

# **CombICAO Applet v3 on ID-One Cosmo X (SSCD Configuration) Public Security Target**

Reference: FQR 550 0284 Ed 5 - ST



## About IDEMIA

OT-Morpho is now IDEMIA, the global leader in trusted identities for an increasingly digital world, with the ambition to empower citizens and consumers alike to interact, pay, connect, travel and vote in ways that are now possible in a connected environment.

Securing our identity has become mission critical in the world we live in today. By standing for Augmented Identity, we reinvent the way we think, produce, use and protect this asset, whether for individuals or for objects. We ensure privacy and trust as well as guarantee secure, authenticated and verifiable transactions for international clients from Financial, Telecom, Identity, Security and IoT sectors.

With close to €3bn in revenues, IDEMIA is the result of the merger between OT (Oberthur Technologies) and Safran Identity & Security (Morpho). This new company counts 14,000 employees of more than 80 nationalities and serves clients in 180 countries.



## DOCUMENT EVOLUTION

Date	Version	Name	Revision
29/11/2021	Ed 1	IDEMIA	Sanitized version created for Public Issue.
01/02/2022	Ed 2	IDEMIA	Sanitized version created for Public Issue after incorporating ANSSI feedbacks.
16/01/2023	Ed 3	IDEMIA	Remove BIO PIN from Evaluation scope see chapters 3.4.3 and 6.1.2. Update [AGD_PRE], [AGD_OPE], [ST_PTF] and [PTF_CERT] references
28/03/2023	Ed 4	IDEMIA	Update [PTF_CERT] and [ST_PTF] references.
19/07/2023	Ed 5	IDEMIA	Update [PTF_CERT] and [ST_PTF] references. Add ALC_FLR.1

## Table of contents

1.1	ST IDENTIFICATION .....	9
1.2	TOE REFERENCE .....	9
2.1	TECHNICAL TERMS .....	10
2.2	ABBREVIATIONS .....	20
2.3	REFERENCES.....	22
3.1	TOE OVERVIEW .....	27
3.2	TOE DESCRIPTION .....	28
3.2.1	<i>Physical scope of the TOE</i> .....	30
3.2.2	<i>Logical scope of the TOE</i> .....	30
3.3	REQUIRED NON-TOE HARDWARE/SOFTWARE/FIRMWARE .....	32
3.4	TOE USAGE AND MAJOR SECURITY FEATURES OF THE TOE.....	32
3.4.1	<i>Keys and PINs</i> .....	34
3.4.2	<i>Access Control Management</i> .....	34
3.4.3	<i>Authentication of entities</i> .....	34
3.4.4	<i>Digital Authentication</i> .....	34
3.4.5	<i>Electronic Services</i> .....	35
3.4.6	<i>Trusted Channel function</i> .....	35
3.4.7	<i>Secure execution</i> .....	35
4.1	DEVELOPMENT ENVIRONMENT .....	37
4.2	PRODUCTION ENVIRONMENT .....	37
4.3	PREPARATION ENVIRONMENT.....	49
4.4	OPERATIONAL ENVIRONMENT .....	49
5.1	COMMON CRITERIA CONFORMANCE CLAIM .....	50
5.2	PROTECTION PROFILE CONFORMANCE CLAIM .....	50
5.3	PACKAGE CLAIM .....	51
5.4	CONFORMANCE RATIONALE .....	51
5.4.1	<i>Additional Assets</i> .....	58
5.4.2	<i>Additional Subjects</i> .....	59
5.4.3	<i>Additional Threats</i> .....	59
5.4.4	<i>Additional Organisational Security Policies</i> .....	59
5.4.5	<i>Additional Security Objectives</i> .....	60
5.4.6	<i>Additional Security Objectives for the Operational Environment</i> .....	60
5.4.7	<i>Additional Security Functional Requirements</i> .....	60
6.1	ASSETS .....	62
6.1.1	<i>Assets from Protection Profiles</i> .....	62
6.1.2	<i>Additional Assets</i> .....	62
6.2	USERS / SUBJECTS .....	64
6.2.1	<i>Subjects from Protection Profiles</i> .....	64
6.2.2	<i>Threat agents</i> .....	65
6.2.3	<i>Additional Subjects</i> .....	65
6.3	THREATS .....	66
6.3.1	<i>Threats drawn from the Protection Profiles</i> .....	66
6.3.2	<i>Additional Threats</i> .....	67
6.4	ORGANIZATIONAL SECURITY POLICIES .....	70
6.4.1	<i>Security Policies drawn from the Protection Profiles</i> .....	70
6.4.2	<i>Additional Security Policies</i> .....	70
6.5	ASSUMPTIONS.....	73
6.5.1	<i>All SSCD parts</i> .....	73

6.5.2	<i>Parts 3 and 6 only</i> .....	73
7.1	SECURITY OBJECTIVES FOR THE TOE.....	74
7.1.1	<i>All SSCD parts</i> .....	74
7.1.2	<i>SSCD parts 2, 4 and 5 only</i> .....	75
7.1.3	<i>SSCD parts 3 and 6 only</i> .....	75
7.1.4	<i>SSCD part 4 only</i> .....	75
7.1.5	<i>SSCD parts 5 and 6 only</i> .....	76
7.1.6	<i>Additional Security Objectives for the TOE</i> .....	76
7.2	SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT.....	79
7.2.1	<i>All SSCD parts</i> .....	79
7.2.2	<i>SSCD parts 2, 3 and 4 only</i> .....	80
7.2.3	<i>SSCD parts 2, 3, 5 and 6 only</i> .....	80
7.2.4	<i>SSCD parts 3 and 6 only</i> .....	80
7.2.5	<i>SSCD part 4 only</i> .....	81
7.2.6	<i>SSCD parts 5 and 6 only</i> .....	81
7.2.7	<i>Additional Security Objectives for the Operational Environment</i> .....	82
7.3	SECURITY OBJECTIVES RATIONALE.....	84
7.3.1	<i>Threats</i> .....	84
7.3.2	<i>Organizational Security Policies</i> .....	89
7.3.3	<i>Assumptions</i> .....	93
7.3.4	<i>SPD and Security Objectives</i> .....	94
8.1	EXTENDED FAMILIES.....	103
8.1.1	<i>Extended Family FPT_EMS - TOE Emanation</i> .....	103
8.1.2	<i>Extended Family FMT_LIM - Limited capabilities</i> .....	104
8.1.3	<i>Extended Family FIA_API - Authentication Proof of Identity</i> .....	105
8.1.4	<i>Extended Family FCS_RND - Generation of random numbers</i> .....	106
9.1	SECURITY FUNCTIONAL REQUIREMENTS.....	108
9.1.1	<i>Security Attributes</i> .....	108
9.1.2	<i>All SSCD parts</i> .....	109
9.1.3	<i>SSCD parts 2, 4 and 5 only</i> .....	116
9.1.4	<i>SSCD parts 3 and 6 only</i> .....	119
9.1.5	<i>SSCD part 4 only</i> .....	121
9.1.6	<i>SSCD parts 5 and 6 only</i> .....	122
9.1.7	<i>Additional SFRs</i> .....	123
9.2	SECURITY ASSURANCE REQUIREMENTS.....	137
9.2.1	<i>ADV Development</i> .....	137
9.2.2	<i>AGD Guidance documents</i> .....	142
9.2.3	<i>ALC Life-cycle support</i> .....	144
9.2.4	<i>ASE Security Target evaluation</i> .....	149
9.2.5	<i>ATE Tests</i> .....	156
9.2.6	<i>AVA Vulnerability assessment</i> .....	158
9.3	SECURITY REQUIREMENTS RATIONALE .....	159
9.3.1	<i>Objectives</i> .....	159
9.3.2	<i>Rationale tables of Security Objectives and SFRs</i> .....	168
9.3.3	<i>Dependencies</i> .....	176
9.3.4	<i>Rationale for the Security Assurance Requirements</i> .....	182
9.3.5	<i>AVA_VAN.5 Advanced methodical vulnerability analysis</i> .....	182
9.3.6	<i>ALC_DVS.2 Sufficiency of security measures</i> .....	182
9.3.7	<i>ALC_FLR.1 Basic flaw remediation</i> .....	183



10.1 TOE SUMMARY SPECIFICATION ..... 184

10.2 SFRs AND TSS ..... 189

    10.2.1 SFRs and TSS - Rationale ..... 189

    10.2.2 Association tables of SFRs and TSS ..... 196



Table of figures

Figure 1 TOE's logical architecture ..... 31

Figure 2 Life cycle Overview ..... 36

## Table of tables

Table 1 Different evaluated configurations of the CombICAO application .....	28
Table 2 : Development R&D Sites .....	37
Table 3 : Audited Production Sites .....	38
Table 4 Option 1: Both Platform and Applet packages are loaded at IC Manufacturer Site...	38
Table 5 Option 2: Both Platform and Applet packages are loaded at CC Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites .....	39
Table 6 Option 3(a): Platform package is loaded at IC Manufacturer Site and Applet package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites through GP Mechanism .....	40
Table 7 Platform package is loaded at IC Manufacturer Site and Applet package is loaded through resident application using LSK format or DUMP Package in Ciphred format is loaded .....	42
Table 8 Option 3(c): Platform package is loaded at IC Manufacturer Site and Applet package in plain format is loaded at Audited IDEMIA Sites only .....	43
Table 9 Option 4(a): Platform package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites and Applet package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites through GP Mechanism.....	45
Table 10 Platform package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites and Options and Applet package is loaded through Resident application using LSK format or DUMP Package in Ciphred format is loaded .....	47
Table 11 Option 4(c): Platform package is loaded at IC Manufacturer Site and Applet package in plain format is loaded at CC Audited IDEMIA Sites only .....	48
Table 12 Common Criteria conformance claim.....	50
Table 13 PP SPDs vs. ST .....	53
Table 14 PP Security Objectives vs. ST .....	55
Table 15 PP SFRs vs. ST .....	58
Table 16 Threats and Security Objectives - Coverage .....	95
Table 17 Security Objectives and Threats - Coverage .....	97
Table 18 OSPs and Security Objectives - Coverage.....	99
Table 19 Security Objectives and OSPs - Coverage.....	101
Table 20 Assumptions and Security Objectives for the Operational Environment - Coverage .....	101
Table 21 Security Objectives for the Operational Environment and Assumptions - Coverage .....	102
Table 22 Security Objectives and SFRs - Coverage .....	171
Table 23 SFRs and Security Objectives.....	176
Table 24 SFRs Dependencies.....	181
Table 25 SARs Dependencies .....	182
Table 26 SFRs and TSS - Coverage .....	199
Table 27 TSS and SFRs - Coverage .....	200



# 1 Security Target Introduction

---

## 1.1 ST Identification

<b>Title</b>	CombICAO Applet v3 on ID-One Cosmo X (SSCD Configuration) Public Security Target
<b>ST Identification</b>	FQR 550 0284 Ed 5
<b>CC Version</b>	3.1 revision 5
<b>Assurance Level</b>	EAL5 augmented with ALC_DVS.2, ALC_FLR.1 and AVA_VAN.5
<b>ITSEF</b>	CEA-LETI
<b>Certification Body</b>	ANSSI
<b>Compliant to Protection Profile</b>	[PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6]

## 1.2 TOE Reference

<b>TOE Commercial Name</b>	CombICAO Applet v3 in SSCD configuration on ID-One Cosmo X
<b>Applet Code Versions (SAAAAR Code)</b>	'20 37 42 FF'
<b>Applet Internal Version</b>	'00 00 02 0D'
<b>Platform Name</b>	ID-One Cosmo X
<b>Platform Certificate</b>	[PTF_CERT]
<b>Guidance Documents</b>	[AGD_PRE], [AGD_OPE].

