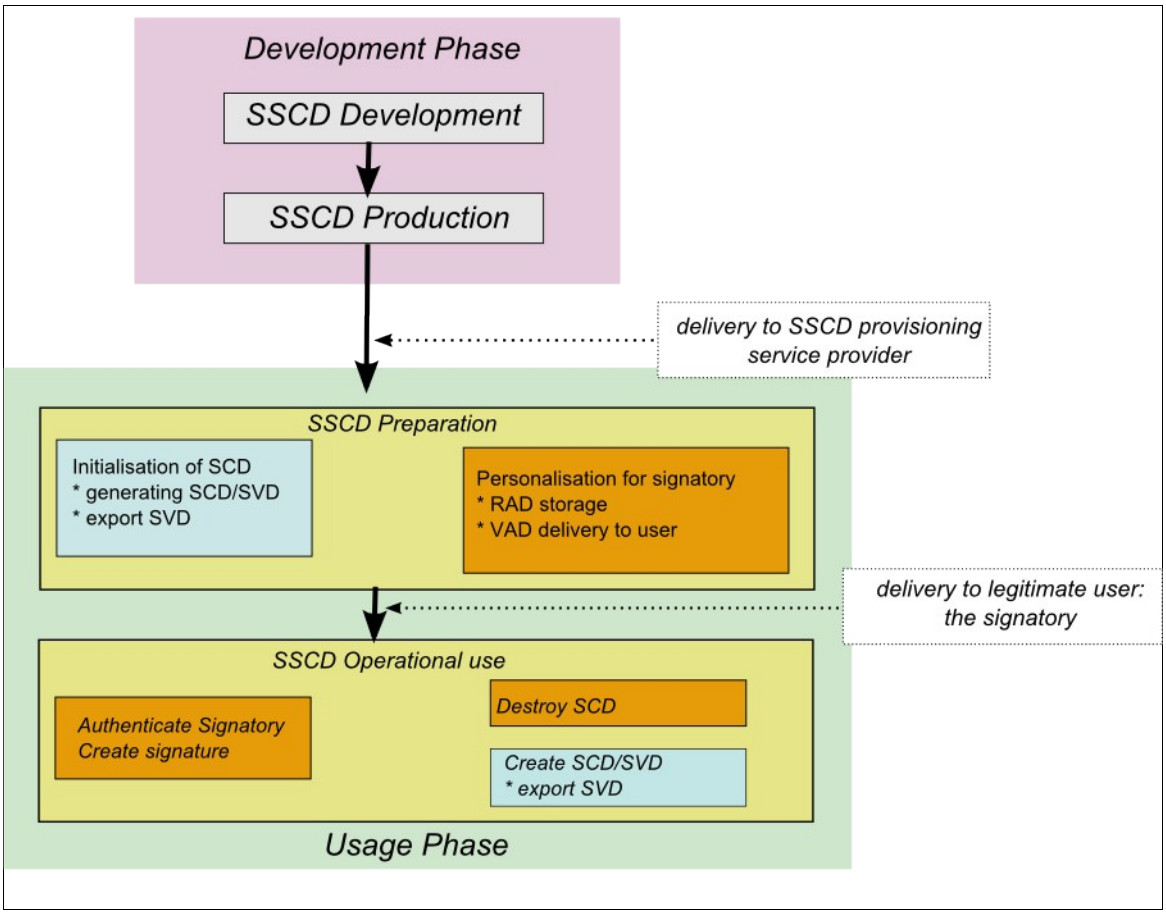

Figure 2: TOE life cycle according to PP, [BSI-PP0059-2009] section 5.4.3.1 "TOE life cycle".

PP's 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 initialization of SCD (generation of SCD/SVD, export of SVD) and personalization for signatory (RAD storage and VAD delivery to user)
- SSCD Operational Use, which includes authenticate signatory, create signature and a possible new creation of SCD/SVD with the following export of SVD.

The PP states the following about the life cycle, see [BSI-PP0059-2009] section 5.4.3.1:

> The development and production of the TOE (cf. CC part 1, para.139) together constitute the development phase of the TOE. The development phase is subject of CC evaluation according to the assurance life cycle (ALC) class. The development phase ends with the delivery of the TOE to an SSCD-provisioning service provider. The functional integrity of the TOE shall be protected in delivering it to an SSCD-provisioning service provider.
>
> The TOE operational use stage begins when the signatory performs the TOE operation to enable it for use in signing operations. Enabling the TOE for signing requires at least one key stored in its memory. The TOE life cycle ends when all keys stored in it have been

rendered permanently unusable. Rendering a key in the SSCD unusable may include deletion of any stored corresponding certificate info.

This ST is derived from PP, [BSI-PP0059-2009]. The TOE provides other notations for the life cycle.

The following table maps this TOE's life cycle, [Users-Manual-V50] section "Card Life Cycle Phases", onto PP's life cycle:

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

Note:

1. CardOS V5.0 User's Manual, [Users-Manual-V50], lists in section "Card Life Cycle Phases" two additional phases: "PHYSINIT" and "PHYSPERS". These two phases do not concern this TOE, because these phases deal with CardOS V5.0 personalization images.

This document refers mainly to ADMINISTRATION and OPERATIONAL. ADMINISTRATION represents initialization and personalization including SCD/SVD generation and start-up in the CC terminology. During ADMINISTRATION, the TOE is initialized and personalized for the signatory, i.e. the SCD/SVD key pair is generated and the RAD used for authentication of the signatory is imported. For this TOE the generation of a SCD/SVD key pair is allowed only once. The main functionality in OPERATIONAL is signature-creation including all supporting functionality like secure SCD storage and use. MANUFACTURING is the phase after chip production and provides an implicit authentication of the administrator.

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.

Phase ADMINISTRATION comprises two stages:

1. Initialization with

    1. reading out serial number
    2. card authentication
    3. creation of master file
    4. loading and activation of packages
    5. creation of files and objects e.g. PIN / PUK object
    6. generation of a SCD/SVD pair for the signatory

2. Personalization with

    1. importing of card holder's data
    2. importing of reference authentication data (RAD)
    3. exporting SVD and optional import of the certificate of the SVD
    4. generating and importing of Transport-PIN
    5. secure delivery to the end user

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 (R3), CC Part 2 (R3) extended, and CC Part 3 (R3) conformant (cf. [CF-IFX-Chip-B11-MaintRep] which is an addendum to [CF-IFX-Chip-A21]).

As required by [AIS36], compatibility between this Composite Security Target and the Platform Security Target [ST-IFX-Chip-B11-Maint] and of the Infineon chip SLE78CFX*P (M7892 B11) is claimed. In section "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 10: Relevant Platform SFRs used by Composite ST, and
2. irrelevant Platform TSF not being used by the composite ST, see Table 11: 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 3, cf. [CC-3.1-P1], [CC-3.1-P2], and [CC-3.1-P3].

The ST is [CC-3.1-P2] extended, [CC-3.1-P3] conformant and the assurance level for this ST is EAL4 augmented.

For the evaluation the following methodology is used:

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, cf [CEM-3.1].

4.2 PP Claim, Package Claim

This Security Target does not claim any PP conformance but is derived from the Protection Profile for Secure signature creation device - Part 2: Device with key generation, cf [BSI-PP0059-2009].

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 Security Target does not claim conformance to a package.

The Infineon chip SLE78CFX*P (M7892 B11) is conformant to Security IC Platform Protection Profile [BSI-PP-0035], which has been certified by BSI, cf [BSI-CC-PP-0035-2007].

Notes:

1. The Protection Profile [BSI-PP0059-2009] is established by CEN as an European standard for products to create electronic signatures. It fulfills requirements of directive 1999/93/ec, [DIR-EP-1993], of the European parliament and of the council of 13 December 1999 on a community framework for electronic signatures.
2. References in [DIR-EP-1993] to a specific article and paragraph of this directive are of the form '(The Directive: n.m)'.
3. References in one of the annexes of [DIR-EP-1993] are of the form (The Directive: A.I) or (The

Directive: A.II) or (The Directive: A.III)

4. The Protection Profile [BSI-PP0059-2009] has been certified by the Bundesamt für Sicherheit in der Informationstechnik (BSI), cf [BSI-CF-PP0059-2009].

4.3 Conformance Rationale

4.3.1 PP Claims Rationale

The Security Target does not include a PP claim, see also section "PP Claim, Package Claim".

5 Security Problem Definition (ASE_SPD)

5.1 General

CC defines assets as entities that the owner of the TOE presumably places value upon. The term 'asset' is used to describe the threats in the TOE operational environment.

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 **alone** intends to sign **or which the signatory and the attester intend to sign**. Their integrity and the unforgeability of the link to the signatory **/ attester** provided by the digital signature must be maintained.
4. Signature-creation function of the TOE to create digital signature for the DTBS/R with the SCD.
5. Hash generation function of the TOE to create hash values.

Notes:

1. The bold text "**alone**", "**or which the signatory and the attester intend to sign**" and "**/ attester**" within (3) are added to contents of PP [BSI-PP0059-2009].
2. Part (5) is added to contents of PP [BSI-PP0059-2009].

5.1.2 User and subjects acting for users

1. User: End user of the TOE who can be identified as Administrator, Signatory or **Attester**. In the TOE the subject S.User may act as S.Admin in the role R.Admin, as S.Sigy in the role R.Sigy or as **S.Attester** in the role **R.Attester**.
2. Administrator: User who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions. In the TOE 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. In the TOE the subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as Signatory.
4. Attester: User who is in charge to assist the Signatory in achieving a four eyes principle. In the TOE, the subject S.Attester is acting in the role R.Attester for this user after successful authentication as Attester.

Note: "Attester", "S.Attester" and "R.Attester" and (4) are added to contents of PP [BSI-PP0059-2009].

5.1.3 Threat agents

1. S.OFFCARD: Attacker as being a human or process acting on his behalf located outside the TOE. The main goal of the attacker is to access the SCD or to falsify the digital signature. An attacker has 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.

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 or signatory and attester** intended to sign.

Note: "**alone or signatory and attester**" is added to contents of PP [BSI-PP0059-2009].

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.

5.2.8 T.Hash_Misuse (Misuse of the hash generation function of the TOE)

An attacker misuses the hash generation function of the TOE to create a hash value for data, which is then signed but which 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.

Note: "T.Hash_Misuse" is added to contents of PP [BSI-PP0059-2009].

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 (The Directive: 2:9, 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 (The Directive: 1, 2), which is a qualified electronic signature if it is based on a valid qualified certificate (Annex I) [3]. The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the digital signature created with a SCD implemented in the SSCD that the signatory maintains under his 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. 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 his un-revoked 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 initialization/personalization by the administrator only takes place within a trusted environment.

Note: "A.Env_Admin" is added to the contents of [BSI-PP0059-2009].

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

5.4.4 A.Env_Mass_Signature (Environment for a mass signature TOE)

Mass signature generation only takes place within a trusted environment.

Note: "A.Env_Mass_Signature" is added to the contents of [BSI-PP0059-2009].

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 initialization, personalization and operational usage.

Note:

1. The second statement "The TOE shall provide functionality to securely destroy the SCD." of "OT.Lifecycle_Security" is removed, see PP [BSI-PP0059-2009].

6.2.2 OT.SCD/SVD_Gen (SCD/SVD generation)

The TOE provides security features to ensure that authorized users only 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.

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. This objective does not conflict with a signature-creation process where the TOE applies a cryptographic hash function on the DTBS/R to prepare for signature creation algorithm.

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.

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 ensures the integrity of the SVD exported by the TOE to the CGA. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the input it provides to the certificate generation function of the CSP.

6.3.2 OE.CGA_QCert (Generation of qualified certificates)

The CGA generates a qualified certificate that includes, inter alias

- the name of the signatory controlling the TOE,
- the SVD matching the SCD stored in the TOE and controlled by the signatory,
- the advanced signature of the CSP.

The CGA confirms with the generated 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 handles authentic devices that implement the TOE to be prepared for the legitimate user as signatory personalizes and delivers the TOE as SSCD to the signatory.

6.3.4 OE.HID_VAD (Protection of the VAD)

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

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

The signatory **or the signatory and the attester** uses **/ use** trustworthy SCA that

- generates the DTBS/R of the data that has been presented as DTBS and which the signatory **alone** intends to sign **or the signatory and the attester intend 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.

Notes:

1. "**or the signatory and the attester**", "**/ use**", "**alone**"
2. "**or the signatory and the attester intend to sign**"

are added to contents of PP [BSI-PP0059-2009].

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

The operational environment ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE.

6.3.7 OE.Signatory (Security obligation of the signatory)

The signatory checks that the SCD stored in the SSCD received from SSCD provisioning service is in non-operational state. The signatory keeps his or her SVAD confidential.

6.3.8 OE.Attester (Security obligation of the attester for signatures with 4EP)

The Attester checks that the SCD **of the signatory** stored in the SSCD received from SSCD provisioning service is in non-operational state. The Attester keeps his or her SVAD confidential.

Notes:

1. "OE.Attester" is added to contents of PP [BSI-PP0059-2009].
2. "OE.Attester" is only an objective for **QES-Two-PIN-Signatures**.

6.3.9 OE.Env_Admin (Administrator works in trusted environment)

Authentication and initialization/personalization, particularly generation of the SCD/SVD key pair, are only started by the administrator within a trusted environment.

Note: "OE.Env_Admin" is added to the contents of [BSI-PP0059-2009].

6.3.10 OE.Env_Mass_Signature (Mass signatures are generated in trusted environment only)

Mass signature generation without four eyes principle is only started by signatory within a trusted environment. Mass signature generation with four eyes principle is only started by signatory in combination with attester within a trusted environment.

Note: "OE.Env_Mass_Signature" is added to the contents of [BSI-PP0059-2009].

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.Attester	OE.Env_Mass_Signature
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		x	
T.Hash_Misuse								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.Env_Admin																			x		
A.CGA												x	x								
A.SCA															x						
A.Env_Mass_ Signature																					x

Note: "OE.Attester" is only an objective for **QES-Two-PIN-Signatures**.

6.4.2 Security Objectives Sufficiency

6.4.2.1 Policies and Security Objective Sufficiency

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

- the TOE security objective **OT.Lifecycle_Security**, which requires the TOE to detect flaws during the initialization, personalization and operational usage,
- the TOE security objective **OT.SCD_SVD_Corresp**, which requires the TOE to ensure the correspondence between the SVD and the SCD during their generation, and
- the security objective for the operational environment **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.

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 generation function for the legitimate signatory only and to protect the SCD against the use of others. **OT.Sig_Secure** ensures that the TOE generates digital signatures that 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. The **OE.DTBS_Intend** ensures that the SCA provides only those DTBS to the TOE, which the signatory intends to sign **or signatory and attester intend to sign**.

Note: "**or signatory and attester intend to sign**" is added to contents of PP [BSI-PP0059-2009].

P.Sigy_SSCD (TOE as secure signature-creation device) requires the TOE to meet (The Directive: A.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 generation can practically occur only once;
- **OT.SCD_Unique**, **OT.SCD_Secrecy** and **OT.Sig_Secure** meet the requirement in (The Directive: A.III, paragraph 1(a)) 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 digital signatures or any other data exported outside the TOE;
- **OT.Sigy_SigF** meets the requirement in (The Directive: A.III, paragraph 1(c)) by the requirements to ensure that the TOE provides the signature generation function for the legitimate signatory only and protects the SCD against the use of others;
- **OT.DTBS_Integrity_TOE** meets the requirements in (The Directive: A.III, paragraph 2) as the TOE must not alter the DTBS/R.

(The Directive: A.III, Paragraph 2) 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 initialization, personalization and operational usage,
- **OT.SCD/SVD_Gen**, which limits invoke the generation of the SCD and the SVD to authorized users only,
- **OT.Sigy_SigF**, which requires the TOE to provide the signature generation 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 a TOE sample as an authentic, initialized and personalized SSCD from an SSCD provisioning service.

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 his 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 ensure the aspects of signatory's sole control over and responsibility for the digital signatures generated with the TOE. **OE.SSCD_Prov_Service** ensures that the signatory uses an authentic TOE, initialized and personalized for the signatory. **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 (in case of signatures without/with four eyes principle) ensures that the signatory checks that the SCD, stored in the SSCD received from an SSCD provisioning service is in non-operational state (i.e. the SCD cannot be used before the signatory becomes into sole control over the SSCD).

QES-Two-PIN-Signatures only:

OE.Attester (in case of signatures with four eyes principle) ensures that the Attester checks that the SCD of the signatory, stored in the SSCD received from an SSCD provisioning service is in non-operational state (i.e. the SCD cannot be used before the signatory in combination with Attester become into sole control over the SSCD).

Note: "**QES-Two-PIN-Signatures** only:" is added to the contents of [BSI-PP0059-2009].

OT.Sigy_SigF (in case of signatures without four eyes principle) provides that only the signatory may use the TOE for signature creation. As prerequisite **OE.Signatory** ensures that the signatory keeps his or her SVAD confidential.

QES-Two-PIN-Signatures only:

OT.Sigy_SigF in combination with **OE.Attester** (in case of signatures with four eyes principle) provides that only the signatory in combination with the attester may use the TOE for signature creation. As prerequisite **OE.Signatory** ensures that the signatory keeps his or her SVAD confidential. As a second prerequisite **OE.Attester** ensures that the attester keeps his or her SVAD confidential.

Note: "**QES-Two-PIN-Signatures** only:" is added to the contents of [BSI-PP0059-2009].

OE.DTBS_Intend, **OE.DTBS_Protect** and **OT.DTBS_Integrity_TOE** ensure that the TOE generates digital signatures only for a DTBS/R that the signatory has decided to sign as DTBS **or that the signatory in combination with attester have decided to sign as DTBS**. The robust cryptographic techniques required by **OT.Sig_Secure** ensure that only this SCD may generate a valid digital 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: "**or that the signatory in combination with attester have decided to sign as DTBS**" is added to contents of PP [BSI-PP0059-2009].

OE.Env_Admin (Administrator works in trusted environment) ensures that authentication and initialization/personalization, particularly generation of the SCD/SVD key pair, are only started by the administrator within a trusted environment.

Note: "**OE.Env_Admin**" is added to the contents of [BSI-PP0059-2009].

OE.Env_Mass_Signature (Mass signatures are generated in trusted environment only) ensures that generation of mass signatures with or without four eyes principle takes place only in a trusted environment.

Note: "**OE.Env_Mass_Signature**" is added to the contents of [BSI-PP0059-2009].

6.4.2.2 Threats and Security Objective Sufficiency

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 [DIR-EP-1993]. 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_Gen** counters this threat by implementing cryptographic secure generation of the SCD/SVD-pair. **OT.Sig_Secure** ensures cryptographic secure digital 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 to generation a certificate. **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 a digital signature on data for which the signatory has not expressed the intent to sign, as required by (The Directive, A.III, paragraph 1(c)). **OT.Lifecycle_Security** (Lifecycle security) requires the TOE to detect flaws during the initialization, personalization and operational usage. **OT.Sigy_SigF** (Signature creation function for the legitimate signatory only) ensures that the TOE provides the signature-generation 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 **or for data the signatory and attester intend 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 his or her SVAD confidential.

QES-Two-PIN-Signatures only:

In case of four eyes mass signature **OE.Attester** counters that the signature creation function can used by the signatory alone. **OE.Attester** ensures also that the Attester keeps his or her SVAD confidential.

Notes:

1. "**or for data the signatory and attester intend to sign**" is added to contents of PP [BSI-PP0059-2009].
2. "**QES-Two-PIN-Signatures** only:"
   are added to contents of PP [BSI-PP0059-2009].
3. The statement "...including secure destruction of the SCD, which may be initiated by the signatory." for "OT.Lifecycle_Security" is removed, see PP [BSI-PP0059-2009].

T.Hash_Misuse (Misuse of the hash generation function of the TOE) addresses the threat of misuse of the TOE hash generation function to create DTBS/R on data for which the signatory has not expressed the intent to hash. **OE.DTBS_Intend** (Data intended to be signed) ensures that the SCA sends the DTBS only for data the signatory intends to sign or for data the signatory and attester intend 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.

Note: **T.Hash_Misuse** sufficiency is added to contents of PP [BSI-PP0059-2009].

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 **or to the signatory and attester** 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 can not 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.

Note: "**or to the signatory and attester**" is added to contents of PP [BSI-PP0059-2009].

T.Sig_Forgery (Forgery of the digital signature) deals with non-detectable forgery of the digital signature. **OT.Sig_Secure**, **OT.SCD_Unique** and **OE.CGA_Qcert** address this threat in general. The **OT.Sig_Secure** (Cryptographic security of the digital signature) ensures by means of robust cryptographic techniques that the signed data and the digital signature are securely linked together. **OT.SCD_Unique** 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 on a forged signature.

6.4.2.3 Assumptions and Security Objective Sufficiency

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 for the data that has been presented to the signatory **or to the signatory and attester** as DTBS and which the signatory intends to sign **or the signatory and the attester intend to sign** in a form which is appropriate for being signed by the TOE.

Note: "**or to the signatory and attester**" and "**or the signatory and the attester intend to sign**" are added to contents of PP [BSI-PP0059-2009].

A.CGA (Trustworthy certification-generation application) establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by **OE.CGA_QCert** (Generation of qualified certificates), which ensures the generation of qualified certificates and by **OE.SVD_Auth** (Authenticity of the SVD), which ensures the protection of the integrity 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 initialization and personalization 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 initialization/personalization, particularly generation of the SCD/SVD key pair, are only started by the administrator within a trusted environment.