## 2 Technical Terms, Abbreviations and Associated References

### 2.1 Technical Terms

Term	Definition
<i>Agreement</i>	This term is used in the current ST in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
<i>Application note</i>	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7).
<i>Authenticity</i>	Ability to confirm the travel document and its data elements on the travel document's chip were created by the issuing State or Organization
<i>Basic Access Control</i>	Security mechanism defined in [ICAO_9303] by which means the travel document's chip proves and the inspection system protect their communication by means of secure messaging with Basic Access Keys (see there).
<i>Biographical data (bio data).</i>	The personalised details of the bearer of the travel document appearing as text in the visual and machine readable zones on the biographical data page of a travel document [ICAO_9303].
<i>Biometric reference data</i>	Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) digital portrait and (ii) optional biometric reference data.
<i>Card Access Number (CAN)</i>	Password derived from a short number printed on the front side of the data-page.
<i>Certificate chain</i>	A sequence defining a hierarchy certificates. The Inspection System Certificate is the lowest level, Document Verifier Certificate in between, and Country Verifying Certification Authority Certificates are on the highest level. A certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level.
<i>Counterfeit</i>	An unauthorized copy or reproduction of a genuine security document made by whatever means.
<i>Country Signing CA Certificate (C<sub>CSA</sub>)</i>	Self-signed certificate of the Country Signing CA Public Key (K <sub>PU CSA</sub> ) issued by CSA stored in the inspection system.
<i>Country Signing Certification Authority (CSCA)</i>	An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the

Term	Definition
	<p>PKI for the travel documents and creates the Document Signer Certificates within this PKI.</p> <p>The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [ICAO_9303], 5.5.1.</p> <p>The Country Signing Certification Authority issuing certificates for Document Signers (cf. [6]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [TR-03110-3].</p>
<p><i>Country Verifying Certification Authority (CVCA)</i></p>	<p>An organisation enforcing the privacy policy of the travel document Issuer with respect to protection of user data stored in the travel document (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the terminals using it and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [TR-03110-3].</p> <p>Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a CVCS as a subject; hence, it merely represents an organizational entity within this ST.</p> <p>The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [ICAO_9303]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [TR-03110-3].</p>
<p><i>Current date</i></p>	<p>The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.</p>
<p><i>CV Certificate</i></p>	<p>Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.</p>
<p><i>CVCA link Certificate</i></p>	<p>Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.</p>

Term	Definition
<i>Document Details Data</i>	Data printed on and electronically stored in the travel document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
<i>Document Security Object (SO<sub>D</sub>)</i>	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the travel document's chip. It may carry the Document Signer Certificate (CDS). [ICAO_9303]
<i>Document Signer (DS)</i>	<p>An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication.</p> <p>A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS), see [ICAO_9303].</p> <p>This role is usually delegated to a Personalisation Agent.</p>
<i>Document Verifier (DV)</i>	<p>An organisation enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organisation / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a Certification Authority, authorised by at least the national CVCA to issue certificates for national terminals, see [TR-03110-3].</p> <p>Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a DV as a subject; hence, it merely represents an organisational entity within this ST.</p> <p>There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the travel document Issuer und a foreign CVCA ensuring enforcing the travel document Issuer's privacy policy) <sup>1 2</sup></p>
<i>Eavesdropper</i>	A threat agent with low attack potential reading the communication between the travel document's chip and the inspection system to gain the data on the travel document's chip.

<sup>1</sup> The form of such an agreement may be of formal and informal nature; the term 'agreement' is used in the current ST in order to reflect an appropriate relationship between the parties involved.

<sup>2</sup> Existing of such an agreement may be technically reflected by means of issuing a CCVCA-F for the Public Key of the foreign CVCA signed by the domestic CVCA.

Term	Definition
<i>Enrolment</i>	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO_9303]
<i>travel document (electronic)</i>	The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.
<i>ePassport application</i>	[PP-EAC] definition Non-executable data defining the functionality of the operating system on the IC as the travel document's chip. It includes the file structure implementing the LDS [ICAO_9303], the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and the TSF Data including the definition the authentication data but except the authentication data itself.
<i>Extended Access Control</i>	Security mechanism identified in [ICAO_9303] by which means the travel document's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalisation Agent may use the same mechanism to authenticate themselves with Personalisation Agent Authentication Private Key and to get write and read access to the logical travel document and TSF data.
<i>Forgery</i>	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait.
<i>Global Interoperability</i>	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all travel document's. [ICAO_9303]
<i>IC Dedicated Software</i>	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases.
<i>IC Dedicated Support Software</i>	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.

<b>Term</b>	<b>Definition</b>
<i>IC Dedicated Test Software</i>	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
<i>IC Embedded Software</i>	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
<i>IC Identification Data</i>	The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.
<i>Impostor</i>	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document.
<i>Improperly documented person</i>	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [ICAO_9303]
<i>Initialisation</i>	Process of writing Initialisation Data (see below) to the TOE (TOE life-cycle, Phase 2 Manufacturing, Step 3).
<i>Initialisation Data</i>	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as travel document material (IC identification data).
<i>Inspection</i>	The act of a State examining an travel document presented to it by a traveller (the travel document's holder) and verifying its authenticity. [ICAO_9303]
<i>Inspection system (IS)</i>	A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as travel document holder.
<i>Integrated circuit (IC)</i>	Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit.
<i>Integrity</i>	Ability to confirm the travel document and its data elements on the travel document's chip have not been altered from that created by the issuing State or Organization
<i>Issuing Organization</i>	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO_9303]]
<i>Issuing State</i>	The Country issuing the travel document. [ICAO_9303]

Term	Definition
<i>Logical travel document</i>	Data of the travel document holder stored according to the Logical Data Structure [ICAO_9303] as specified by ICAO on the contact based/contactless integrated circuit. It presents contact based/contactless readable data including (but not limited to) personal data of the travel document holder the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), the digitized portraits (EF.DG2), the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and the other data according to LDS (EF.DG5 to EF.DG16). EF.COM and EF.SOD
<i>Machine Readable Travel Document (MRTD)</i>	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [ICAO_9303]
<i>Machine Readable Zone (MRZ)</i>	Fixed dimensional area located on the front of the travel document or MRP Data Page or, in the case of the TD1, the back of the travel document, containing mandatory and optional data for machine reading using OCR methods. [ICAO_9303].
<i>Machine-verifiable biometrics feature</i>	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO_9303]
<i>Manufacturer</i>	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
<i>Metadata of a CV Certificate</i>	Data within the certificate body (excepting Public Key) as described in [TR-03110-3]. The metadata of a CV certificate comprise the following elements: - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorisation Template, - Certificate Effective Date, - Certificate Expiration Date.
<i>Optional biometric reference data</i>	Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) encoded finger image(s) (DG3) or (ii) encoded iris image(s) (DG4) or (iii) both. Note that the European commission decided to use only finger print and not to use iris images as optional biometric reference data.

Term	Definition
<i>Password Authenticated Connection Establishment (PACE)</i>	A communication establishment protocol defined in [ICAO_9303] part 11. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password $n$ ). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
<i>PACE passwords</i>	Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [ICAO_9303] part 11 or a user PIN or PUK as specified in [TR-03110-3]
<i>Passive authentication</i>	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
<i>Personalisation</i>	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document. This may also include the optional biometric data collected during the "Enrolment" (cf. paragraph 1.7.4.3, TOE life-cycle, Phase 3, Step 6).
<i>Personalisation Agent</i>	<p>An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities:</p> <p>ICAO travel document</p> <ul style="list-style-type: none"> <li>(i) establishing the identity of the travel document holder for the biographic data in the travel document,</li> <li>(ii) enrolling the biometric reference data of the travel document holder,</li> <li>(iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [TR-03110-1],</li> <li>(iv) writing the document details data,</li> <li>(v) writing the initial TSF data,</li> <li>(vi) signing the Document Security Object defined in [ICAO_9303] (in the role of DS).</li> </ul> <p>Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer.</p> <p>Generating signature key pair(s) is not in the scope of the tasks of this role.</p>



<b>Term</b>	<b>Definition</b>
<i>Personalisation Data</i>	<p>A set of data incl. individual-related data (biographic and biometric data) of the travel document holder, dedicated document details data and dedicated initial TSF data (incl. the Document Security Object).</p> <p>Personalisation data are gathered and then written into the non-volatile memory of the TOE by the Personalisation Agent in the life-cycle phase card issuing.</p>
<i>Personalisation Agent Authentication Information</i>	TSF data used for authentication proof and verification of the Personalisation Agent.
<i>Personalisation Agent Key</i>	Symmetric cryptographic key or key set (MAC, ENC) used by the Personalisation Agent to prove his identity and get access to the logical travel document.
<i>Physical part of the travel document</i>	travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) biographical data, data of the machine-readable zone, photographic image and other data.
<i>Pre-personalisation</i>	Process of writing Pre-Personalisation Data (see below) to the TOE including the creation of the travel document Application (TOE life-cycle, Phase 2, Step 5)
<i>Pre-personalisation Data</i>	Any data that is injected into the non-volatile memory of the TOE by the travel document Manufacturer (Phase 2) for traceability of non-personalised travel document's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalisation Agent Key Pair and Chip Life-Cycle Production data (CPLC data).
<i>Pre-personalised travel document's chip</i>	travel document's chip equipped with a unique identifier.
<i>Receiving State</i>	The Country to which the travel document holder is applying for entry. [ICAO_9303]
<i>Reference data</i>	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.

<b>Term</b>	<b>Definition</b>
<i>RF-terminal</i>	A device being able to establish communication with an RF-chip according to ISO/IEC 14443 [ISO14443].
<i>Secondary image</i>	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means [ICAO_9303].
<i>Secure messaging in encrypted /combined mode</i>	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [ISO7816]
<i>Service Provider</i>	An official organisation (inspection authority) providing inspection service which can be used by the travel document holder.
<i>Skimming</i>	Imitation of a rightful terminal to get access to the user data stored on or transferred between the TOE and the Inspection authority connected via the contactless/contact communication channel of the TOE without knowledge of the MRZ, CAN, PIN and PUK PACE passwords.
<i>Standard Inspection Procedure [SIP]</i>	A specific order of authentication steps between an travel document and a terminal as required by [ICAO_9303] and [TR-03110-1], namely PACE or BAC and Passive Authentication with SO <sub>D</sub> .
<i>Inspection Procedure for multi-application travel document's</i>	This section describes an inspection procedure designed for travel document's containing one or more applications besides the travel document's application ("LDS2-documents"): [LDS2_TR] Annex A2.
<i>Terminal</i>	<p>A terminal is any technical system communicating with the TOE either through the contact based or contactless interface. A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter.</p> <p>In this ST the role 'Terminal' corresponds to any terminal being authenticated by the TOE.</p>
<i>Terminal Authorization</i>	Intersection of the Certificate Holder Authorizations of the Inspection System Certificate, the Document Verifier Certificate and Country Verifier Certification Authority which shall be valid for the Current Date.
<i>Terminal Authorisation Level</i>	Intersection of the Certificate Holder Authorisations defined by the Terminal Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
<i>TOE tracing data</i>	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document.
<i>travel document</i>	Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data

Term	Definition
	and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [ICAO_9303] (there "Machine readable travel document").
<i>travel document (electronic)</i>	The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: <i>ePassport</i> .
<i>travel document Holder</i>	The rightful holder of the travel document for whom the issuing State or Organisation personalised the travel document.
<i>travel document's Chip</i>	A contact based / contactless integrated circuit chip complying with ISO/IEC 14443 [15] and programmed according to the Logical Data Structure as specified by ICAO, [ICAO_9303], sec III.
<i>Traveller</i>	Person presenting the travel document to the inspection system and claiming the identity of the travel document holder.
<i>TSF data</i>	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [CC1]).
<i>Unpersonalised travel document</i>	The travel document that contains the travel document chip holding only Initialisation Data and Pre-personalisation Data as delivered to the Personalisation Agent from the Manufacturer.
<i>User data</i>	<p>All data (being not authentication data) stored in the context of the ePassport application of the travel document as defined in [5] and being allowed to be read out solely by an authenticated terminal.</p> <p>CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC2]).</p>
<i>Verification</i>	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [ICAO_9303]
<i>Verification data</i>	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

## 2.2 Abbreviations

<b>Acronym</b>	<b>Definition</b>
ADF	Application Dedicated File
BAC	Basic Access Control
BAT	Basic Authentication Terminal
CA	Chip Authentication
CAN	Card Access Number
CC	Common Criteria
CHAT	Certificate Holder Authorization Template
CLFDB	Ciphered Load File Data Block
CMT	Certificate Management Terminal
DES	Data Encryption Standard
DH	Diffie Hellman
DSK	Dump Secret Key
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EF	Elementary File
GP	Global Platform
IC	Integrated Chip
ICAO	International Civil Aviation Organization
ICC	Integrated Chip card
IS	Inspection System
LSK	Load Secure Key
MAC	Message Authentication code
MF	Master File
MRTD	Machine Readable Travel Document
MRZ	Machine readable zone
OE	Security Objectives for the Operational Environment
OSP	Organisational security policy
OT	Security Objectives for the TOE
PACE	Password Authenticated Connection Establishment
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMT	Password Management Terminal
PP	Protection Profile
PS	Personalisation System
PT	Personalisation Terminal
QSCD	Qualified Signature Creation Device
RF	Radio Frequency
ROM	Read Only Memory

RSA	Rivest Shamir Adleman
RSA CRT	Rivest Shamir Adleman – Chinese Remainder Theorem
SAR	Security Assurance Requirement
SCP	Secure Channel Procotol
SFR	Security functional requirement
SHA	Secure Hashing Algorithm
SIP	Standard Inspection Procedure
SSCD	Secure Signature Creation Device
ST	Security Target
TA	Terminal Authentication
TOE	Target Of Evaluation
TSF	TOE Security Functions

## 2.3 References

Reference	Description
[ADDENDUM]	20190821-Module-PP0056 - v1.1
[AGD_OPE]	FQR 220 1641 - CombICAO Applet V3 on ID-One Cosmo X - AGD_OPE
[AGD_PRE]	FQR 220 1640 - CombICAO Applet V3 on ID-One Cosmo X - AGD_PRE
[ANSSI_NOTE_10]	JIL – Certification of “open” smart card products – Version 1.1 – 4 February 2013
[ANSIX9.31]	“Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (DSA)” – ANSI X9.31-1998, American Bankers Association
[ANSIX9.62]	ANSI x9.62-2005 Public Key Cryptography for the Financial Services Industry – The Elliptic Curve Digital Signature Algorithm (ECDSA)
[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 5. April 2017. CCMB-2017-04-001.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-002.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1. Revision 5. April 2017. CCMB-2017-04-004.
[CEN_14890]	CEN/EN 14890:2013 Application Interface for smart cards used as Secure Signature Creation.
[Directive]	Directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on a community framework for electronic signatures
[eIDAS_Regulation]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[FIPS_180_4]	FIPS 180-4, Federal Information Processing Standards Publication (FIPS PUB) 180-4, Secure Hash Standard, August 2015
[FIPS_186_3]	FIPS 186-3, Federal Information Processing Standards Publication (FIPS PUB) 186-3, Digital Signature Standard (DSS), June 2009
[FIPS_197]	FIPS 197, Federal Information Processing Standards Publication (FIPS PUB 197), Advanced Encryption Standard (AES)
[FIPS_46_3]	FIPS 46-3, Federal Information Processing Standards Publication (FIPS PUB) 46-3, Data Encryption Standard (DES), 1999 October 25
[GP2.3]	Global Platform, Card Specification – Version 2.3 – October 2015.
[GPC_SPE_014]	GlobalPlatform Card Technology - Secure Channel Protocol '03', Card Specification v2.3 – Amendment D" Version 1.1.2 - Public Release March 2019
[GPC_SPE_034]	"GlobalPlatform Card Specification" Version 2.3.1 Public Release - March 2018
[ICAO_9303]	International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – 7 <sup>th</sup> and 8 <sup>th</sup> edition.
[IEEE]	IEEE Std 1363a-2004 Standard Specification of Public-Key Cryptography
[ISO_15946]	ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002
[ISO_18013-3]	ISO/IEC 18013-3: Information technology — Personal identification — ISO-compliant driving licence. Part 3: Access control, authentication and integrity validation, April, 2017
[ISO_TR_19446]	ISO/IEC TR 19446:2015 Differences between the driving licences based on the ISO/IEC 18013 series and the European Union specifications
[ISO_9796-2]	ISO/IEC 9796-2:2002 - Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Mechanisms using a hash-function

[ISO_9797_1]	ISO/IEC 9797-1 Information technology – Security techniques – Message Authentication codes (MACs) – part 1: Mechanisms using a block cipher, Second edition 2011-03-01
[ISO11770-2]	ISO/IEC 11770-2. Information Technology – Security techniques – Key management – part 2: Mechanisms using symmetric techniques, 1996
[ISO11770-3]	ISO/IEC 11770-3. Information Technology – Security techniques – Key management – part 3: Mechanisms using asymmetric techniques, 2015
[ISO14443]	ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2016
[ISO7816]	ISO/IEC 7816: Identification cards — Integrated circuit cards.
[NIST_800_38A]	NIST Special Publication 800-38A: 2001, <i>Recommendation for Block Cipher Modes of Operation: Methods and Techniques</i> , December 2001
[NIST_800_38B]	NIST Special Publication 800-38B: 2005, <i>Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication</i> , May 2005
[PKCS#1]	PKCS #1 v2.1: RSA Cryptography Standard – June 14, 2002
[PKCS#3]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4 Revised November 1, 1993
[PP_BAC]	Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control, BSI-CC-PP-0055-2009, Version 1.10, 25th March 2009
[PP_EAC]	EAC- Machine readable travel documents with "ICAO Application", Extended Access control – BSI-PP-0056 v1.10 25th march 2009
[PP_EACwPACE]	Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), BSI-CC-PP0056-V2-2012-MA-02, version 1.3.2, 5th December 2012
[PP_IC]	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014.



[PP_PACE]	Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011-MA-01, Version 1.01, 22 July 2014
[PP-SSCD2]	Protection profiles for secure signature creation device — Part 2: Device with key Generation, EN 419211-2 : 18 <sup>th</sup> May 2013, CEN/TC 224, BSI-CC-PP-0059-2009-MA-02, June 30 2016
[PP-SSCD3]	Protection profiles for secure signature creation device – Part3: Device with key import, EN 419211-3 : 14 <sup>th</sup> September 2013, CEN/TC 224, BSI-CC-PP-0075-2012-MA-01, June 30 2016
[PP-SSCD4]	Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application, EN 419211-4 : 12 <sup>th</sup> October 2013, CEN/TC 224, BSI-CC-PP-0071-2012-MA-01, June 30 2016
[PP-SSCD5]	Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application, EN 419211-5: 12 <sup>th</sup> October 2013, CEN/TC 224, BSI-CC-PP-0072-2012-MA-01, June 30 2016
[PP-SSCD6]	Protection profiles for secure signature creation device – Part6: Extension for device with key import and trusted communication with signature-creation application, EN 419211-6 : 25 <sup>th</sup> July, 2014, CEN/TC 224, BSI-CC-PP-0076-2013-MA-01, June 30 2016
[PTF_CERT]	NSCIB-CC-2300050-01
[QR_Guide]	FQR 220 1646 Ed 1 - CombICAO Applet V3 - Recommendations for Compatibility with QR
[RGS2_B1]	GUIDE DES MÉCANISMES CRYPTOGRAPHIQUES RÈGLES ET RECOMMANDATIONS CONCERNANT LE CHOIX ET LE DIMENSIONNEMENT DES MÉCANISMES CRYPTOGRAPHIQUES, Version 2.04 du 01 Janvier 2020
[SCP03]	Global Platform Card Technology, Secure Channel Protocol 03, Card Specification v 2.2 - Amendment D - Version 1.1 - September 2009
[ST_PTF]	Security Target Lite ID-ONE Cosmo X, FQR 110 A23D

[TR-03110-1]	Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26.02.2015 by BSI
[TR-03110-2]	Technical Guideline TR-03110-2, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 2 – Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.21, 21.12.2016 by BSI
[TR-03110-3]	TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3: Common Specifications, version 2.21, 21-12-2016 by BSI
[TR-03111]	Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 1.11, 17.04.2009

### 3 TOE Overview and Description

#### 3.1 TOE Overview

The TOE is a composite product made up of an embedded software developed using Java Card technology, composed on a Java Card open platform. Both are developed by IDEMIA. The Java Card open platform has already been certified. For more details see [PTF\_CERT].

The embedded software is made up of Java Card CombICAO Applet v3, which relies on Java Card API provided by the underlying Java Card open platform.

The CombICAO Applet v3 is a configurable applet designed primarily for Identification, Authentication, Signature generation, and as a Machine Readable Travel document (MRTD). This security target focuses on **Secure Signature Creation Device (SSCD)**. In addition, the product can be used as a **Qualified Signature Creation Device (QSCD)** used to create advanced or qualified signature in the sense of new [eIDAS\_Regulation] provided the appropriate [QR\_Guide] is respected.

In addition, the CombICAO Applet v3 supports the following secure authentication protocols defined in [TR-03110-1] and [TR-03110-3]:

- PACE protocol to ensure a trusted channel for secure communication between the TOE and a CGA and/or SCA, with
  - support for ECDH in Generic and Integrated Mapping modes (PACE-GM, PACE-IM),
  - MRZ, CAN, PIN and PUK passwords and
  - PIN/PUK suspend and resume mechanism
- Chip Authentication v1 (CAv1)
- Terminal Authentication v1 (TAv1)

The CombICAO Applet v3 is also evaluated in other configurations as mentioned in the Table below.

This ST considers the CombICAO Applet v3 in the **SSCD configuration**.

Configuration	PP Conformity	Extensions to the PP
BAC and CA	[PP_BAC]	<ul style="list-style-type: none"> <li>- Active Authentication (AA)</li> <li>- Chip Authentication Protocol (v1)</li> <li>- Restart secure messaging in AES128, AES192 or AES256 secure messaging (in addition to 3DES) after Chip Authentication Protocol (v1)</li> </ul>
EAC in combination with BAC	[PP_EAC]	<ul style="list-style-type: none"> <li>- Active Authentication (AA)</li> </ul>

Configuration	PP Conformity	Extensions to the PP
EAC with PACE	[PP_PACE]	- Active Authentication (AA)
	[PP_EACwPACE]	
EAC with PACE for French ID	[PP_PACE]	- [ADDENDUM] - Active Authentication (AA)
	[PP_EACwPACE]	
SSCD	[PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], and [PP-SSCD6]	- <b>ADMIN role</b> - <b>Integrity token</b> - <b>EAC v1 (Chip Authentication v1 and Terminal Authentication v1)</b> - <b>PACE</b>

**Table 1 Different evaluated configurations of the CombICAO application**

### 3.2 TOE Description

The TOE is compliant with the specification [CEN\_14890], with the following types of data structures:

- Files (MF, EF's and ADF's);
- Keys;
- PINs;

All these files are organized within a File System compliant to part 4 of [ISO7816]. It represents the hierarchy between all the files. At the top of the structure stands the Master File, it is the default selected file after applet selection. Under the Master File, are located the Application Dedicated File(s). The Master File, as well as each ADF, may contain Elementary File, keys and/or PINs.

Each file is characterized by its own attributes, such as:

- Access conditions for read and write access (for EF) or selection (for ADF);
- File identifier;
- Location within the File System;
- Size (for EF);



The TOE allows to:

- create two types of file (Application Dedicated File and Elementary File), which updates the File System;
- read, update, resize any Elementary File;
- move within the File Structure by use of file selection;

### **3.2.1 Physical scope of the TOE**

The TOE is physically made up of several components hardware and software. Once constructed, the TOE is a bare microchip with its external interfaces for communication.

The TOE may be used on several physical medium like wafer, module, smart card or inlay, eCover, eDatapage and eMRTD booklet.