Note: "A.Env_Admin" is added to the contents of [BSI-PP0059-2009].

A.Env_Mass_Signature (Environment for a mass signature TOE) establishes a trustworthy environment for the signatory (in case of mass signatures without four eyes principle) or for the signatory in combination with attester (in case of mass signatures with four eyes principle) for generating mass signatures after the signatory is successfully authenticated or the signatory and the attester are successfully authenticated. This is addressed by **OE.Env_Mass_Signature** (Mass signatures are generated in trusted environment only) which ensures that generation of mass signatures with or without four eyes principle takes place only in a trusted environment.

Note: "A.Env_Mass_Signature" is added to the contents of [BSI-PP0059-2009].

7 Extended Component Definition (ASE_ECD)

Notes:

1. This chapter is a complete and unchanged copy of chapter 9 "Extended Component Definition" of PP [BSI-PP0059-2009].
2. [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-0006-2002T, also short SSVG-PPs or CWA14169".

The following definition of the family FPT_EMSEC is a complete copy from the Protection Profile Secure Signature Creation Device [BSI-PP0059-2009],

The additional family FPT_EMSEC (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_EMSEC 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_EMSEC is taken from the Protection Profile Secure Signature Creation Device [5], chapter 6.6.1.

FPT_EMSEC TOE Emanation

Family behavior: This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMSEC TOE Emanation	1

FPT_EMSEC.1 TOE Emanation has two constituents:

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

Management: FPT_EMSEC.1

> There are no management activities foreseen.

Audit: FPT_EMSEC.1

> There are no actions identified that must be auditable if **FAU_GEN** (Security audit data generation) is included in a protection profile or security target.

7.1 FPT_EMSEC.1 *TOE Emanation*

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMSEC.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_EMSEC.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].

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 extended component FPT_EMSEC.1. Section 'TOE Security Functional Requirements' provides the security functional requirements.

Operations not performed in Protection Profile [BSI-PP0059-2009] are performed.

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

8.2 TOE Security Functional Requirements

The requirements are split up into 5 sub-chapters, see part "5. **Split-up of TOE's requirements**" of chapter "TOE overview".

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 2.1.4 of part 2 of the CC. Each of these operations is used in [BSI-PP0059-2009].

This Security Target performs the missing operations as given by Application Notes in [BSI-PP0059-2009].

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,
- assignments 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 a leading **[REFINEMENT]** and in case of a longer section with a closing **[END REFINEMENT]**.

8.2.2 Part ONE (general SFRs)

8.2.2.1 Cryptographic support (FCS)

8.2.2.1.1 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

Note:

1. FCS_CKM.4 Cryptographic key destruction is not fulfilled but justified:
   There is no need to destruct a RSA key

- according to [QES-Germany-SigG] or [QES-Swiss-SigGesetz] and
- because the signature card gets unusable.

FCS_CKM.1.1/RSA

The TSF shall generate an SCD/SVD pair in accordance with a specified cryptographic key generation algorithm **RSA_Key_Generator** [4] and specified cryptographic key sizes **1976 up to 4096** [5] that meet the following: **[Geeignete-Algorithmen]** [6].

8.2.2.1.2 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

Note:

1. FCS_CKM.4 Cryptographic key destruction is not fulfilled but justified:
   There is no need to destruct a RSA key
   - according to [QES-Germany-SigG] or [QES-Swiss-SigGesetz] and
   - because the signature card gets unusable.

FCS_COP.1.1/RSA

The TSF shall perform digital signature-generation in accordance with a specified cryptographic algorithm **RSA** [7] and cryptographic key sizes **1976 up to 4096** [8] that meet the following:

1. **RSASSA-PKCS1-v1_5 or RSASSA-PSS** [RSA-PKCS1-v2.1], chapter 8, [9]
2. **[Geeignete-Algorithmen]** [10]

8.2.2.1.3 FCS_COP.1/SHA-2 *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

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.

4 [assignment: cryptographic key generation algorithm]
5 [assignment: cryptographic key sizes]
6 [assignment: list of standards]
7 [assignment: cryptographic algorithm]
8 [assignment: cryptographic key sizes]
9 [assignment: list of standards]
10 [assignment: list of standards]

FCS_COP.1.1/SHA-2

The TSF shall perform **hashing** [11] in accordance with a specified cryptographic algorithms **SHA-256**, **SHA-384** and **SHA-512** [12] and cryptographic key sizes **none** [13] that meet the following:

1. **[Geeignete-Algorithmen]** [14]

Note: "FCS_COP.1/SHA-2" is added to contents of PP [BSI-PP0059-2009].

8.2.2.2 User data protection (FDP)

Note: The security attributes and related status for the subjects and objects depend on signatures without four eyes principle (see part two) or signatures with four eyes principle (see part five).

8.2.2.2.1 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.

8.2.2.2.2 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 initialization

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:

11 [assignment: list of cryptographic operations]
12 [assignment: cryptographic algorithm]
13 [assignment: cryptographic key sizes]
14 [assignment: list of standards]

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

8.2.2.2.3 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.

8.2.2.2.4 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 initialization

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.

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.Admin is allowed to export SVD** [15] .

FDP_ACF.1.3/SVD_Transfer_SFP

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

FDP_ACF.1.4/SVD_Transfer_SFP

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

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 EN14169-3 "Protection Profiles for Secure signature creation device - Part 3: Device with key generation and trusted channel between SSCD and CGA" for additional requirements for use of an SSCD in an environment that cannot provide such protection.

8.2.2.2.5 FDP_RIP.1 *Subset residual information protection*

Hierarchical to: No other components.

Dependencies: No dependencies.

15 [selection: R.Admin, R.Sigy]

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.

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).

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

8.2.2.2.6 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.

8.2.2.2.7 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.

8.2.2.3 Identification and authentication (FIA)

8.2.2.3.1 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. **no TSF-mediated action** [16]

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.

8.2.2.3.2 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

1. Self test according to FPT_TST.1,
2. Identification of the user by means of TSF required by FIA_UID.1.
3. **none additional TSF mediated actions** [17]

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.

8.2.2.3.3 FIA_AFL.1/Transport_PIN *Authentication failure handling*

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/Transport_PIN

The TSF shall detect when **3** [18] unsuccessful authentication attempts occur related to consecutive failed authentication attempts.

FIA_AFL.1.2/Transport_PIN

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

Note: "FIA_AFL.1/Transport_PIN" is added to contents of PP [BSI-PP0059-2009].

8.2.2.3.4 FIA_AFL.1/PUK *Authentication failure handling*

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/PUK

The TSF shall detect when **3** [19] unsuccessful authentication attempts occur related to consecutive failed authentication attempts.

16 [assignment: list of TSF-mediated actions]
17 [assignment: list of additional TSF mediated actions]
18 [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
19 [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

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**.

Note: "FIA_AFL.1/PUK" is added to contents of PP [BSI-PP0059-2009].

8.2.2.4 Security management (FMT)

8.2.2.4.1 FMT_MSA.1/Admin *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/Admin

The TSF shall enforce the SCD/SVD_Generation_SFP to restrict the ability to **modify** [20] the security attributes SCD / SVD management to R.Admin.

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

8.2.2.4.3 FMT_MTD.1/Admin *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/Admin

The TSF shall restrict the ability to create the RAD **[REFINEMENT] and Transport-PIN(s)** to R.Admin.

20 [assignment: other operations]

8.2.2.5 Protection of the TSF (FPT)

8.2.2.5.1 FPT_EMSEC.1 *TOE Emanation*

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMSEC.1.1

The TOE shall not emit **information about IC power consumption** [21] in excess of **unintelligible limits** [22] enabling access to RAD and SCD.

FPT_EMSEC.1.2

The TSF shall ensure **S.User and S.OFFCARD** [23] are unable to use the following interface **physical contacts of the underlying IC hardware** [24] to gain access to RAD and SCD.

8.2.2.5.2 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** [25]
3. **Memory failures during TOE execution** [26]
4. **Out of range failures of temperature, clock and voltage sensors** [27]
5. **Failures during random number generation** [28].

8.2.2.5.3 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.

8.2.2.5.4 FPT_PHP.3 *Resistance to physical attack*

Hierarchical to: No other components.

21 [assignment: types of emissions]
22 [assignment: specified limits]
23 [assignment: type of users]
24 [assignment: type of connection]
25 [assignment: list of other types of failures in the TSF]
26 [assignment: list of other types of failures in the TSF]
27 [assignment: list of other types of failures in the TSF]
28 [assignment: list of other types of failures in the TSF]

Dependencies: No dependencies.

FPT_PHP.3.1

The TSF shall resist **tampering scenarios by intrusion of physical or mechanical means** [29] to the **underlying IC hardware** [30] by responding automatically such that the SFRs are always enforced.

8.2.2.5.5 FPT_TST.1 *TSF testing*

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1

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

1. **Generation of the SCD/SVD key pair according to FCS_CKM.1/RSA**
2. **Signature-creation according to FCS_COP.1/RSA**
3. **VAD verification**
4. **RAD modification**
5. **RAD unblocking** [31]

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.

8.2.3 Part TWO (SFRs according to signatures without four eyes principle)

8.2.3.1 User data protection (FDP)

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

Table 3: Security Attributes and related Status for the Subjects and Objects (in case of signatures without 4EP)

Subject or object the security attribute is associated	with Security attribute type	Value of the security attribute
S.User	Role	R.Admin - S.User acts as S.Admin R.Sigy - S.User acts as S.Sigy
S.User	SCD / SVD Management	Authorized, not authorized
SCD	SCD Operational	No, yes
SCD	SCD identifier	arbitrary value

29 [assignment: physical tampering scenarios]
30 [assignment: list of TSF devices/elements]
31 [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]]

SVD	(This ST does not define security attributes for SVD)	(This ST does not define security attributes for SVD)

8.2.3.1.1 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.

8.2.3.1.2 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 initialization

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

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".

8.2.3.2 Security management (FMT)

8.2.3.2.1 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.

8.2.3.2.2 FMT_MSA.3 *Static attribute initialization*

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 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.

8.2.3.2.3 FMT_SMF.1 *Security management functions (signatures without 4EP)*

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,
4. Change the default value of the security attribute SCD Identifier,
5. **Unblocking of RAD** and
6. **Enabling the SHA-2_hashing_SFP** [32]

8.2.3.2.4 FMT_SMR.1 *Security roles for signature without 4EP*

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1

The TSF shall maintain the roles R.Admin and R.Sigy.

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

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

8.2.3.2.5 FMT_MOF.1 *Management of security functions behavior without 4EP* [33]

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.