The physical medium on which the microchip is mounted is not part of the target of evaluation as it does not alter nor modify any security functions of the TOE. Also, the inlay production (if any) including the application of the antenna is not part of the TOE

### **3.2.2 Logical scope of the TOE**

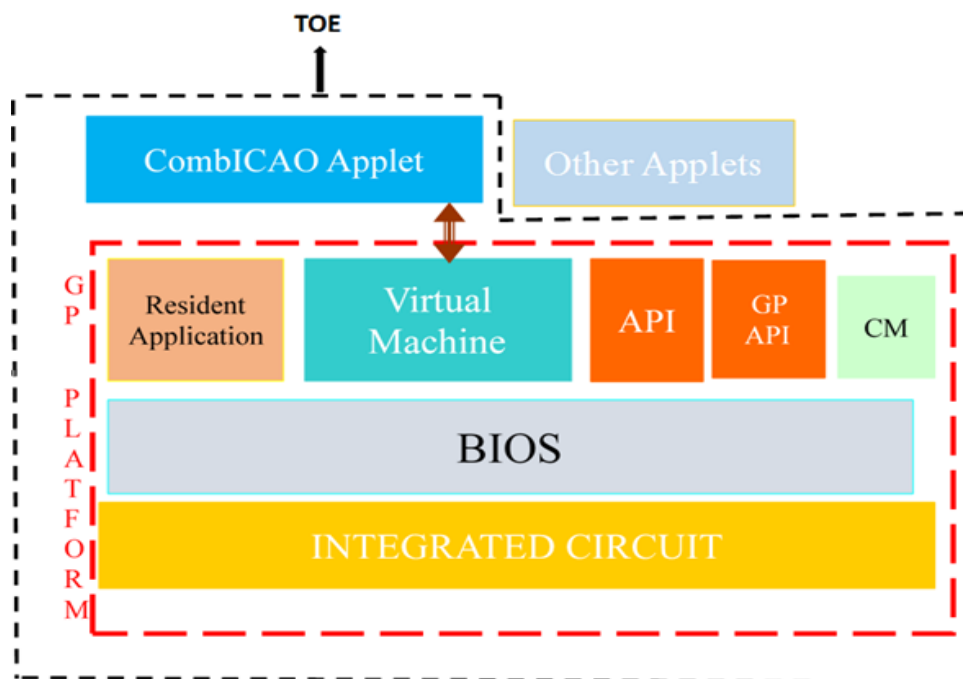
The TOE is made up of:

- The underlying Java Card open platform,
- The Java Card CombICAO Applet v3 code [Applet],
- The associated guidance documentation in [AGD\_PRE] and [AGD\_OPE] (delivered in electronic version),
- The (pre)personalization Agent Key sets.

Moreover, as the underlying platform is certified as a Java Card open platform and complies with the requirements of the Application note 10 [ANSSI\_NOTE\_10], and as the TOE complies also with [ANSSI\_NOTE\_10], the TOE may also contain any other applets that comply with [ANSSI\_NOTE\_10] and the specific requirements of the TOE stated in the guidance documents.

The TOE scope is shown in figure 1. Once constructed, the TOE is a bare microchip with its external interfaces for communication. The physical medium on which the microchip is mounted does not alter nor modify any security functions of the TOE.

A schematic overview of the TOE’s logical architecture is shown in below figure:



**Figure 1 TOE’s logical architecture**

The following guidance documents will be provided with the TOE:

Guidance	Audience	Form Factor of Delivery
[AGD_PRE]	Personalising Agent	Electronic Version
[AGD_OPE]	End user of the TOE	

The following guide is provided only in case compliancy with QR scheme is required:

Guidance	Purpose	Form Factor of Delivery
[QR_Guide]	Recommendations for QR	Electronic Version

This ST Lite version of this Security Target will also be provided along with above-mentioned documents.

Platform related guidance documents are mentioned in [ST\_PTF].

“Life Cycle” section in this ST provides more details about the TOE delivery for the different options.

### 3.3 Required non-TOE hardware/Software/firmware

The TOE is a Qualified Signature Creation Device. It is an independent product and does not need any additional hardware/software/firmware to ensure its security.

In order to be powered up and to be able to communicate, the TOE needs a reader.

### 3.4 TOE Usage and major security features of the TOE

The TOE intended usage is to be used as a “qualified signature creation device” with key generation and/or key import, with respect to the new [eIDAS\_Regulation].

Since the TOE claims compliancy to protection profiles from CEN-EN 419 211-2 to CEN-EN 419 211-6 (Signature Protection Profiles **[PP-SSCD2]**, **[PP-SSCD3]**, **[PP-SSCD4]**, **[PP-SSCD5]** and **[PP-SSCD6]**), the TOE can be used as (depending on its configuration during personalization):

- Config#1 claiming compliancy to CEN/EN 419 211-2/3/4/5/6 (**[PP-SSCD2]**, **[PP-SSCD3]**, **[PP-SSCD4]**, **[PP-SSCD5]** and **[PP-SSCD6]**).
- Config#2 claiming compliancy to CEN/EN 419 211-2/3/4 (**[PP-SSCD2]**, **[PP-SSCD3]**, **[PP-SSCD4]**). This configuration does not support the trusted channel between the TOE and the SCA.
- Config#3 claiming compliancy to CEN/EN 419 211-2/3 (**[PP-SSCD2]**, **[PP-SSCD3]**). This configuration does not support the trusted channel between: (i) the TOE and the SCA; (ii) the TOE and the CGA.

Within the framework described by **[PP-SSCD2]**, **[PP-SSCD3]**, **[PP-SSCD4]**, **[PP-SSCD5]** and **[PP-SSCD6]**, the TOE allows to:

- perform basic, advanced and qualified signature;
- authenticate the signatory thanks to PIN verification;
- authenticate one (or several) administrator(s) of the TOE, that may have special rights to administrate the SCD and SVD (generation, import);
- establish trusted channel, protected in integrity, authenticity and confidentiality, with trusted IT entities such as a CGA and SCA;
- Secure execution of services.



The scope of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6] is extended in several ways:

- Personalization phase including:
  - authentication protocol;
  - access control;
  - encryption mechanism;
  - initialization of the data structure;
  - data loading;
  - phase switching.
- All authentication protocols (PACE-GM/IM) and secure messaging type (DES-128,AES128/192/256);
- The integrity token of a public key;
- All supported digital signature algorithm;
- Authentication of the TOE using asymmetric cryptography;
- All PIN management operations available after delivery point (spanning the three types of PIN : PIN<sub>Auth</sub>, PIN<sub>Sig</sub> (called also RAD) & PUK):
  - PIN initialization;
  - Upgrade of PIN attributes;
  - PIN change, unlocking, (re-)initialization;
  - Certificate management.
- PACE authentication;
- Extended Access Control Version 1 as defined in [TR-03110-1] and [TR-03110-3]. It consists of two parts: Chip Authentication Protocol Version 1 and Terminal Authentication Protocol Version 1;
- Signature key import;
- Signature key generation;
- Signature key public key export;
- Digital authentication feature including :
  - the corresponding key management operation (generation, import);

The TOE may be used for various use cases requiring qualified signature:

- Digital signature application;
- Electronic health card;
- Electronic services cards etc.

Depending on the use case and or the ability of the underlying Java Card open platform, the TOE may be used

- in contact mode (T=0 and/or T=1 protocol);
- in contactless protocol (T=CL);

### **3.4.1 Keys and PINs**

The TOE handles as well cryptographic data objects, such as keys (for digital signature, authentication, and encryption key decipherment) and PINs.

The TOE enables to create, update and use PINs as detailed in [AGD\_OPE].

For keys, the TOE enables to create, import, generate and erase keys as detailed in [AGD\_OPE].

### **3.4.2 Access Control Management**

The TOE ensures access control on any operations acting on any objects it handles (files, keys or PINs).

Each EF is configured at creation with access conditions protecting read and write access, while the ADF may be configured at creation with access conditions protecting their selection. Keys used for digital authentication, digital signature creation, encryption key decipherment and PINs require specific conditions before they can be used, updated or managed.

Prior to granting access to a given operation, the TOE checks the requested access rights are fulfilled. The access conditions can only be fulfilled upon successful authentication of an entity (see below).

### **3.4.3 Authentication of entities**

The TOE allows authenticating several types of entities in order to grant them some access rights:

- **Authentication of a natural person.** It relies on a successful verification of a PIN code presented to the TOE by the natural person. (only available in phase 7)
- **Authentication of a remote server.** It relies on a mutual authentication - based on PKI - generating a trusted channel ensuring authenticity, integrity and confidentiality of the messages, used to securely communicate. (only available in phase 7)
- **Authentication of personalization agent** (only in phase 6);

These authentication mechanisms allows fulfilling the access control mechanisms described above.

### **3.4.4 Digital Authentication**

The TOE supports digital authentication based on RSA and elliptic curves cryptography (ECC). Digital authentication is the process by which (1) the holder of TOE authenticates itself to the TOE using a PIN, releasing access right to an authentication key stored in the TOE, (2) subsequently the authentication key is used by the TOE to authenticate itself on behalf of the TOE holder. Digital authentication is useful so that the TOE holder can authenticate himself on line, without compromising any sensitive assets (PINs or authentication key).

### **3.4.5 Electronic Services**

The TOE supports as well several electronic services:

- **Digital signature:** this feature enables the signatory to electronically signs documents. The signature may be either advanced or qualified (compliant with [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6] ).
- **Encryption key decipherment:** this feature enables the document holder to store secret data on an electronic vault. The key needed to decipher the key encrypting these data is securely stored in the TOE. The document holder's computer sends the encrypted encryption key to the TOE to get the plain encryption key.

### **3.4.6 Trusted Channel function**

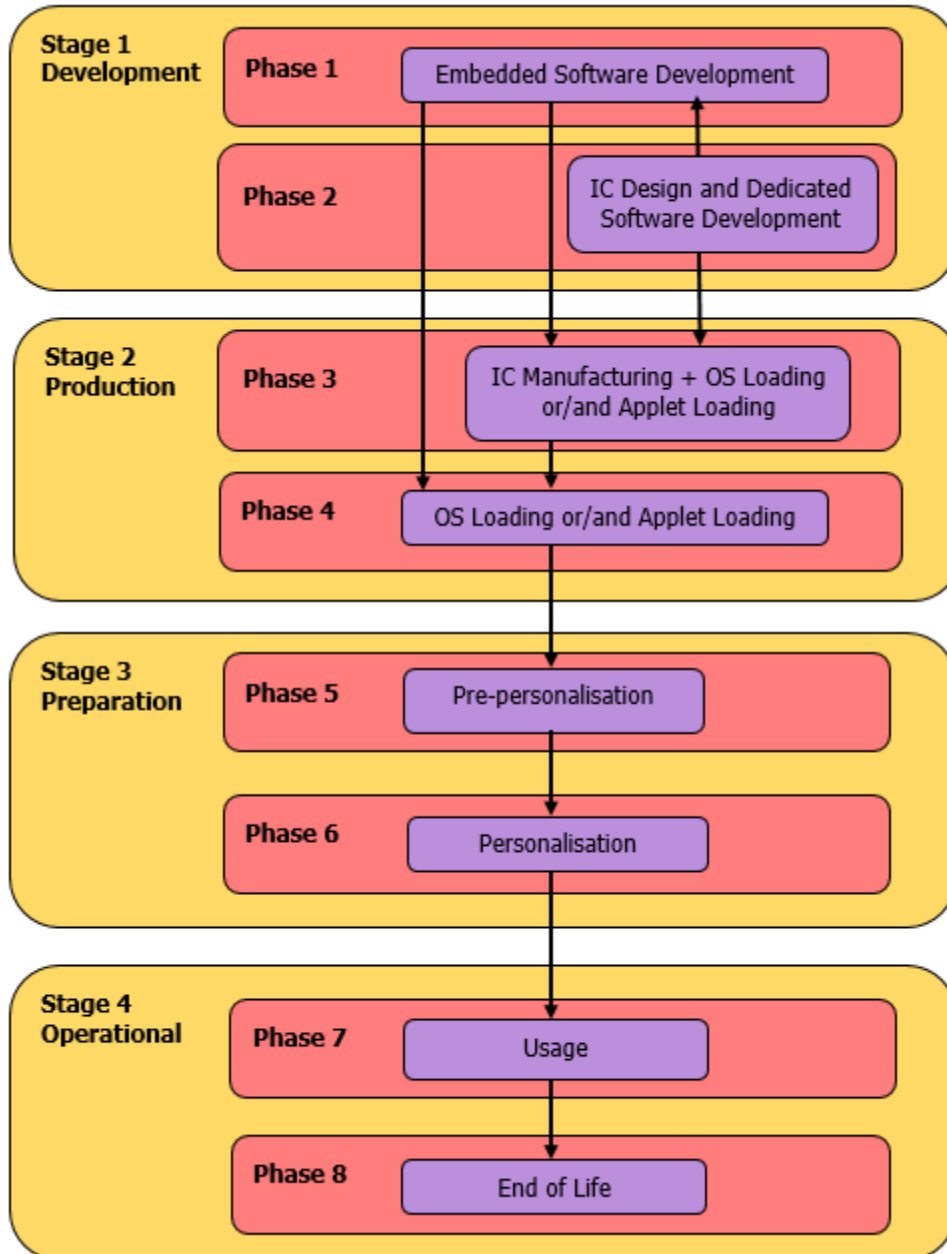
This feature realizes a secure communication channel to verify authenticity and integrity as well as securing confidentiality of user data between the TOE and other devices connected.

### **3.4.7 Secure execution**

The TOE ensures a secure execution of its services. First, the TOE ensures its execution is protected against physical manipulation or attempt to tamper with. Secondly, should the execution of the TOE be tampered with in any manner, the TOE ensures it remains in a safe state protecting its assets and the TSFs, so that no vulnerabilities can be exploited by an attacker.

## 4 Life Cycle

The TOE life cycle in the following figure distinguishes stages for development, production, preparation and operational use in accordance with the standard smart card life cycle [PP\_IC].



**Figure 2 Life cycle Overview**

## 4.1 Development Environment

In this environment, the following two phases take place:

- Phase 1: IC Embedded Software Development (Java Card Open Platform components and CombICAO Applet v3)
- Phase 2: IC Development

The IC Embedded Software Developer is in charge of the specification, development and validation of the software (Java Card Open Platform and CombICAO Applet v3).

The IC Developer designs the IC, develops the IC dedicated software and provides information, software or tools to the IC embedded software developer.

Roles, actors, sites and coverage for this environment of the product life-cycle are listed in the table below:

Role	Actor	Site	Covered by
CombICAO Applet v3 Developer	IDEMIA	MANILA, JAKARTA, COURBEVOIE and PESSAC R&D sites	ALC
Embedded Software Developer (Java Card Open Platform)	IDEMIA	Platform Developer Refer to [ST_PTF]	ALC
Redaction and Review of Documents	IDEMIA	NOIDA, COURBEVOIE and PESSAC R&D sites	ALC
IC Developer	INFINEON	IC Manufacturer Refer to [ST_PTF]	ALC

**Table 2 : Development R&D Sites**

## 4.2 Production Environment

In this environment, the following two phases take place:

- Phase 3: IC Manufacturing
- Phase 4: ID-One Cosmo X Platform loading and CombICAO Applet v3 loading

The CombICAO Applet v3 run time code is integrated in the FLASH memory of the chip.

Depending on the intention, the following different loading options are supported. Details on delivery methods for each option are provided in the **[AGD\_PRE]**.

IDEMIA CC Audited Production Sites are listed below:

IDEMIA CC Audited Production Sites/Plants	Country
Haarlem	Netherlands
Noida	India
Ostrava	Czech Republic
Shenzhen	China
Vitré	France

**Table 3 : Audited Production Sites**

**(Option 1) Image Loading audited IC Manufacturer site**

FLASH image containing both the "ID-One Cosmo X" Java Card Platform OS along with the CombICAO Applet v3 is securely delivered directly from the software developer (IDEMIA R&D Audited Site) to the **IC Manufacturer** (Infineon CC Audited Site) to be loaded into FLASH memory. The FLASH image is always encrypted.

**TOE Delivery point (i.e. point in time where the TOE starts to exist):**

- The TOE delivery point occurs in Phase 4, as soon as the loading of the image with ID-One Cosmo X Platform + CombICAO Applet v3 by the IC Manufacturer has been completed.

Package	Actor for FLASH image loading	Site For FLASH image loading	Covered by CC
FLASH image containing ID-One Cosmo X Platform + CombICAO Applet v3	IC Manufacturer	IC Manufacturer CC Audited Production Plants specified in [ST_PTF]	ALC

**Table 4 Option 1: Both Platform and Applet packages are loaded at IC Manufacturer Site**

**(Option 2) Image loading at IDEMIA and External sites**

FLASH image containing both ID-One Cosmo X Platform along with CombICAO Applet v3 is securely delivered directly from the software developer (IDEMIA R&D Audited Site) for loading to **CC Audited IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited IDEMIA Sites** or **External Sites**.

**TOE Delivery point:**

- If loading of ID-One Cosmo X Platform + CombICAO Applet v3 is performed in Audited IDEMIA Production Sites, then TOE delivery is considered at the end of Phase 4.



- If loading of ID-One Cosmo X Platform + CombICAO Applet v3 is performed in Non-Audited IDEMIA Production Sites or External Sites, then TOE delivery is considered after Phase 4.

Package	Actor for FLASH image loading	Site for FLASH image loading	Covered by CC
FLASH image containing the ID-One Cosmo X Platform + CombICAO Applet v3	IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited IDEMIA Sites or External Sites	AGD

**Table 5 Option 2: Both Platform and Applet packages are loaded at CC Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites**

**(Option 3) Platform loaded by IC Manufacturer, Applet loaded by IDEMIA or 3<sup>rd</sup> party**

Only the ID-One Cosmo X Platform is delivered to the IC Manufacturer (Infineon Audited Sites) to be loaded.

With the ID-One Cosmo X Platform already loaded (i.e. present) on the chip, the following options (**3a or 3b (i) or 3b (ii) or 3c**) can be chosen for loading the CombICAO Applet v3.

**(Option 3a) Applet loading using GP CLFDB mechanism.**

The CombICAO Applet v3 along with the TOE’s guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited IDEMIA Sites or External Sites**.

Loading of the CombICAO Applet v3 on top of the already present ID-One Cosmo X Platform GP Java Card OS in any of these sites is accomplished by using a GP CLFDB decryption Key.

**TOE Delivery points:**

- If loading of the CombICAO Applet v3 on top of already loaded ID-One Cosmo X Platform (as described below) is done in a CC Audited IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.
- If loading of the CombICAO Applet v3 on top of already loaded ID-One Cosmo X Platform (as described below) is done in Non-Audited IDEMIA Production Sites or External Sites then, TOE delivery is considered after phase 4.

Package	Actor	Site	Covered by
Image containing only ID-One Cosmo X Platform	IC Manufacturer	IC Manufacturer Production Plants Refer to [PTF-CERT]	ALC
CombICAO Applet v3 loaded through GP mechanism using CLFDB Key	IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited IDEMIA Sites or External Sites	AGD

**Table 6 Option 3(a): Platform package is loaded at IC Manufacturer Site and Applet package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites through GP Mechanism**





### **(Option 3b) Applet loading using the IDEMIA Resident Application**

- (i) CombICAO Applet v3 along with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited IDEMIA Sites** or **External Sites**.

CombICAO Applet v3 package is securely loaded via LSK on top of the present ID-One Cosmo X Platform Java Card OS in any of these sites. This loading is accomplished by using the IDEMIA "Resident Application" of the ID-One Cosmo X Platform.

- (ii) The DUMP package (including CombICAO Applet v3) with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited IDEMIA Sites** or **External Sites**.

Loading of DUMP PACKAGES in any of these sites is done through Resident Application using DSK secret production key on top of the platform already loaded by IC Manufacturer (Infineon).

#### **TOE Delivery points:**

- If loading of Applet package /DUMP Package on top of already loaded ID-One Cosmo X Platform (as described below) is done in Audited IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.
- If loading of Applet package /DUMP Package on top of already loaded ID-One Cosmo X Platform (as described below) is done in Non-Audited IDEMIA Production Sites or External Sites then, TOE delivery after Phase 4.

Package	Actor	Site	Covered by
Image containing only ID-One Cosmo X Platform	IC Manufacturer	IC Manufacturer Production Plants Refer to [PTF-CERT]	ALC
<b>3b (i)</b> CombICAO Applet v3 loaded through Resident Application using LSK format	IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited IDEMIA Sites or External Sites	AGD
<b>3b (ii)</b> DUMP PACKAGE Ciphred format [DSK Secret Live Key]	IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited IDEMIA Sites or External Sites	AGD

**Table 7 Platform package is loaded at IC Manufacturer Site and Applet package is loaded through resident application using LSK format or DUMP Package in Ciphred format is loaded**



**(Option 3c) Applet loading in plain (unprotected) format using GP**

CombICAO Applet v3 along with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **CC Audited IDEMIA Production Sites** (Refer Audited Production Sites Table).

Here, there is a provision for loading the applet in plain format in **Common Criteria Audited IDEMIA Sites only**, on top of the platform already loaded by IC Manufacturer (Infineon). This applet loading in plain format is not allowed in Non-Audited IDEMIA Sites or External Sites.

**TOE Delivery points:**

- The loading of CombICAO Applet v3 on top of already loaded ID-One Cosmo X Platform is done in plain (unprotected) format in Common Criteria Audited IDEMIA Production Sites. The TOE delivery is considered at the end of Phase 4.

Package	Actor	Site	Covered by
Image containing only ID-One Cosmo X Platform	IC Manufacturer	IC Manufacturer Production Plants Refer to [PTF-CERT]	ALC
CombICAO Applet v3 in Plain Format	IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC

**Table 8 Option 3(c): Platform package is loaded at IC Manufacturer Site and Applet package in plain format is loaded at Audited IDEMIA Sites only**



**(Option 4) Platform and Applet loaded by IDEMIA or 3<sup>rd</sup> party**

Only ID-One Cosmo X Platform is securely delivered directly from the software developer (IDEMIA R&D Audited Site) for loading to **CC Audited IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited IDEMIA Sites** or **External Sites**.

*Note: Here, when the ID-One Cosmo X Platform package is loaded in Non-Audited IDEMIA Sites or External Sites, then the Platform is in self-protected mode by its secure functions*

The following options (**4a or 4b (i) or 4b (ii) or 4c**) can be chosen for loading applets on top of the already loaded platform.

**(Option 4a) Applet loading using GP CLFDB mechanism**

CombICAO Applet v3 along with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited IDEMIA Sites** or **External Sites**.

Loading of Applet in any of these sites is done through GP mechanism using CLFDB Key on top of the platform already loaded by **CC Audited IDEMIA Production Sites** or **Non-Audited IDEMIA Sites** or **External Sites**.

**TOE Delivery points:**

- If loading of the CombICAO Applet v3 on top of already loaded ID-One Cosmo X Platform (as described below) is done in CC Audited IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.
- If loading of the CombICAO Applet v3 onto the already loaded ID-One Cosmo X Platform (as described below) is done in Non-Audited IDEMIA Production Sites or External Sites then, TOE delivery is considered after Phase 4.



Package	Actor	Site	Covered by
Image containing only ID-One Cosmo X Platform	IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited IDEMIA Sites or External Sites	AGD
CombICAO Applet v3 loaded through GP mechanism using CLFDB Key	IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited IDEMIA Sites or External Sites	AGD

**Table 9 Option 4(a): Platform package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites and Applet package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites through GP Mechanism**



#### **(Option 4b) Applet loading using the IDEMIA Resident Application**

- (i) CombICAO Applet v3 along with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited IDEMIA Sites** or **External Sites**.

Secure loading of CombICAO Applet v3 is done via LSK on top of the present Cosmo X Java Card OS (already loaded by **Audited IDEMIA Production Sites** or **Non-Audited IDEMIA Sites** or **External Sites**) in any of these sites. This loading is accomplished by using the IDEMIA "Resident Application" of the ID-One Cosmo X Platform OS

- (ii) DUMP package (including the CombICAO Applet v3) with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited IDEMIA Sites** or **External Sites**.

Loading of DUMP PACKAGES in any of these sites is done through Resident Application using DSK secret production key on top of the platform already loaded by **Audited IDEMIA Production Sites** or **Non-Audited IDEMIA Sites** or **External Sites**.

#### **TOE Delivery points:**

- If loading of Applet package /DUMP Package on top of already loaded ID-One Cosmo X Platform (as described below) is done in Audited IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.
- If loading of Applet package /DUMP Package on top of already loaded ID-One Cosmo X Platform (as described below) is done in Non-Audited IDEMIA Production Sites or External Sites then, TOE delivery is considered after Phase 4.

Package	Actor	Site	Covered by
Image containing only ID-One Cosmo X Platform	IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited IDEMIA Sites or External Sites	AGD
<b>4b (i)</b> CombICAO Applet v3 package loaded through Resident Application using LSK format	IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited IDEMIA Sites or External Sites	AGD
<b>4b (ii)</b> DUMP PACKAGE Ciphred format [DSK Secret Live Key]	IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited IDEMIA Sites or External Sites	AGD

**Table 10 Platform package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites and Options and Applet package is loaded through Resident application using LSK format or DUMP Package in Ciphred format is loaded**

**(Option 4c) Applet loading in plain (unprotected) format using GP**

CombICAO Applet v3 along with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Refer Audited Production Sites Table).

Here, there is a provision of loading the applet in plain format in Audited IDEMIA Sites **only**, on top of the platform already loaded by Audited IDEMIA Production Sites or Non-Audited IDEMIA Sites or External Sites. This applet loading in plain format is not allowed in Non-Audited IDEMIA Sites or External Sites.