8.2.3.2.6 FMT_MSA.2 *Secure security attributes without 4EP* [34]

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 and SCD operational.

[REFINEMENT]:

Security attribute "SCD/SVD Management" can only have the values "authorized" or "not authorized". 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.

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 4: Secure Values of the Combinations for Signatures without 4EP

SCD/SVD Management	SCD operational	Secure
authorized	yes	NO
authorized	no	YES
not authorized	yes	YES
not authorized	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]

33 [deleteted "Management of security functions behavior"]
34 [deleted "Secure security attributes"]

8.2.3.3 Identification and authentication (FIA)

8.2.3.3.1 FIA_UAU.6/without_4EP *Re-authenticating on Signature without 4EP*

Hierarchical to: No other components. Dependencies: No dependencies.

FIA_UAU.6.1/without_4EP

The TSF shall re-authenticate the user under the conditions

1. **Single signature**
   S.Sigy before every single DTBS/R signature.
2. **Limited Mass signature without four eyes principle**
   S.Sigy before next signature after card reset or after Application Digital Signature (ADS) was left or otherwise before (N+1)-th DTBS/R signature in a row when limit for consecutive signatures is N.
3. **Unlimited Mass signature without four eyes principle**
   S.Sigy before next signature after card reset or after ADS was left [35].

Note: "FIA_UAU.6/without_4EP Re-authenticating on Signature without 4EP" is added to contents of PP [BSI-PP0059-2009].

8.2.4 Part THREE (SFRs based on German QES)

8.2.4.1 Identification and authentication (FIA)

8.2.4.1.1 FIA_AFL.1/PIN *Authentication failure handling*

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 *Timing of authentication*

FIA_AFL.1.1/PIN

The TSF shall detect when **an administrator configurable positive integer within 3 up to 15** [36] unsuccessful authentication attempts occur related to consecutive failed authentication attempts.

FIA_AFL.1.2/PIN

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

Note: "FIA_AFL.1/PIN" is added to contents of PP [BSI-PP0059-2009].

8.2.4.2 Security management (FMT)

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

Hierarchical to: No other components.

Dependencies:

35 [assignment: list of conditions under which re-authentication is required].
36 [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

- 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 or **unblock** [37] the RAD **[REFINEMENT] of S.Sigy** to R.Sigy.

8.2.4.2.2 FMT_MTD.1/Signatory_PIN_T *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_PIN_T

The TSF shall restrict the ability to **[REFINEMENT] unblock** the **[REFINEMENT] Transport-PIN of S.Sigy** to R.Sigy.

Note: "FMT_MTD.1/Signatory_PIN_T" is added to contents of PP [BSI-PP0059-2009].

8.2.5 Part FOUR (SFRs according to QES-Switzerland only)

8.2.5.1 Identification and authentication (FIA)

8.2.5.1.1 FIA_AFL.1/Swiss_PIN *Authentication failure handling*

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/Swiss_PIN

The TSF shall detect when **an administrator configurable positive integer within 4 up to 15** [38] unsuccessful authentication attempts occur related to consecutive failed authentication attempts.

FIA_AFL.1.2/Swiss_PIN

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

Note: "FIA_AFL.1/Swiss_PIN" is added to contents of PP [BSI-PP0059-2009].

8.2.5.2 Security management (FMT)

8.2.5.2.1 FMT_MTD.1/Swiss_Signatory_Modifying *Management of TSF data*

Hierarchical to: No other components.

Dependencies:

- FMT_SMR.1 Security roles

37 [assignment: other operations]
38 [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

- FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/Swiss_Signatory_Modifying

The TSF shall restrict the ability to **modify** [39] the **PIN of S.Sigy** [40] to **R.Sigy** [41].

Note: "FMT_MTD.1/Swiss_Signatory_Modifying" is added to contents of PP [BSI-PP0059-2009].

8.2.5.2.2 FMT_MTD.1/Swiss_Signatory_Unblocking *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/Swiss_Signatory_Unblocking

The TSF shall restrict the ability to **unblock or unblock and then modify** [42] the **PIN of S.Sigy** [43] to **R.Admin** [44].

Note: "FMT_MTD.1/Swiss_Signatory_Unblocking" is added to contents of PP [BSI-PP0059-2009].

8.2.5.2.3 FMT_MTD.1/Swiss_Admin *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/Swiss_Admin

The TSF shall restrict the ability to **modify** [45] the **PUK belonging to the PIN of S.Sigy** [46] to **R.Admin** [47].

Note: "FMT_MTD.1/Swiss_Admin" is added to contents of PP [BSI-PP0059-2009].

8.2.5.2.4 FMT_MTD.1/Swiss_Admin_PIN_T *Management of TSF data without 4EP*

Hierarchical to: No other components.

Dependencies:

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

FMT_MTD.1.1/Swiss_Admin_PIN_T

The TSF shall restrict the ability to **[REFINEMENT] unblock** the **[REFINEMENT] Transport-**

39 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
40 [assignment: list of TSF data]
41 [assignment: the authorized identified roles].
42 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
43 [assignment: list of TSF data]
44 [assignment: the authorized identified roles].
45 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
46 [assignment: list of TSF data]
47 [assignment: the authorized identified roles].

PIN of S.Sigy to R.Admin.

Note: "FMT_MTD.1/Swiss_Admin_PIN_T" is added to contents of PP [BSI-PP0059-2009].

8.2.6 Part FIVE (SFRs according to QES-Two-PIN-Signatures)

8.2.6.1 User data protection (FDP)

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

Table 5: Security Attributes and related Status for the Subjects and Objects (in case of signatures with 4EP)

Subject or object the security attribute is associated	with Security attribute type	Value of the security attribute
S.User	Role	R.Admin - S.User acts as S.Admin R.Sigy - S.User acts as S.Sigy **R.Attester** - S.User acts as **S.Attester**
S.User	SCD / SVD Management	Authorized, not authorized
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: **R.Attester** and **S.Attester** are added to contents of PP [BSI-PP0059-2009].

8.2.6.1.1 FDP_ACC.1/4EP_Mass_Signature-creation_SFP *Subset access control*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/4EP_Mass_Signature-creation_SFP

The TSF shall enforce the **4EP_Mass_Signature-creation_SFP** [48] on

1. **two subjects: S.User,**
2. **objects: DTBS/R, SCD,**
3. **operations: signature-creation** [49].

Note: "FDP_ACC.1/4EP_Mass_Signature-creation_SFP" is added to contents of PP [BSI-PP0059-2009].

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

8.2.6.1.2 FDP_ACF.1/4EP_Mass_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 initialization

FDP_ACF.1.1/4EP_Mass_Signature-creation_SFP

The TSF shall enforce the **4EP_Mass_Signature-creation_SFP** [50] to objects based on the following:

1. **two users S.User are associated with the security attribute "Role" and**
2. **the SCD with the security attribute "SCD Operational"** [51].

FDP_ACF.1.2/4EP_Mass_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" if a subject with role R.Attester is present at the point in time of signature creation [52].

FDP_ACF.1.3/4EP_Mass_Signature-creation_SFP

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none** [53].

FDP_ACF.1.4/4EP_Mass_Signature-creation_SFP

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" [54].

Note: "FDP_ACF.1/4EP_Mass_Signature-creation_SFP" is added to contents of PP [BSI-PP0059-2009].

8.2.6.2 Identification and authentication (FIA)

8.2.6.2.1 FIA_UAU.6/with_4EP *Re-authenticating on Signature with 4EP*

Hierarchical to: No other components. Dependencies: No dependencies.

FIA_UAU.6.1/with_4EP

The TSF shall re-authenticate the user under the conditions

1. **Unlimited Mass signature with four eyes principle**
   S.Sigy and S.Attester before next signature after card reset or after ADS was left [55].

Note: "FIA_UAU.6/with_4EP Re-authenticating on Signature with 4EP" is added to contents of PP [BSI-PP0059-2009].

50 [assignment: access control SFP]
51 [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].
52 [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].
53 [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].
54 [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].
55 [assignment: list of conditions under which re-authentication is required].

8.2.6.3 Security management (FMT)

8.2.6.3.1 FMT_MSA.3/4EP_Mass_Signature *Static attribute initialization for 4EP mass signature*

Hierarchical to: No other components.

Dependencies:

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

FMT_MSA.3.1/4EP_Mass_Signature

The TSF shall enforce the SCD/SVD_Generation_SFP, SVD_Transfer_SFP, and **[REFINEMENT] 4EP_Mass_Signature-creation_SFP** to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/4EP_Mass_Signature

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

Note: "FMT_MSA.3/4EP_Mass_Signature Static attribute initialization for 4EP mass signature" is added to contents of PP [BSI-PP0059-2009].

8.2.6.3.2 FMT_SMF.1/with_4EP *Security management functions for signatures with 4EP*

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1/with_4EP

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

1. Creation and modification of RAD,
2. **[REFINEMENT] Enabling the 4EP_Mass_Signature-creation_SFP**,
3. Modification of the security attribute SCD/SVD management, SCD operational,
4. Change the default value of the security attribute SCD Identifier,
5. **Unblocking of RAD** and
6. **Enabling the SHA-2_hashing_SFP** [56]

Note: "FMT_SMF.1/with_4EP Security management functions for signatures with 4EP" is added to contents of PP [BSI-PP0059-2009].

8.2.6.3.3 FMT_SMR.1/with_4EP *Security roles for Mass_Signature with 4EP*

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1/with_4EP

The TSF shall maintain the roles **R.Admin, R.Sigy and R.Attester** [57].

FMT_SMR.1.2/with_4EP

The TSF shall be able to associate users with roles.

Note: "FMT_SMR.1/with_4EP Security roles for Mass_Signature with 4EP" is added to contents of PP [BSI-PP0059-2009].

56 [assignment: list of other security management functions to be provided by the TSF].
57 [assignment: the authorized identified roles]

8.2.6.3.4 FMT_MTD.1/Attester *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/Attester

> The TSF shall restrict the ability to **modify or unblock** [58] the **RAD of S.Attester** [59] to **R.Attester** [60].

Note: "FMT_MTD.1/Attester" is added to contents of PP [BSI-PP0059-2009].

8.2.6.3.5 FMT_MTD.1/Attester_PIN_T *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/Attester_PIN_T

> The TSF shall restrict the ability to **unblock** [61] the **Transport-PIN of S.Attester** [62] to **R.Attester** [63].

Note: "FMT_MTD.1/Attester_PIN_T" is added to contents of PP [BSI-PP0059-2009].

8.2.6.3.6 FMT_MOF.1/4EP_Mass_Signature *Management of security functions behavior for 4EP_Mass_Signature*

Hierarchical to: No other components.

Dependencies:

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

FMT_MOF.1.1/4EP_Mass_Signature

> The TSF shall restrict the ability to **enable** [64] the function **4EP_mass signature-creation function** [65] to **R.Sigy in combination with R.Attester** [66].

Note: "FMT_MOF.1/4EP_Mass_Signature Management of security functions behavior for 4EP_Mass_Signature" is added to contents of PP [BSI-PP0059-2009].

8.2.6.3.7 FMT_MSA.1/Signatory_Attester *Management of security attributes*

Hierarchical to: No other components.

58 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
59 [assignment: list of TSF data]
60 [assignment: the authorized identified roles].
61 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
62 [assignment: list of TSF data]
63 [assignment: the authorized identified roles].
64 [selection: determine the behavior of, disable, enable, modify the behavior of]
65 [assignment: list of functions]
66 [assignment: the authorized identified roles]

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_Attester

The TSF shall enforce the **4EP_Mass_Signature-creation_SFP** [67] to restrict the ability to **modify** [68] the security attributes **SCD operational** [69] to **R.Sigy in combination with R.Attester** [70].

Note: "FMT_MSA.1/Signatory_Attester Management of security attributes" is added to contents of PP [BSI-PP0059-2009].

8.2.6.3.8 FMT_MSA.2/4EP_Mass_Signature *Secure security attributes for 4EP_Mass_Signature*

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.2.1/4EP_Mass_Signature

The TSF shall ensure that only secure values are accepted for SCD / SVD Management and SCD operational.

[REFINEMENT]:

Security attribute "SCD/SVD Management" can only have the values "authorized" or "not authorized". 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.

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 6: Secure Values of the Combinations for 4EP_Mass_Signature

SCD/SVD Management	SCD operational	Secure
authorized	yes	NO
authorized	no	YES
not authorized	yes	YES
not authorized	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]

Note: "FMT_MSA.2/4EP_Mass_Signature Secure security attributes for 4EP_Mass_Signature" is added to contents of PP [BSI-PP0059-2009].

67 [assignment: access control SFP(s), information flow control SFP(s)]
68 [selection: change_default, query, modify, delete, [assignment: other operations]]
69 [assignment: list of security attributes]
70 [assignment: the authorized identified roles]

8.3 TOE Security Assurance Requirements

Table 7: 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
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 8: Functional Requirement to TOE security objective 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	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
FCS_CKM.1/RSA	x		x	x	x						
FCS_COP.1/RSA	x					x					
FCS_COP.1/SHA-2						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_ACC.1/ 4EP_Mass_ 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_ACF.1/ 4EP_Mass_ Signature-creation_SFP	x						x				
FDP_RIP.1					x		x				
FDP_SDI.2/Persistent				x	x	x					

FDP_SDI.2/DTBS							x	x			
FIA_AFL.1/ Transport_PIN	x						x				
FIA_AFL.1/PIN							x				
FIA_AFL.1/PUK							x				
FIA_AFL.1/Swiss_PIN							x				
FIA_UAU.1		x					x				
FIA_UAU.6/without_4EP							x				
FIA_UAU.6/with_4EP							x				
FIA_UID.1		x					x				
FMT_MOF.1	x						x				
FMT_MOF.1/ 4EP_Mass_Signature	x						x				
FMT_MSA.1/Admin	x	x									
FMT_MSA.1/Signatory	x						x				
FMT_MSA.1/ Signatory_Attester	x						x				
FMT_MSA.2	x	x					x				
FMT_MSA.2/ 4EP_Mass_Signature	x	x					x				
FMT_MSA.3	x	x					x				
FMT_MSA.3/ 4EP_Mass_Signature	x	x					x				
FMT_MSA.4	x	x					x				
FMT_MTD.1/Admin	x						x				
FMT_MTD.1/Signatory	x						x				
FMT_MTD.1/Attester	x						x				
FMT_MTD.1/ Swiss_Signatory_Modif.	x						x				
FMT_MTD.1/ Swiss_Signatory_Unblo.	x						x				
FMT_MTD.1/ Signatory_PIN_T	x										

FMT_MTD.1/ Attester_PIN_T	x										
FMT_MTD.1/ Swiss_Admin	x										
FMT_MTD.1/ Swiss_Admin_PIN_T	x										
FMT_SMR.1	x						x				
FMT_SMR.1/with_4EP	x						x				
FMT_SMF.1	x						x				
FMT_SMF.1/with_4EP	x						x				
FPT_EMSEC.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

OT.Lifecycle_Security (Lifecycle security) is provided by the SFR for SCD/SVD generation FCS_CKM.1/RSA and SCD usage FCS_COP.1/RSA 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. **Access by the end user (signatory or by signatory and attester) is ensured by FIA_AFL.1/Transport_PIN.**

Notes:

1. **Access by the end user (signatory or by signatory and attester) is ensured by FIA_AFL.1/Transport_PIN.**

are added to contents of PP [BSI-PP0059-2009].

The SCD usage is ensured by access control

QES-Germany and **QES-Switzerland** only:

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

QES-Two-PIN-Signatures only:

FDP_ACC.1/4EP_Mass_Signature-creation_SFP and FDP_ACF.1/4EP_Mass_Signature-creation_SFP

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

QES-Germany only:

FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, **FMT_MTD.1/Signatory_PIN_T**, FMT_SMF.1 and FMT_SMR.1.

QES-Switzerland only:

FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, **FMT_MTD.1/Swiss_Signatory_Modifying, FMT_MTD.1/Swiss_Signatory_Unblocking, FMT_MTD.1/Swiss_Admin**, **FMT_MTD.1/Swiss_Admin_PIN_T**, FMT_SMF.1 and FMT_SMR.1.

QES-Two-PIN-Signatures only:

FMT_MOF.1/4EP_Mass_Signature, FMT_MSA.1/Admin, **FMT_MSA.1/Signatory_Attester**, **FMT_MSA.2/4EP_Mass_Signature**, **FMT_MSA.3/4EP_Mass_Signature**, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, **FMT_MTD.1/Attester**, **FMT_MTD.1/Signatory_PIN_T**, **FMT_MTD.1/Attester_PIN_T FMT_SMF.1/with_4EP and FMT_SMR.1/with_4EP**.

Notes:

1. "**FDP_ACC.1/4EP_Mass_Signature-creation_SFP and FDP_ACF.1/4EP_Mass_Signature-creation_SFP**",
2. **FMT_MTD.1/Signatory_PIN_T**,
3. "**FMT_MTD.1/Swiss_Signatory_Modifying**", "**FMT_MTD.1/Swiss_Signatory_Unblocking**", "**FMT_MTD.1/Swiss_Admin**", **FMT_MTD.1/Swiss_Admin_PIN_T** and
4. "**FMT_MOF.1/4EP_Mass_Signature**", "**FMT_MSA.1/Signatory_Attester**", "**FMT_MSA.2/4EP_Mass_Signature**", "**FMT_MSA.3/4EP_Mass_Signature**", "**FMT_MTD.1/Attester**", "**FMT_SMF.1/with_4EP and FMT_SMR.1/with_4EP**"
5. "**FMT_MTD.1/Attester_PIN_T**"

are added to contents of PP [BSI-PP0059-2009].

OT.SCD/SVD_Gen (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,

QES-Germany and **QES-Switzerland** only:

FMT_MSA.2 and FMT_MSA.3 for static attribute initialization.

QES-Two-PIN-Signatures only:

FMT_MSA.2/4EP_Mass_Signature and FMT_MSA.3/4EP_Mass_Signature for static attribute initialization.

The SFR FMT_MSA.4 defines rules for inheritance of the security attribute "SCD operational" of the SCD.

Note: "**FMT_MSA.2/4EP_Mass_Signature and FMT_MSA.3/4EP_Mass_Signature**" is added to contents of PP [BSI-PP0059-2009].

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/RSA.

OT.SCD_SVD_Corresp (Correspondence between SVD and SCD) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1/RSA 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.

Note: The sentence "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." is part of the description of [BSI-PP0059-2009] for **OT.SCD_SVD_Corresp** but removed here because both SFR are not mapped to **OT.SCD_SVD_Corresp**, see Table 8: Functional Requirement to TOE security objective mapping.

OT.SCD_Secrecy (Secrecy of signature-creation data) is provided by the security functions specified by the following SFR. 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 ensure that residual information on SCD is destroyed after the SCD has been used for signature creation.

Note:

1. The statement "...and that destruction of SCD leaves no residual information." for "The security functions specified by FDP_RIP.1 ensure..." is removed, see PP [BSI-PP0059-2009].

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_EMSEC.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

OT.Sig_Secure (Cryptographic security of the digital signature) is provided by the cryptographic algorithms specified by FCS_COP.1/RSA **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/RSA if DTBS is sent to the TOE. The use of FCS_COP.1/RSA is provides by FMT_SMF.1.**

Notes:

1. "**and by FCS_COP.1/SHA-2**",
2. "**FCS_COP.1/SHA-2 is used before FCS_COP.1/RSA if DTBS is sent to the TOE.**" and
3. **The use of FCS_COP.1/RSA is provides by FMT_SMF.1.**

are added to contents of PP [BSI-PP0059-2009].

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 (in case of signatures without four eyes principle) or the signatory and the attester (in case of signatures with four eyes principle) is/are identified and authenticated. The security functions specified by FMT_MTD.1/Admin,

QES-Germany only:

FMT_MTD.1/Signatory

QES-Switzerland only:

FMT_MTD.1/Swiss_Signatory_Modifying and FMT_MTD.1/Swiss_Signatory_Unblocking

QES-Two-PIN-Signatures only:

FMT_MTD.1/Signatory and **FMT_MTD.1/Attester**

manage the authentication function.

The Security Functional Requirement(s)

FIA_AFL.1/Transport_PIN and

QES-Germany and **QES-Two-PIN-Signatures** only:

FIA_AFL.1/PIN and FIA_AFL.1/PUK

QES-Switzerland only:

FIA_AFL.1/Swiss_PIN and FIA_AFL.1/PUK

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).

Notes:

1. For **QES-Switzerland** the PUK (FIA_AFL.1/PUK) is only known to the administrator (FMT_MTD.1/Swiss_Signatory_Unblocking).
2. "**FIA_AFL.1/Transport_PIN, FIA_AFL.1/PIN, FIA_AFL.1/PUK**",
3. "**FIA_AFL.1/Swiss_PIN**",
4. "**FMT_MTD.1/Swiss_Signatory_Modifying and FMT_MTD.1/Swiss_Signatory_Unblocking**" and
5. "**FMT_MTD.1/Attester**

are added to contents of PP [BSI-PP0059-2009].

The security functions specified by

QES-Germany and **QES-Switzerland** only:

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

QES-Two-PIN-Signatures only:

FDP_ACC.1/4EP_Mass_Signature-creation_SFP and **FDP_ACF.1/4EP_Mass_Signature-creation_SFP**

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

QES-Germany only:

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

QES-Switzerland only:

FMT_MTD.1/Swiss_Signatory_Modifying, FMT_MTD.1/Swiss_Signatory_Unblocking, FMT_MSA.2, FMT_MSA.3

QES-Two-PIN-Signatures only:

SFR FMT_MTD.1/Signatory, **FMT_MTD.1/Attester**, **FMT_MSA.2/4EP_Mass_Signature**, **FMT_MSA.3/4EP_Mass_Signature**.