**TOE Delivery points:**



- Here, since the loading of Applet package on top of already loaded ID-One Cosmo X Platform (as described below) is done in Plain format in CC Audited IDEMIA Production Sites, so TOE delivery is considered at the end of Phase 4.

Package	Actor	Site	Covered by
Image containing only ID-One Cosmo X Platform	IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC
	External Authorized Agent	Non-Audited IDEMIA Sites or External Sites	AGD
CombICAO Applet v3 in Plain Format	IDEMIA Authorized Entity	Refer Audited Production Sites Table	ALC

**Table 11 Option 4(c): Platform package is loaded at IC Manufacturer Site and Applet package in plain format is loaded at CC Audited IDEMIA Sites only**



### 4.3 Preparation Environment

In this environment, the following two phases take place:

- Phase 5: Pre-personalisation of the applet
- Phase 6: Personalisation

The preparation environment may not necessarily take place in a manufacturing site, but may be performed anywhere. All along these two phases, the TOE is self-protected as it requires the authentication of the pre-personalisation agent or personalisation agent prior to any operation.

The CombICAO Applet v3 is pre-personalised and personalised according to [AGD\_PRE].

These two phases are covered by [AGD\_PRE] tasks of the TOE and Guidance tasks of [ST\_PTF].

### 4.4 Operational Environment

Phase 7: Use Phase

The TOE is used as a travel document's chip by the traveller and the inspection systems in the "Operational Use" phase. The user data can be read according to the security policy of the issuing State or Organisation and can be used according to the security policy of the issuing State but they can never be modified for eMRTD application.

Note that applications can be loaded onto the ID-One Cosmo X platform during this phase.

During this phase, the TOE may be used as described in [AGD\_OPE] of the TOE.

This phase is covered by [AGD\_OPE] tasks of the TOE and Guidance tasks of [ST\_PTF].

## 5 Conformance claims

---

### 5.1 Common Criteria Conformance Claim

This security target claims conformance to the Common Criteria version 3.1, revision 5 [CC2] and [CC3].

The conformance to the CC is claimed as follows:

CC	Conformance rationale
Part 2	Conformance with the extended <sup>3</sup> part: <ul style="list-style-type: none"> <li>▪ FCS_RND.1 "Quality metric for random numbers"</li> <li>▪ FMT_LIM.1 "Limited capabilities"</li> <li>▪ FMT_LIM.2 "Limited availability"</li> <li>▪ FPT_EMS.1 "TOE Emanation"</li> <li>▪ FIA_API.1<sup>2</sup> "Authentication Proof of Identity"</li> </ul>
Part 3	Conformance to assurance package EAL 5, augmented with: <ul style="list-style-type: none"> <li>▪ AVA_VAN.5: "Advanced methodical vulnerability analysis"</li> <li>▪ ALC_DVS.2: "Sufficiency of security measures"</li> <li>▪ ALC_FLR.1: "Basic flaw remediation"</li> </ul>

**Table 12 Common Criteria conformance claim**

*Application Note:*

The component ALC\_FLR.3 is added in the evaluation. But as the platform is only FLR.1, the product can claim only ALC\_FLR.1

**Remark:**

The Common Methodology for Information Technology Security Evaluation [CEM] has been taken into account.

### 5.2 Protection Profile Conformance Claim

This security target is strict compliant with the following PPs:

- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 2: Device with key generation" [PP-SSCD2].
- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 3: Device with key import" [PP-SSCD3].

---

<sup>2</sup> FIA\_API.1 has been added to this security target for the needs of the Chip Authentication Protocol.

- “Common Criteria Protection Profile for Secure Signature Creation Device – Part 4: Extension for device with key generation and trusted communication with certificate generation application” [PP-SSCD4].
- “Common Criteria Protection Profile for Secure Signature Creation Device – Part 5: Extension for device with key generation and trusted communication with signature creation application” [PP-SSCD5].
- “Common Criteria Protection Profile for Secure Signature Creation Device – Part 6: Extension for device with key import and trusted communication with signature creation application” [PP-SSCD6].

### 5.3 Package Claim

The protection profiles require an assurance level of level EAL4 augmented with AVA\_VAN.5. This security target considers an assurance level EAL5 augmented with AVA\_VAN.5, ALC\_FLR.1 and ALC\_DVS.2, which still complies with the requirements of the protection profiles.

### 5.4 Conformance Rationale

[PP-SSCD4] and [PP-SSCD5] are strictly conforming to the core PP-SSCD2 [PP-SSCD2]. [PP-SSCD6] is strictly conforming to the core PP-SSCD3 [PP-SSCD3]. This ST is claimed to be conformant to the above mentioned PPs [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6]. A detailed justification is given in the following:

- 1) The SPD of this ST contains the security problem definition [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6]. The SPD for this ST is described by the same threats, organisational security policies and assumptions as for the TOE in the PPs.
- 2) The security objectives for the TOE in this ST include all the security objectives for the TOE of the core PPs [PP-SSCD2] and [PP-SSCD3] and add
  - a. the security objectives OT.TOE\_TC\_VAD\_Imp and OT.TOE\_TC\_DTBS\_Imp from [PP-SSCD5] and [PP-SSCD6],
  - b. the security objectives OT.TOE\_SSCD\_Auth and OT.TOE\_TC\_SVD\_Exp from [PP-SSCD4],
- 3) The assumptions in this ST include A.CSP from [PP-SSCD3] and [PP-SSCD6]. This assumption doesn't mitigate any threat and doesn't fulfil any OSP meant to be addressed by security objectives for the TOE in the other PPs.
- 4) The security objectives for the operational environment in this ST include all security objectives for the operational environment of the core PPs [PP-SSCD2] and [PP-SSCD3] except OE.HI\_VAD, OE.DTBS\_Protect and OE.SSCD\_Prov\_Service.
  - This ST adapts OE.HI\_VAD and OE.DTBS\_Protect to the support provided by the TOE by new security functionality (cf. OT.TOE\_TC\_VAD\_Imp, OT.TOE\_TC\_DTBS\_Imp) provided by the TOE and changes them into OE.HID\_TC\_VAD\_Exp and OE.SCA\_TC\_DTBS\_Exp ([PP-SSCD5] and [PP-SSCD6] for details).
  - OE.SSCD\_Prov\_Service is replaced by OE.Dev\_Prov\_Service from [PP-SSCD4].

This ST also includes security objectives for the operational environment OE.CGA\_SSCD\_Auth and OE.CGA\_TC\_SVD\_Imp from [PP-SSCD4]

- 5) The SFRs specified in this ST includes all security functional requirements (SFRs) specified in the core PPs [PP-SSCD2] and [PP-SSCD3]. Additional SFRs address :
  - a. trusted channel between the TOE and the SCA from [PP-SSCD5] and [PP-SSCD6]: FDP\_UIT.1/DTBS, FTP\_ITC.1/VAD and FTP\_ITC.1/DTBS.
  - b. Trusted communication with CGA from [PP-SSCD4] : FIA\_API.1 and FDP\_DAU.2/SVD, FTP\_ITC.1/SVD
- 6) This ST provides refinements for the SFR FIA\_UAU.1 according to [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6].
- 7) The security assurance requirements (SARs) are originally taken from SARs of part 3 [CC3] according to the package conformance EAL 5 augmented with ALC\_DVS.2, ALC\_FLR.1 and AVA\_VAN.5 (the Evaluation Assurance Level EAL5+ of the current ST exceeds the EAL4+ defined by [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6]).

This security target is compliant with the SPD of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6] as shown in the following table:

TOE SPDs	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
<b>Assumptions</b>						
A.CGA	x		x	x		x
A.SCA	x		x	x		x
A.CSP		x			x	x
<b>Threats</b>						

<b>TOE SPDs</b>	<b>PP SSCD2</b>	<b>PP SSCD3</b>	<b>PP SSCD4</b>	<b>PP SSCD5</b>	<b>PP SSCD6</b>	<b>Included</b>
T.SCD_Divulg	x	x	x	x	x	x
T.SCD_Derive	x	x	x	x	x	x
T.Hack_Phys	x	x	x	x	x	x
T.SVD_Forgery	x	x	x	x	x	x
T.SigF_Misuse	x	x	x	x	x	x
T.DTBS_Forgery	x	x	x	x	x	x
T.Sig_Forgery	x	x	x	x	x	x
<b>Organisational Security Policies</b>						
P.CSP_QCert	x	x	x	x	x	x
P.QSign	x	x	x	x	x	x
P.Sigy_SSCD	x	x	x	x	x	x
P.Sig_Non-Repud	x	x	x	x	x	x

**Table 13 PP SPDs vs. ST**

This security target is compliant with the security objectives of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6] as shown in the following table:

TOE Objectives	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
<b>Objectives for the TOE</b>						
OT.Lifecycle_Security	x	x	x	x	x	x
OT.SCD/SVD_Auth_Gen	x		x	x		x
OT.SCD_Unique	x		x	x		x
OT.SCD_SVD_Corresp	x		x	x		x
OT.SCD_Secrecy	x	x	x	x	x	x
OT.Sig_Secure	x	x	x	x	x	x
OT.Sigy_SigF	x	x	x	x	x	x
OT.DTBS_Integrity_TOE	x	x	x	x	x	x
OT.EMSEC_Design	x	x	x	x	x	x
OT.Tamper_ID	x	x	x	x	x	x
OT.Tamper_Resistance	x	x	x	x	x	x
OT.TOE_TC_VAD_Imp				x	x	x
OT.TOE_TC_DTBS_Imp				x	x	x
OT.TOE_SSCD_Auth			x			x
OT.TOE_TC_SVD_Exp			x			x
OT.SCD_Auth_Imp		x			x	x

Objectives for the Operational Environment						
OE.SVD_Auth	x	x	x	x	x	x
OE.CGA_QCert	x	x	x	x	x	x
OE.SSCD_Prov_Service	x	x		x	x	
OE.SCD/SVD_Auth_Gen		x			x	x
OE.SCD_Unique		x			x	x
OE.SCD_SVD_Corresp		x			x	x
OE.SCD_Secrecy		x			x	x
OE.HID_VAD	x	x	x			
OE.DTBS_Intend	x	x	x	x	x	x
OE.DTBS_Protect	x	x	x			
OE.Signatory	x	x	x	x	x	x
OE.HID_TC_VAD_Exp				x	x	x
OE.SCA_TC_DTBS_Exp				x	x	x
OE.Dev_Prov_Service			x			x
OE.CGA_SSCD_Auth			x			x
OE.CGA_TC_SVD_Imp			x			x

**Table 14 PP Security Objectives vs. ST**

This security target is compliant with the security functional requirements of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6] as shown in the following table:

TOE SFRs	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
FCS_CKM.1	x		x	x		x
FCS_CKM.4	x	x	x	x	x	x
FCS_COP.1	x	x	x	x	x	x
FDP_ACC.1/SCD/SVD_Generation	x		x	x		x
FDP_ACF.1/SCD/SVD_Generation	x		x	x		x
FDP_ACC.1/SVD_Transfer	x		x	x		x
FDP_ACF.1/SVD_Transfer	x		x	x		x
FDP_ACC.1/Signature_Creation	x	x	x	x	x	x
FDP_ACF.1/Signature_Creation	x	x	x	x	x	x
FDP_ACC.1/SCD_Import		x			x	x
FDP_ACF.1/SCD_Import		x			x	x
FDP_RIP.1	x	x	x	x	x	x
FDP_SDI.2/Persistent	x	x	x	x	x	x
FDP_SDI.2/DTBS	x	x	x	x	x	x



FIA_UID.1	x	x	x	x	x	x
FIA_UAU.1	x	x	x	x	x	x
FIA_AFL.1	x	x	x	x	x	x
FMT_SMR.1	x	x	x	x	x	x
FMT_SMF.1	x	x	x	x	x	x
FMT_MOF.1	x	x	x	x	x	x
FMT_MSA.1/Admin	x	x	x	x	x	x
FMT_MSA.1/Signat ory	x	x	x	x	x	x
FMT_MSA.2	x	x	x	x	x	x
FMT_MSA.3	x	x	x	x	x	x
FMT_MSA.4	x	x	x	x	x	x
FMT_MTD.1/Admi n	x	x	x	x	x	x
FMT_MTD.1/Signat ory	x	x	x	x	x	x
FPT_EMS.1	x	x	x	x	x	x
FPT_FLS.1	x	x	x	x	x	x
FPT_PHP.1	x	x	x	x	x	x
FPT_PHP.3	x	x	x	x	x	x

FPT_TST.1	x	x	x	x	x	x
FIA_API.1			x			x
FTP_ITC.1/SVD			x			x
FDP_DAU.2/SVD			x			x
FDP_UIT.1/DTBS				x	x	x
FTP_ITC.1/VAD				x	x	x
FTP_ITC.1/DTBS				x	x	x
FDP_ITC.1/SCD		x				x
FDP_UCT.1/SCD		x				x
FTP_ITC.1/SCD		x				x
FCS_RNG.1						x

**Table 15 PP SFRs vs. ST**

- 8) The additional functionalities (PACE authentication, Chip Authentication Protocol Version 1 and Terminal Authentication Protocol Version 1) have been added to the TOE with: (i) additional security problem definition; (ii) additional security objectives; (iii) additional SFRs. All these additions are based on the [PP\_EACwPACE].