The Security Functional Requirement(s)

QES-Germany only:

FMT_SMF.1 and FMT_SMR.1

QES-Switzerland only:

FMT_SMF.1 and FMT_SMR.1

QES-Two-PIN-Signatures only:

FMT_SMF.1/with_4EP and FMT_SMR.1/with_4EP

list these management functions and the roles. These ensure that the signature process is restricted to the signatory (in case of signatures without four eyes principle) and signatory/attester (in case of signatures with four eyes principle).

Notes:

1. "**FDP_ACC.1/4EP_Mass_Signature-creation_SFP**" and "**FDP_ACF.1/4EP_Mass_Signature-creation_SFP**",
2. "**FMT_MTD.1/Swiss_Signatory_Modifying**", "**FMT_MTD.1/Swiss_Signatory_Unblocking**",
3. "**FMT_MTD.1/Attester**", "**FMT_MSA.2/4EP_Mass_Signature**", "**FMT_MSA.3/4EP_Mass_Signature**" and
4. "**FMT_SMF.1/with_4EP and FMT_SMR.1/with_4EP**"

are added to contents of PP [BSI-PP0059-2009].

QES-Germany and **QES-Switzerland** only:

FMT_MOF.1 restricts the ability to enable the signature-creation function to the signatory.

QES-Two-PIN-Signatures only:

FMT_MOF.1/4EP_Mass_Signature restricts the ability to enable the 4EP_mass signature-creation function to the signatory in combination with attester.

QES-Germany and **QES-Switzerland** only:

FMT_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory.

QES-Two-PIN-Signatures only:

FMT_MSA.1/Signatory_Attester restricts the ability to modify the security attributes SCD operational to the signatory and attester.

Notes:

1. "**FMT_MOF.1/4EP_Mass_Signature**" and
2. "**FMT_MSA.1/Signatory_Attester**"

are added to contents of PP [BSI-PP0059-2009].

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.

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

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

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

9.1.2.1 Different possibilities to create signatures

Note: This chapter is added to contents of PP [BSI-PP0059-2009].

With the security functions specified by

QES-Germany and **QES-Switzerland** only:

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

QES-Two-PIN-Signatures only:

FDP_ACC.1/4EP_Mass_Signature-creation_SFP and **FDP_ACF.1/4EP_Mass_Signature-creation_SFP**

the TOE ensures only following possibilities to create signatures:

QES-Germany and **QES-Switzerland** only:

1. The signatory alone signs one DBTS/R with Signature-creation_SFP (FMT_MOF.1)
2. The signatory alone signs a limited number of DBTS/R with Signature-creation_SFP in a row (FMT_MOF.1)
3. The signatory alone signs an unlimited number of DTBS/Rs with Signature-creation_SFP in a row (FMT_MOF.1)

QES-Two-PIN-Signatures only:

1. The signatory in combination with attester sign an unlimited number of DTBS/Rs with 4EP_Mass_Signature-creation_SFP in a row (**FMT_MOF.1/4EP_Mass_Signature**)

Additionally

QES-Two-PIN-Signatures only:

the signatory in combination with attester (**FDP_ACF.1/4EP_Mass_Signature-creation_SFP** and **FMT_MOF.1/4EP_Mass_Signature**) ensure that

1. one user is successfully authorized as signatory with subject S.Sigy and a second user is successfully authorized as Attester with subject S.Attester and
2. both the signatory and the attester intend to sign the following DTBS/Rs for the four eyes mass signature.

Notes:

1. "**FDP_ACC.1/4EP_Mass_Signature-creation_SFP**" and "**FDP_ACF.1/4EP_Mass_Signature-creation_SFP**",
2. "**FMT_MOF.1/4EP_Mass_Signature**" and

are added to contents of PP [BSI-PP0059-2009].

9.1.2.2 Different reasons for authentication

Note: This chapter is added to contents of PP [BSI-PP0059-2009].

OT.Sigy_SigF (Signature creation function for the legitimate signatory only) is ensured by re-authentication

1. according to **FIA_UAU.6/without_4EP** as follows:

QES-Germany and **QES-Switzerland** only:

1. S.Sigy
   a) before every single DTBS/R signature
   if S.Sigy is allowed to create a single signature.
2. S.Sigy
   a) before next signature after card reset
   b) or after Application Digital Signature (ADS) was left
   c) or otherwise before (N+1)-th DTBS/R signature in a row when limit for consecutive signatures is N
   if S.Sigy is allowed to create a limited number of signatures in a row.
3. S.Sigy
   a) before next signature after card reset
   b) or after ADS was left
   if S.Sigy is allowed to create unlimited mass signatures without four eyes principle in a row.

2. according to **FIA_UAU.6/with_4EP** as follows:

QES-Two-PIN-Signatures only:

1. S.Sigy and S.Attester
   1. before next signature after card reset
   2. or after ADS was left

   if S.Sigy in combination with attester (**FDP_ACF.1/4EP_Mass_Signature-creation_SFP** and **FMT_MOF.1/4EP_Mass_Signature**) is allowed to create unlimited mass signatures with four eyes principle in a row.

Note:

1. "**FIA_UAU.6/without_4EP**",
2. "**FIA_UAU.6/with_4EP**" and
3. "**FDP_ACF.1/4EP_Mass_Signature-creation_SFP**" and "**FMT_MOF.1/4EP_Mass_Signature**"

are added to contents of PP [BSI-PP0059-2009].

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 9: Functional Requirements Dependencies

Requirement	Dependencies	Fulfilled
FCS_CKM.1/RSA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/RSA, see note (3)
FCS_COP.1/RSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/RSA, see note (3)
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
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_Generation_SFP	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/ SCD/SVD_Generation_SFP, FMT_MSA.3, FMT_MSA.3/ 4EP_Mass_Signature
FDP_ACF.1/ Signature-creation_SFP	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/ Signature-creation_SFP, FMT_MSA.3, FMT_MSA.3/ 4EP_Mass_Signature
FDP_ACF.1/ SVD_Transfer_SFP	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/ SVD_Transfer_SFP, FMT_MSA.3, FMT_MSA.3/ 4EP_Mass_Signature
FDP_ACC.1/ 4EP_Mass_ Signature-creation_SFP	FDP_ACF.1	FDP_ACF.1/ 4EP_Mass_ Signature-Creation_SFP
FDP_ACF.1/ 4EP_Mass_ Signature-creation_SFP	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/ 4EP_Mass_ Signature-creation_SFP, FMT_MSA.3, FMT_MSA.3/ 4EP_Mass_Signature
FDR_RIP.1	No dependencies	n.a.
FDP_SDI.2/Persistent	No dependencies	n.a.
FDP_SDI.2/DTBS	No dependencies	n.a.
FIA_AFL.1/ Transport_PIN	FIA_UAU.1	FIA_UAU.1

FIA_AFL.1/PIN	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/PUK	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/Swiss_PIN	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.6/without_4EP	No dependencies	n.a.
FIA_UAU.6/with_4EP	No dependencies	n.a.
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MOF.1/ 4EP_Mass_Signature	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1/with_4EP, FMT_SMF.1/with_4EP
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/ Signatory	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/ Signature_Creation_SFP, FMT_SMR.1, FMT_SMF.1, FMT_SMR.1/with_4EP
FMT_MSA.1/ Signatory_Attester	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/ 4EP_Mass_ Signature_Creation_SFP, FMT_SMR.1/with_4EP, FMT_SMF.1/with_4EP
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, FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory
FMT_MSA.2/ 4EP_Mass_Signature	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	FDP_ACC.1/ SCD/SVD_Generation_SFP, FDP_ACC.1/ 4EP_Mass_ Signature_Creation SFP, FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1/with_4EP, FMT_MSA.1/ Signatory_Attester
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.3/	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Admin, FMT_MSA.1/

4EP_Mass_Signature		Signatory_Attester, FMT_SMR.1/with_4EP
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/Admin	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1, FMT_SMR.1/with_4EP, FMT_SMF.1/with_4EP
FMT_MTD.1/Signatory	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1 FMT_SMR.1/with_4EP, FMT_SMF.1/with_4EP
FMT_MTD.1/Attester	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1/with_4EP, FMT_SMF.1/with_4EP
FMT_MTD.1/ Swiss_Signatory_Modif.	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/ Swiss_Signatory_Unblo.	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/ Signatory_PIN_T	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1, FMT_SMR.1/with_4EP, FMT_SMF.1/with_4EP
FMT_MTD.1/ Attester_PIN_T	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1/with_4EP, FMT_SMF.1/with_4EP
FMT_MTD.1/ Swiss_Admin	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/ Swiss_Admin_PIN_T	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	No dependencies	n.a.
FMT_SMF.1/with_4EP	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FMT_SMR.1/with_4EP	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_EMSEC.1	No dependencies	n.a.

Notes:

1. Justification of "FCS_COP.1/SHA-2" can be found in chapter "Part ONE (general SFRs)", sub-chapter "Cryptographic support (FCS)", section "FCS_COP.1/SHA-2 *Cryptographic operation*".
2. Justification of "FCS_CKM.1/RSA" part "FCS_CKM.4/RSA" or "FCS_COP.1/RSA" part "FCS_CKM.4/RSA" can be found in chapter "Part ONE (general SFRs)", sub-chapter "Cryptographic support (FCS)", section "FCS_CKM.1/RSA *Cryptographic key generation*" or "FCS_COP.1/RSA *Cryptographic operation*".

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 section provides a description of the TOE's Security Services (SS), which show how the TOE meets each SFR of section "TOE Security Functional Requirements".

10.1.1 SS1 User Identification and Authentication

This Security Service is responsible for the identification and authentication of

QES-Germany and **QES-Switzerland** only:

the Administrator and Signatory (FMT_SMR.1)

QES-Two-PIN-Signatures only:

the Administrator, Signatory and Attester (FMT_SMR.1/with_4EP)

This implies that the TOE allows identification of the user before the authentication takes place (FIA_UAU.1). The TOE does not allow the execution of any TSF-mediated actions before the user is identified (FIA_UID.1), authenticated and associated with one of the roles.

Depending on lifecycle phase the administrator can get access to the card with two different keys:

1. The StartKey secures the card within the lifecycle phase MANUFACTURING.
   The administrator is implicitly identified within the lifecycle 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 is not known to the administrator. The command sequence changes the secret StartKey to a default value which is known to the administrator. It is recommended that the administrator change this default value to a value only known to him.
   With this administrator-known (but otherwise secret) value for the StartKey, the TOE's life cycle can be switched from the MANUFACTURING to the ADMINISTRATION phase, which ends by changing into the lifecycle phase OPERATIONAL.
2. An administrator defined key secures the personalization models.
   There are needs for the administrator to switch back from lifecycle phase OPERATIONAL to ADMINISTRATION. To do this the administrator have to define during lifecycle phase ADMINISTRATION a key which is stored on the card. This key is sent at lifecycle phase OPERATIONAL to the card. If the administrator sends the correct key he is successfully authenticated and he is able to switch to lifecycle phase ADMINISTRATION.

Within the lifecycle phase OPERATIONAL, the signatory or attester are 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 or Attester. The following types of VAD/RAD are defined for the TOE:

QES-Germany only:

- PIN to authenticate the user as Signatory
- PUK (optional) to unblock the blocked PIN (and Transport-PIN) by the signatory
- Transport-PIN for the first setting of the PIN (and PUK). The Transport-PIN is used to secure the TOE delivery process. After entering the correct Transport-PIN the signatory has to set his individual PIN (and PUK) value. Thereafter the PIN (and PUK) will be unblocked by the TOE.
- If the PUK value is created by the administrator, the PUK is already usable (unblocked) after card (and PUK letter) delivery to the signatory.

QES-Switzerland only:

- PIN to authenticate the user as Signatory
- PUK (optional) to unblock the blocked PIN (and Transport-PIN) by the administrator
- Transport-PIN for the first setting of the PIN. The Transport-PIN is used to secure the TOE delivery process. After entering the correct Transport-PIN the signatory has to set his individual PIN value. Thereafter the PIN will be unblocked by the TOE.
- If the PUK value is created by the administrator, the PUK is already usable (unblocked) by the administrator.

QES-Two-PIN-Signatures only:

- Two PINs to authenticate the users as Signatory and Attester
- Two PUKs (optional) to unblock the blocked PIN (and Transport-PIN) by the signatory and by the attester
- Two Transport-PINs for the first setting of the PIN (and PUK) for the signatory and the Attester. The Transport-PINs are used to secure the TOE delivery process. After entering the correct Transport-PINs the signatory and the attester have to set their individual PIN (and PUK) value. Thereafter both PINs (and PUKs) will be unblocked by the TOE.
- If the PUK value is created by the administrator, the PUK is already usable (unblocked) after card (and PUK letter) delivery to the signatory and attester.

Notes:

1. PUK (optional) means: The administrator may not provide a PUK.
2. "to unblock a Transport-PIN" means: If the administrator sets the PUK value the signatory or the attester can unblock a Transport-PIN if it has been blocked by too many unsuccessful authentication attempts, see below.
3. All PUKs have use counters. Therefore unlimited number of attempts to guess a Transport-PIN are not possible.

The TOE will check that the provided VAD is equal to the stored and individual value of the corresponding RAD (FIA_UAU.1). The number of unsuccessful consecutive authentication attempts by the user is limited to a value depending on the RAD length. Thereafter SS1 will block the RAD according to FIA_AFL.1/Transport_PIN, FIA_AFL.1/PUK and

QES-Germany and **QES-Two-PIN-Signatures** only:

FIA_AFL.1/PIN

QES-Switzerland only:

FIA_AFL.1/Swiss_PIN

The ability to modify or unblock the RAD of Signatory is restricted to

QES-Germany and **QES-Two-PIN-Signatures** only:

the signatory (FMT_MTD.1/Signatory).

QES-Switzerland only:

the signatory (FMT_MTD.1/Swiss_Signatory_Modifying) and to the administrator (FMT_MTD.1/Swiss_Signatory_Unblocking).

The ability to unblock the Transport-PIN is restricted to

QES-Germany only:

the signatory (FMT_MTD.1/Signatory_PIN_T)

QES-Two-PIN-Signatures only:

the signatory (FMT_MTD.1/Signatory_PIN_T) and the attester (FMT_MTD.1/Attester_PIN_T)

QES-Switzerland only:

the administrator (FMT_MTD.1/Swiss_Admin_PIN_T)

in case that the administrator sets the value of the PUK and the Transport-PIN has been blocked by too many unsuccessful authentication attempts. If the Transport-PIN is successfully used to unblock the PIN it cannot be unblocked by the PUK.

The ability to modify or unblock the RAD of Attester is restricted to

QES-Two-PIN-Signatures only:

the attester (FMT_MTD.1/Attester).

To modify or to unblock RAD the signatory or the attester have to provide

QES-Germany only:

- the correct Transport-PIN to unblock the PIN (and PUK) before the first use (FMT_SMF.1.1 (5)).
- the correct PIN to change resp. modify PIN or PIN length (in a specific interval which is set by the administrator by setting minimum and maximum length) (FMT_MTD.1/Signatory)
- the correct PUK (optional) to unblock the blocked PIN (FMT_MTD.1/Signatory)
- the correct PUK (optional) to change resp. modify PUK or PUK length (in a specific interval which is set by the administrator by setting minimum and maximum length) (FMT_MTD.1/Signatory)

QES-Two-PIN-Signatures only:

- the correct Transport-PIN to unblock the PIN (and PUK) before the first use (FMT_SMF.1.1/with_4EP (5)).
- the correct PIN to change resp. modify PIN or PIN length (in a specific interval which is set by the administrator by setting minimum and maximum length) (FMT_MTD.1/Signatory + FMT_MTD.1/Attester)
- the correct PUK (optional) to unblock the blocked PIN (FMT_MTD.1/Signatory + FMT_MTD.1/Attester)
- the correct PUK (optional) to change resp. modify PUK or PUK length (in a specific interval which is set by the administrator by setting minimum and maximum length) (FMT_MTD.1/Signatory + FMT_MTD.1/Attester)

To modify the RAD the Swiss signatory has to provide

QES-Switzerland only:

- the correct Transport-PIN to unblock the PIN before the first use (FMT_SMF.1.1 (5)).
- the correct PIN to change resp. modify the PIN (FMT_MTD.1/Swiss_Signatory_Modifying)
- the correct PIN to change resp. modify the PIN length (in a specific interval which is set by the Administrator by setting minimum and maximum length) (FMT_MTD.1/Swiss_Signatory_Modifying)

To unblock a blocked RAD of the Swiss signatory after use of correct Transport-PIN by the Swiss signatory the (Swiss) Administrator has to provide

QES-Switzerland only:

the correct PUK to unblock the blocked PIN (FMT_MTD.1/Swiss_Signatory_Unblocking).

To unblock a blocked RAD of the Swiss signatory after use of correct Transport-PIN by the Swiss signatory **in case that the Swiss signatory cannot remember his PIN** the (Swiss) Administrator has to provide

QES-Switzerland only:

the correct PUK

- to unblock the blocked PIN and then
- to modify the PIN of the Swiss signatory to a new value

known to the Swiss signatory (FMT_MTD.1/Swiss_Signatory_Unblocking).

Afterwards the Swiss signatory has to modify his PIN to a value only known to him.

To modify PUK the (Swiss) Administrator has to provide

QES-Switzerland only:

- the correct PUK to change resp. modify the PUK (FMT_MTD.1/Swiss_Admin)
- the correct PUK to change resp. modify the PUK length (in a specific interval which is set by the Administrator by setting minimum and maximum length in lifecycle phase ADMINISTRATION) (FMT_MTD.1/Swiss_Admin)

The ability to initially create

- the RADs (PIN/PUK) for the signatory or for the attester and
- the Transport-PIN(s)

is restricted to the Administrator (FMT_MTD.1/Admin). The individual PIN (and PUK) value is set by the signatory (FMT_SMF.1 (5)) and attester (FMT_SMF.1/with_4EP (5)) after successful authentication with the Transport-PIN.

QES-Germany only:

The PUK value might also be created by the Administrator and can in this case be used to unblock the Transport-PIN (FMT_MTD.1/Signatory_PIN_T), if it has been blocked by too many unsuccessful authentication attempts (FIA_AFL.1/Transport_PIN). If, however, the Transport-PIN is blocked after its successful use, it cannot be unblocked anymore.

QES-Two-PIN-Signatures only:

The PUKs value might also be created by the Administrator and can in this case be used to unblock the Transport-PIN (FMT_MTD.1/Signatory_PIN_T + FMT_MTD.1/Attester_PIN_T) and if it has been blocked by too many unsuccessful authentication attempts (FIA_AFL.1/Transport_PIN). If, however, the Transport-PIN is blocked after its successful use, it cannot be unblocked anymore.

Signature creation functionality of the TOE without four eyes principle:

QES-Germany and **QES-Switzerland** only:

The successful authentication with the Transport-PIN which is possible only once, also changes the value of the attribute "SCD operational" from "no" to "yes", see also SS2 Access Control.

Four eyes mass signature creation functionality of the TOE:

QES-Two-PIN-Signatures only:

The successful authentication with the Transport-PINs of signatory and attester which is possible only once for both Transport-PINs, also changes the value of the attribute "SCD operational" from "no" to "yes", see also SS2 Access Control.

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_EMSEC.1). Further protection functionality is covered by SS5 Protection.

The TOE ensures re-authentication of the signatory (FIA_UAU.6/without_4EP):

QES-Germany and **QES-Switzerland** only:

1. after each signature
   if the personalization allows only a single signature
2. before the (N+1)-th signature or after card reset or after ADS was left
   if the personalization allows N signatures without four eyes principle
3. after card reset or after ADS was left
   if the personalization allows unlimited signatures without four eyes principle.

The TOE ensures re-authentication of the signatory and the attester (FIA_UAU.6/with_4EP):

QES-Two-PIN-Signatures only:

1. after card reset or after ADS was left

10.1.2 SS2 Access Control

This Security Service is responsible for the realization of Signature-creation SFP. The security attributes used for these policies are stated in Table 3: Security Attributes and related Status for the Subjects and Objects (in case of signatures without 4EP) for **QES-Germany** and **QES-Switzerland** and stated in Table 5: Security Attributes and related Status for the Subjects and Objects (in case of signatures with 4EP) for **QES-Two-PIN-Signatures**. Generally, this access control policy is assigned to user roles. The identification, authentication and association of users to roles is realized by SS1 User Identification and Authentication (FMT_SMR.1 and FMT_SMR.1/with_4EP).

SS2 controls the access to the

QES-Germany and **QES-Switzerland** only:

signature creation functionality of the TOE without four eyes principle:

The TOE allows the 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 behavior without Four Eyes Principle):

a) the security attribute "SCD operational" is set to "yes" (FMT_MSA.2 Secure security attributes without

Four Eyes Principle).
b) the signature request is sent by an authorized signatory, see also SS1 User Identification and Authentication.

and

QES-Two-PIN-Signatures only:

four eyes mass signature creation functionality of the TOE:

The TOE allows the generation of a signature if and only if (FDP_ACC.1/4EP_Mass_Signature-creation_SFP, FDP_ACF.1/4EP_Mass_Signature-creation_SFP and FMT_MOF.1/4EP_Mass_Signature):

a) the security attribute "SCD operational" is set to "yes" (FMT_MSA.2/4EP_Mass_Signature)
b) the signature request is sent by an authorized signatory in combination with an authorized attester, see also SS1 User Identification.