Notice that the added security objectives for the operational environment don't mitigate any threats of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6] and don't fulfil any OSPs meant to be addressed by security objectives for the TOE in PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6]. The objectives and SFRs related to the functionality are only valid in case the additional functionalities are configured for the TOE.

The additions are mentioned in the below sections:

#### **5.4.1 Additional Assets**

The following additional Assets are identified:

- **Keys**
- **PIN/PUK**
- **VAD**
- **Session Keys**
- **Authenticity of the Electronic Documents Chip**
- **Tracing Data**

- **Sensitive User Data**
- **User Data stored on the TOE**
- **User Data transferred between the TOE and the Terminal**
- **Accessibility of TOE Functions and Data only for Authorized Subjects**
- **Genuineness of the TOE**
- **Electronic Document Communication Establishment Authorization Data**
- **Secret Document Holder Authentication Data**
- **TOE internal Non-Secret Cryptographic Material**

#### **5.4.2 Additional Subjects**

The following additional Subjects are identified:

- **Issuer Certification Authority (Issuer CA)**
- **Country Verifying Certification Authority (CVCA)**
- **eService Certification Authority**
- **Document Holder**
- **Electronic Document Presenter**
- **Basic Authentication Terminal (BAT)**
- **Authentication Terminal**
- **Administration Terminal**
- **Terminal**

#### **5.4.3 Additional Threats**

The following additional Threats are identified:

- **T.Key\_Divulg**
- **T.Key\_Derive**
- **T.TOE\_PublicAuthKey\_Forgery**
- **T.Authentication\_Replay**
- **T.Counterfeit**
- **T.Sensitive\_Data**
- **T.Abuse-Func**
- **T.Eavesdropping**
- **T.Forgery**
- **T.Information\_Leakage**
- **T.Malfunction**
- **T.Phys-Tamper**
- **T.Skimming**
- **T.Tracing**
- **T.ADMIN\_Configuration**
- **T.Key\_Access**

#### **5.4.4 Additional Organisational Security Policies**

The following additional Organisational Security Policy is identified:

- **P.LinkSCD\_QualifiedCertificate**
- **P.TOE\_PublicAuthKey\_Cert**
- **P.eServices**
- **P.EAC\_Terminal**

- **P.Terminal\_PKI**
- **P.Card\_PKI**
- **P.Pre-Operational**
- **P.Terminal**
- **P.Trustworthy\_PKI**
- **P.Manufact**

#### **5.4.5 Additional Security Objectives**

The following additional Security Objectives of the TOE are identified:

- **OT.Identification**
- **OT.Authentication\_Secure**
- **OT.Key\_Lifecycle\_Security**
- **OT.Keys\_Secrecy**
- **OT.TOE\_AuthKey\_Unique**
- **OT.Lifecycle\_Management**
- **OT.eServices**
- **OT.AC\_Pers\_EAC**
- **OT.Tracing**
- **OT.ADMIN\_Configuration**
- **OT.Key\_Usage\_Counter**

#### **5.4.6 Additional Security Objectives for the Operational Environment**

The following additional Security Objectives of the Operational Environment are identified:

- **OE.LinkSCD\_QualifiedCertificate**
- **OE.AuthKey\_Transfer**
- **OE.AuthKey\_Unique**
- **OE.TOE\_PublicKeyAuth\_Transfer**
- **OE.Terminal\_Authentication**
- **OE.Legislative\_Compliance**
- **OE.Passive\_Auth\_Sign**
- **OE.Personalization**
- **OE.Terminal**
- **OE.Electronic\_Document\_Holder**

#### **5.4.7 Additional Security Functional Requirements**

The following additional Security Functional Requirements are identified:

- **FCS\_RND.1**
- **FCS\_CKM.1/DH\_PACE**
- **FCS\_CKM.1/Session Keys**
- **FCS\_COP.1/GP Secret Data Protection**
- **FCS\_COP.1/SM in Confidentiality**
- **FCS\_COP.1/SM in Integrity**
- **FCS\_COP.1/Digital Auth**
- **FCS\_COP.1/Enc Key Decipherment**
- **FCS\_COP.1/SIG\_VER**
- **FDP\_ACC.1/TRM**
- **FDP\_ACF.1/TRM**

- FDP\_ACC.1/MNG\_File
- FDP\_ACF.1/MNG\_File
- FDP\_UCT.1/TRM
- FDP\_UIT.1/TRM
- FIA\_UID.1/PACE
- FIA\_UAU.1/PACE
- FIA\_UAU.4/PACE
- FIA\_UAU.5/PACE
- FIA\_UAU.6/PACE
- FIA\_UAU.6/EAC
- FIA\_AFL.1/AUTH
- FIA\_API.1/TOE Authentication
- FMT\_SMR.1/PACE
- FMT\_MTD.1/CVCA\_INI
- FMT\_MTD.1/CVCA\_UPD
- FMT\_MTD.1/DATE
- FMT\_MTD.1/CAPK
- FMT\_MTD.1/KEY\_READ
- FMT\_MTD.1/Key\_Usage\_Counter
- FMT\_MTD.1/Initialize\_PIN
- FMT\_MTD.1/Resume\_PIN
- FMT\_MTD.1/Change\_PIN
- FMT\_MTD.1/Unblock\_PIN
- FMT\_MTD.1/UnblockChange\_RAD
- FMT\_MTD.1/Erase\_PIN
- FMT\_MTD.1/Reinitialize\_PIN
- FMT\_MTD.1/UnblockChange\_PUK
- FMT\_MTD.1/TOE State
- FMT\_MTD.3
- FMT\_LIM.1
- FMT\_LIM.2
- FPT\_EMS.1/PIN-PUK-KEYS
- FTP\_ITC.1/PACE

## 6 Security Problem Definition

---

### 6.1 Assets

#### 6.1.1 Assets from Protection Profiles

##### SCD

###### Signature Creation Data

Private key used to perform an electronic signature operation. The confidentiality, integrity and signatory's sole control over the use of the SCD shall be maintained.

##### SVD

###### Signature Verification Data

Public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when it is exported shall be maintained.

##### DTBS/R

###### Data to be signed or its unique Representation

Set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the electronic signature shall be maintained.

#### 6.1.2 Additional Assets

##### Keys

- o Private or secret key(s) used to (1) authenticate an external user or entity, (2) perform authentication protocols, (3) perform digital authentication, (4) perform digital signature or (5) perform encryption key decipherment. Their integrity and confidentiality must be maintained.
- o Public key(s) used as trust anchor to verify a certificate chain used in terminal authentication. Their integrity must be maintained.

##### PIN/PUK

The applet manages two types of PINs (PINSig called also RAD and PINAuth) for user authentication and one PUK for management purpose. They are used to authenticate natural persons. The PINs and PUK must be created and initialized first before they can be used for authentication. Furthermore, PINAuth can only be a Code PIN.

##### VAD

PIN code entered by the end user to perform a signature operation (confidentiality and authenticity of the VAD as needed by the authentication method employed)

### **Session Keys**

Keys computed for secure messaging and used to ensure confidentiality, authenticity and integrity of data.

### **Authenticity of the Electronic Documents Chip**

The authenticity of the electronic document's chip, personalized by the issuing organization for the Document holder, is used by the electronic document presenter to prove his possession of a genuine electronic document.

### **Tracing Data**

Technical information about the current and previous locations of the electronic document gathered unnoticeable by the Document holder recognizing the TOE not knowing any PACE password. TOE tracing data can be provided / gathered.

### **Sensitive User Data**

User data, which have been classified as sensitive data by the electronic document issuer. Sensitive user data are a subset of all user data, and are protected by EAC.

### **User Data stored on the TOE**

All data, with the exception of authentication data, that are stored in the context of the application(s) on the electronic document. These data are allowed to be accessed either by a BAT, or, in the case of sensitive data, by an Authentication Terminal with appropriate authorization level.

### **User Data transferred between the TOE and the Terminal**

All data, with the exception of authentication data, that are transferred (both directions) during usage of the application(s) of the electronic document between the TOE and authenticated terminals.

### **Accessibility of TOE Functions and Data only for Authorized Subjects**

Property of the TOE to restrict access to TSF and TSF-Data stored in the TOE to authorized subjects only.

### **Genuineness of the TOE**

Property of the TOE to be authentic in order to provide claimed security functionality in a proper way.

### **Electronic Document Communication Establishment Authorization Data**

Restricted-revealable authorization information for a human user used for verification of the authorization attempts as an authorized user (PACE password). These data are stored in the TOE and not send to it. Restricted-revealable here refers to the fact that if necessary, the Document holder may reveal her verification values of CAN and MRZ to an authorized person, or to a device that acts according to respective regulations and is considered trustworthy.

### **Secret Document Holder Authentication Data**

Secret authentication information for the Document holder being used for verification of the authentication attempts as authorized Document holder (sent PACE passwords, e.g. PIN, PUK, MRZ or CAN).

### **TOE internal Non-Secret Cryptographic Material**

Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material used by the TOE in order to enforce its security functionality.

## **6.2 Users / Subjects**

### **6.2.1 Subjects from Protection Profiles**

#### **User**

End user of the TOE who can be identified as administrator or signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.

#### **Administrator**

User who is in charge to perform the TOE initialization, TOE (pre-)personalization or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator.

*Application Note:*

For all activities related to Personalization, the subject Administrator is also called Personalization Agent in the rest of the document.

For all activities related to Use Phase, the subject Administrator has following roles as defined below:

- o Manage symmetric authentication using Administration Agent keys,
- o Configure the size or value of the Chip Authentication key to be modified in USE phase,
- o Change the key parameters during the key generation process,
- o Read that Proof that a key has been on board generated,
- o Create or Delete Files in Use Phase,
- o Invalidate one of the Chip Authentication key in USE phase and to set the secondary key as being the primary key
- o Unblock and Change the PUK
- o Unblock and Change the PINSig
- o Generate keypair Chip Authentication Key
- o Generate keypair SCD/SVD



### **Signatory**

User who hold the TOE and use it on their own behalf or on behalf of the natural or legal person or entity they represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as signatory.

### **6.2.2 Threat agents**

#### **Attacker**

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

### **6.2.3 Additional Subjects**

#### **Issuer Certification Authority (Issuer CA)**

An organization enforcing the policy of the electronic document issuer, i. e. confirming correctness of user and TSF data that are stored within the electronic document. The Issuer CA represents both the (1) root and (2) intermediate sub-CAs of the public key infrastructure (PKI) used to issue the electronic document. The Issuer CA signs user and TSF data to create a digital seals that is stored in the electronic document to demonstrate their integrity and authenticity.

#### **Country Verifying Certification Authority (CVCA)**

The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing state or organization, i. e. enforcing protection of sensitive user data that are stored in the electronic document. The CVCA represents the country specific root of the PKI of Authentication Terminals and eServices certification authorities, and creates eServices certification authorities certificates within this PKI. Updates of the public key of the CVCA are distributed as CVCA Link-Certificates, see [TR-03110-3].

#### **eService Certification Authority**

An organization issuing terminal certificates. The eService certification authority is a certificate authority, authorized by the corresponding CVCA to issue certificates for Authentication Terminals.

#### **Document Holder**

A person who the electronic document issuer has personalized the electronic document for. Personalization here refers to associating a person uniquely with a specific electronic document. Note that an Document holder can also be an attacker. The document holder is equivalent to the signatory and can use and manage the PINSig (called also the RAD), the PINAuth and the PUK.