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, FMT_MSA.3/4EP_Mass_Signature and FMT_MSA.4). Thereafter only the signatory (in case of signatures without four eyes principle) is allowed to modify the security attribute "SCD operational" (FMT_MSA.1/Signatory and FMT_SMF.1 (2)) or the signatory and the attester (in case of signatures with four eyes principle) are allowed to modify the security attribute "SCD operational" (FMT_MSA.1/Signatory_Attester and FMT_SMF.1/with_4EP (3)) depending on:

QES-Germany and **QES-Switzerland** only:

1. signature creation functionality of the TOE without four eyes principle.
   The security attribute "SCD operational" is set to "yes" by the TOE (FMT_MSA.1/Signatory and FMT_SMF.1 (2)) after the signatory has successfully authenticated himself with the Transport-PIN and unblocked the PIN, see also SS1 User Identification and Authentication.

QES-Two-PIN-Signatures only:

1. Four eyes mass signature creation functionality of the TOE.
   The security attribute "SCD operational" is set to "yes" by the TOE (FMT_MSA.1/Signatory_Attester and FMT_SMF.1/with_4EP (3)) after the signatory and attester have successfully authenticated themselves with their Transport-PIN and unblocked their PIN, see also SS1 User Identification and Authentication.

Modifying and unblocking of RAD:

QES-Germany only:

Only the signatory is allowed to modify or unblock his or her RAD in form of the PIN (FMT_MTD.1/Signatory and FMT_SMF.1 (1) + (5)), see also SS1 User Identification and Authentication.

QES-Two-PIN-Signatures only:

Only the signatory is allowed to modify or unblock his or her RAD in form of the PIN (FMT_MTD.1/Signatory and FMT_SMF.1/with_4EP (1) + (5)), see also SS1 User Identification and Authentication.

Only the attester is allowed to modify or unblock his or her RAD in form of the PIN (FMT_MTD.1/Attester and FMT_SMF.1/with_4EP (1) + (5)), see also SS1 User Identification and Authentication.

QES-Switzerland only:

Only the Swiss signatory is allowed to modify his or her RAD in form of the PIN (FMT_MTD.1/Swiss_Signatory_Modifying and FMT_SMF.1 (1)), see also SS1 User Identification and Authentication.

Only the Swiss administrator is allowed to unblock the RAD in form of the PIN of signatory (FMT_MTD.1/Swiss_Signatory_Unblocking).

The Transport-PIN cannot be modified and can be used only once.

QES-Germany only:

If the value of the optional PUK is initialized by the Administrator the Transport-PIN can be unblocked (FMT_MTD.1/Signatory_PIN_T), if it has been blocked by too many unsuccessful authentication attempts (FIA_AFL.1/Transport_PIN).

QES-Switzerland only:

If the value of the optional PUK is initialized by the Administrator the Transport-PIN can be unblocked (FMT_MTD.1/Swiss_Admin_PIN_T), if it has been blocked by too many unsuccessful authentication attempts (FIA_AFL.1/Transport_PIN).

QES-Two-PIN-Signatures only:

If the values of the optional PUKs are initialized by the Administrator the Transport-PINs can be unblocked (FMT_MTD.1/Signatory_PIN_T + FMT_MTD.1/Attester_PIN_T), if they have been blocked by too many unsuccessful authentication attempts (FIA_AFL.1/Transport_PIN).

Note: "optional PUK" means: The administrator may not provide a PUK.

If, however, the Transport-PIN is blocked after its successful use, it cannot be unblocked anymore.

The optional PUK (the administrator may not provide a PUK), if unblocked, can always be modified after entering the correct PUK. A PUK can be unblocked only once by Transport-PIN. A PUK can never be unblocked if it has been blocked by too many unsuccessful authentication attempts.

QES-Two-PIN-Signatures only:

The mass signature with four eyes principle with two PINs can only be used for the generation of mass signatures, if both the signatory and the attester are present to enter their respective PINs (FDP_ACC.1/4EP_Mass_Signature-creation_SFP, FDP_ACF.1/4EP_Mass_Signature-creation_SFP). The personal PIN (and PUK) of the signatory and the attester can only be set by the signatory (FMT_MTD.1/Signatory) or by the attester (FMT_MTD.1/Attester) after the corresponding Transport-PIN entry. A Transport-PIN is blocked after too many unsuccessful authentication attempts (FIA_AFL.1/Transport_PIN). The Transport-PINs cannot be modified or unblocked and can be used only once. The signatory and the attester are allowed to modify or unblock their RAD in form of their personal PIN (and PUK). A blocked PUK (optional) can never be unblocked or only once (by Transport-PIN).

Note: "optional PUK" means: The administrator may not provide a PUK.

10.1.3 SS3 SCD/SVD Pair Generation

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

The TOE generates RSA signature key pairs with a module length of 1976 up to 4096 bits (FCS_CKM.1/RSA). The generation is done with secure values for SCD/SVD parameters so that the key pairs fulfill the corresponding requirements of [Geeignete-Algorithmen] for RSA key pairs (FMT_MSA.2, FMT_MSA.2/4EP_Mass_Signature and FCS_CKM.1/RSA). For the generation of primes used for the key pair a GCD (Greatest Common Divisor) test and enough rounds of the Rabin Miller Test are performed. The TOE uses the True Random Number Generator (TRNG) 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_EMSEC.1), see also SS5 Protection.

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 export of the SVD is ensured by FDP_ACC.1/SVD_Transfer_SFP and FDP_ACF.1/SVD_Transfer_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, see Table 3: Security Attributes and related Status for the Subjects and Objects (in case of signatures without 4EP) and Table 5: Security Attributes and related Status for the Subjects and Objects (in case of signatures with 4EP). The Administrator can set/change security attribute "SCD identifier" to a desired value (FMT_SMF.1 (4) and FMT_SMF.1/with_4EP (4)). The Administrator is thus able to override the default values when an object or information (here: SCD) is created (FMT_MSA.3 and FMT_MSA.3/4EP_Mass_Signature).

10.1.4 SS4 Signature Creation

This Security Service is responsible for signature creation (FCS_COP.1/RSA) using the SCD of the signatory (in case of signatures without/with four eyes principle). Before a signature is generated by the TOE, the signatory has to be authenticated successfully, see SS1 User Identification and Authentication.

Before mass signatures with four eyes principle, which require the entry of two PINs, are generated by the TOE, both the signatory and the attester have to be authenticated successfully, see SS1 User Identification and Authentication.

Mass signatures with or without four eyes principle are allowed only in a trusted environment.

The signatory is informed if stored data is altered (FDP_SDI.2/Persistent and FDP_SDI.2/DTBS).

10.1.4.1 Signature Creation with RSA

Technically, SS4 generates RSA signatures for hash values with RSASSA-PKCS1-v1_5 or RSASSA-PSS padding using the SCD of the signatory (FCS_COP.1/RSA). The signatures generated by this Security Service meet the following standards:

- [RSA-PKCS1-v2.1]
- [Geeignete-Algorithmen]

The Security Service supports RSA key length from 1976 to 4096 bits (FCS_COP.1/RSA).

10.1.4.2 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 SS2 Access Control.

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_EMSEC.1). It is furthermore not possible to gain unauthorized access to the SCD using the physical contacts of the underlying hardware. The certificate [CF-IFX-Chip-B11-MaintRep] which is an addendum to [CF-IFX-Chip-A21] of the chip SLE78CFX*P (M7892 B11) (Common Criteria level EAL 5+) cover the RSA functionality for signature creation.

10.1.4.3 TOE generated hash values

In the case that DTBS instead of a hash value (DTBS/R) is sent to the TOE under the control of the Signature-creation SFP, see SS2 Access Control, the TOE directly generates a hash value over the sent DTBS first

QES-Germany and **QES-Switzerland** only:

(FCS_COP.1/SHA-2 + FMT_SMF.1)

QES-Two-PIN-Signatures only:

(FCS_COP.1/SHA-2 + FMT_SMF.1/with_4EP)

which is used afterwards 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_EMSEC.1). It is furthermore not possible to gain unauthorized access to the SCD using the physical contacts of the underlying hardware. The certificate [CF-IFX-Chip-B11-MaintRep] which is an addendum to [CF-IFX-Chip-A21] of the chip SLE78CFX*P (M7892 B11) (Common Criteria level EAL 5+) cover the RSA bit functionality for signature creation and the SHA-2 v1.01 library, which is used here.

10.1.5 SS5 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 [Chip-Data-Book], 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 (section "SS3 SCD/SVD Pair Generation") (FPT_TST.1.1 (1)) and during signature creation (section "SS4 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 section "SS3 SCD/SVD Pair Generation" is demonstrated by performing the following checks:

- The TOEs life cycle phase is checked. Only Administrator can perform SCD/SVD pair generation.
- Before a random number from the TRNG 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 TRNG status register.
- All command parameters are checked for consistency.
- Access rights are checked.

- The right to generate a RSA key pair is checked (key pair generation allowed only once).

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).

SS5 actively destructs 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 have the user data attribute "integrity checked persistent stored data":

- SCD
- RAD
- SVD

If the integrity of SCD, RAD or SVD 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. section "SS1 User Identification and Authentication") for a certain action (cf. section "SS2 Access Control").

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 10: 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_EMSEC.1
FDP_IFC.1	Subset Information Flow Control	FPT_EMSEC.1
FPT_ITT.1	Basic Internal TSF Data Transfer Protection	FPT_EMSEC.1
FCS_RNG.1	Quality Metric for Random Numbers	FCS_CKM.1/RSA (Signature Key Pair generation) FPT_EMSEC.1 (blinding)
FPT_TST.2	Subset TOE Security Testing	FPT_TST.1 FPT_PHP.3 (active shield and sensors)
FCS_COP.1/AES	Cryptographic Support (AES)	no conflicts with TSF
FCS_COP.1/RSA	Cryptographic Support (RSA)	FCS_COP.1/RSA
FCS_CKM.1/RSA	Cryptographic Key Generation (RSA)	FCS_CKM.1/RSA
FCS_COP.1/SHA	Cryptographic operation (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 Initialization	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 11: 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

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 12: 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 are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are 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 Personalization: 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	automatically fulfilled (CfPA)	Will automatically be fulfilled by application of the security assurance requirements of the families ALC_DVS and ALC_DEL

	of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).		
dedicatedly defined in [ST-IFX-Chip-B11-Maint]			
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