#### **Electronic Document Presenter**

A person presenting the electronic document to a terminal and claiming the identity of the Document holder. Note that an electronic document presenter can also be an attacker.

### **Basic Authentication Terminal (BAT)**

A BAT implements the terminal part of the PACE protocol and/or the VERIFY PIN command and authenticates itself to the electronic document using a shared password (CAN, MRZ, PIN, PUK). A BAT is not allowed to access sensitive user data.

### **Authentication Terminal**

A terminal that has successfully passed Terminal Authentication is an Authentication Terminal. It is authorized by the electronic document issuer through the eServices certification authorities of the receiving branch (by issuing terminal certificates) to access a subset or all of the data stored on the electronic document.

### **Administration Terminal**

A terminal that has successfully performed GP Authentication in phase 7 is an Administration Terminal. This terminal is linked to Administrator role in Use phase (phase 7).

### **Terminal**

A terminal is any technical system communicating with the TOE through the contactless or contact-based interface. The role terminal is the default role for any terminal being recognized by the TOE that is neither a BAT nor an Authentication Terminal nor an Administration Terminal.

## **6.3 Threats**

### **6.3.1 Threats drawn from the Protection Profiles**

#### **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.

#### **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.

#### **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.

#### **T.SVD\_Forgery**

##### ***Forgery of the signature verification data***

An attacker forges the SVD presented by the CSP to the CGA. This results in loss of SVD integrity in the certificate of the signatory.

#### **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.

#### **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 intended to sign.

#### **T.Sig\_Forgery**

##### ***Forgery of the electronic signature***

An attacker forges a signed data object, maybe using an electronic signature that has been created by the TOE, and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature created 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.

### **6.3.2 Additional Threats**

#### **T.Key\_Divulg**

##### ***Storing, copying, and releasing of a key stored in the TOE***

An attacker can store and copy a key (other than SCD) stored in the TOE outside the TOE. An attacker can release a key during generation, storage and use in the TOE.

#### **T.Key\_Derive**

##### ***Derive a key***

An attacker derives a key (other than SCD) from public known data, such as the corresponding public key or cryptogram created by means of the key or any other data communicated outside the TOE, which is a threat against the secrecy of the key.

#### **T.TOE\_PublicAuthKey\_Forgery**

##### ***Forgery of the public key of a TOE authentication key***

An attacker forges the public key of a TOE authentication key presented by the TOE. This results in loss of the public key integrity in the authentication certificate of the TOE.

#### **T.Authentication\_Replay**

##### ***Replay of an authentication of an external entity***

An attacker retrieves by observation authentication data used by a third party during an authentication sequence. The attacker tries to replay this authentication sequence to grant access to the TOE.

### **T.Counterfeit**

An attacker with high attack potential produces an unauthorized copy or reproduction of a chip of a genuine electronic document. This copy or reproduction can be used as a part of a counterfeit electronic document. This violates the authenticity of the electronic document's chip used for authentication of an electronic document presenter by possession of an electronic document. The attacker may generate a new data set or extract completely or partially the data from a genuine electronic document's chip and copy them to another appropriate chip to imitate the chip of the genuine electronic document.

Threat agent: having high attack potential, being in possession of one or more legitimate ID-Cards

### **T.Sensitive\_Data**

An attacker tries to gain access to sensitive user data through the communication interface (contact or contactless) of the electronic document's chip. The attack T.Sensitive\_Data is similar to the threat T.Skimming from [PACEPP] w.r.t. the attack path (communication interface) and the motivation (to get data stored on the electronic document's chip) but differs from those in the asset under the attack, the opportunity (i.e. knowing the PACE Password or the PIN) and therefore the possible attack methods.

Threat agent: having high attack potential, knowing the PACE Password or the PIN, being in possession of a legitimate electronic document

### **T.Abuse-Func**

An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE or (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE. This threat addresses the misuse of the functions for the initialization and Personalization in the operational phase after delivery to the holder.

### **T.Eavesdropping**

An attacker is listening to the contactless communication between the electronic document and the BAT in order to gain the user data transferred between the TOE and the terminal connected.

### **T.Forgery**

An attacker fraudulently alters the User Data or/and TSF-data stored on the electronic document or/and exchanged between the TOE and the terminal connected in order to outsmart the BAT by means of changed electronic document holder's related reference data. The attacker does it in such a way that the terminal connected perceives these modified data as authentic one.

### **T.Information\_Leakage**

An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the electronic document or/and exchanged between the TOE and the terminal connected. The information leakage may be inherent in the normal operation or caused by the attacker.

### **T.Malfunction**

An attacker may cause a malfunction the electronic document's hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE' hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the electronic document outside the normal operating conditions, exploiting errors in the electronic document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

### **T.Phys-Tamper**

An attacker may perform physical probing of the electronic document in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the electronic document in order to alter (i) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the travel document.

### **T.Skimming**

An attacker imitates a terminal in order to get access to the user data stored on or transferred between the TOE and the inspecting authority connected via the contactless interface of the TOE.

### **T.Tracing**

An attacker tries to gather TOE tracing data (i.e. to trace the movement of the electronic document) unambiguously identifying it remotely by establishing or listening to a communication via the contactless interface of the TOE.

### **T.ADMIN\_Configuration**

*Adverse action:* An attacker may access to the TOE at user phase (phase 7) to try to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the eDigitalIdentity document's embedded software or (iii) Create or Delete EF files without properly authenticating as Administrator.

*Threat agent:* having high attack potential, being in possession of one or more legitimate eDigitalIdentity document in Operational use phase.

*Asset:* authenticity of logical eDigitalIdentity document data and Accessibility of TOE Functions and Data only for Authorized Subjects

### **T.Key\_Access**

*Adverse action:* An attacker may access to the internal secret cryptographic keys of the TOE.

*Threat agent:* having high attack potential, knowing the key values, being in possession of a legitimate eDigitalIdentity document.

*Asset:* TOE internal secret cryptographic keys

## 6.4 Organizational Security Policies

### 6.4.1 Security Policies drawn from the Protection Profiles

#### P.CSP\_QCert

##### ***Qualified certificate***

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. previous [Directive], Article 2, clause 10 or new [eIDAS\_Regulation], Article 3, clause 15) 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.

#### P.QSign

##### ***Qualified electronic signatures***

The signatory uses a signature creation system to sign data with an advanced electronic signature (cf. the [Directive], Article 2, clause 2 or new [eIDAS\_Regulation], Article 3, clause 11), which is a qualified electronic signature if it is based on a valid qualified certificate (according to the [Directive], Article 2, clause 10 or new [eIDAS\_Regulation], Article 3, clause 15). The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature created with a SCD implemented in the SSCD that the signatory maintain under their sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable

#### P.Sigy\_SSCD

##### ***TOE as secure signature creation device***

The TOE meets the requirements for an SSCD laid down in (Article 2, clause 6 of the [Directive] or new [eIDAS\_Regulation], Article 3, clause 22/23). This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once.

#### P.Sig\_Non-Repud

##### ***Non-repudiation of signatures***

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

### 6.4.2 Additional Security Policies

#### P.LinkSCD\_QualifiedCertificate

##### ***Link between a SCD stored in the TOE and the relevant qualified certificate***

The Role in charge of creating and updating the SCD (Personalization Agent, R.Admin), or the trusted IT entity involved in the updating process (CSP) shall ensure an unambiguous link between the (qualified) certificate(s) and the corresponding SCD(s). This link might be figured out by a PKCS#15 structure, an XML structure, an identifier linking the file containing the (qualified) certificate or the URL hosting them to the SCD(s) stored in the TOE. In particular, it implies this link is updated, each time the SCD(s) is created, imported, erased or generated.

#### **P.TOE\_PublicAuthKey\_Cert**

##### ***Certificate for asymmetric TOE authentication keys***

The TOE contains certificate(s) issued by a known entity ensuring its public key corresponding to the authentication private key is genuine.

#### **P.eServices**

##### ***Provision of eServices***

The TOE provides the following mechanisms:

- o decrypt encryption decipherment keys using asymmetric mechanisms;
- o digital authentication: authentication of the TOE (on behalf of the TOE holder) using an asymmetric private key;

Moreover, the TOE ensures these keys remain genuine by enforcing an access control over the update of these keys, in order to ensure that only entitled entities can change them.

#### **P.EAC\_Terminal**

Terminals that intent to be Authentication Terminals must implement the respective terminal part of the protocols required to execute EAC protocol, and store (static keys) or generate (temporary keys and nonces) the corresponding credentials.

#### **P.Terminal\_PKI**

The electronic document issuer shall establish a public key infrastructure for the card verifiable certificates used for Terminal Authentication. For this aim, the electronic document issuer shall run a Country Verifying Certification Authority. The instances of the PKI shall fulfill the requirements and rules of the corresponding certificate policy. The electronic document issuer shall make the CVCA certificate available to the personalization agent or the manufacturer.

#### **P.Card\_PKI**

The description below states the responsibilities of involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.

- o The electronic document Issuer shall establish a public key infrastructure to ensure the integrity and authenticity of the content of the electronic document, through the generation of digital seals protecting the data it contains. For this aim, it runs an Issuer CA.

- o The Issuer CA shall securely generate, store and use the Issuer CA key pair. The Issuer CA shall keep the Issuer CA Private Key secret.

### **P.Pre-Operational**

- o The electronic document Issuer issues the electronic document and approves it using the terminals complying with all applicable laws and regulations.
- o The electronic I document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE.
- o The electronic document Issuer uses only such TOE's technical components (IC) which enable traceability of the electronic documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase,
- o If the electronic document Issuer authorizes a Personalization Agent to personalize the electronic document for electronic document holders, the electronic document Issuer has to ensure that the Personalization Agent acts in accordance with the electronic document Issuer's policy.

### **P.Terminal**

The BAT shall operate their terminals as follows:

- o The related terminals shall be used by terminal operators and by electronic document holders.
- o They shall implement the terminal parts of the PACE protocol and check the digital seal generated by the Issuer CA included in the electronic document and protecting its content. The BAT shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
- o They shall also securely store the Issuer CA certificate in order to be able to verify the digital seals generated by the Issuer CA and included in the electronic document to protect its content (integrity and authenticity of the data stored in the electronic document).
- o The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords or the PIN, integrity of PKI certificates, etc.).

### **P.Trustworthy\_PKI**

The Issuer CA shall ensure that it issues its certificates exclusively to the rightful organizations and that they create exclusively correct digital seals to be stored on the electronic document.

### **P.Manufact**

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The electronic document Manufacturer writes the Pre-personalisation Data which contains at least the Personalisation Agent Key.



## 6.5 Assumptions

### 6.5.1 All SSCD parts

#### A.CGA

##### ***Trustworthy certificate 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.

#### A.SCA

##### ***Trustworthy signature creation application***

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

### 6.5.2 Parts 3 and 6 only

#### A.CSP

##### ***Secure SCD/SVD management by CSP***

The CSP uses only a trustworthy SCD/SVD generation device and ensures that this device can be used by authorised user only. The CSP ensures that the SCD generated practically occurs only once, that generated SCD and SVD actually correspond to each other and that SCD cannot be derived from the SVD. The CSP ensures the confidentiality of the SCD during generation and export to the TOE, does not use the SCD for creation of any signature and irreversibly deletes the SCD in the operational environment after export to the TOE.

## 7 Security Objectives

---

### 7.1 Security Objectives for the TOE

#### 7.1.1 All SSCD parts

##### **OT.Lifecycle\_Security**

###### ***Lifecycle security***

The TOE shall detect flaws during the initialization, personalization and operational usage. The TOE shall securely destroy the SCD on demand of the signatory.

##### **OT.SCD\_Secrecy**

###### ***Secrecy of the signature creation data***

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

##### **OT.Sig\_Secure**

###### ***Cryptographic security of the electronic signature***

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

##### **OT.Sigy\_SigF**

###### ***Signature creation function for the legitimate signatory only***

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

##### **OT.DTBS\_Integrity\_TOE**

###### ***DTBS/R integrity inside the TOE***

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

##### **OT.EMSEC\_Design**

###### ***Provide physical emanations security***

The TOE shall be designed and built in such a way as to control the production of intelligible emanations within specified limits.

##### **OT.Tamper\_ID**

###### ***Tamper detection***

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

#### **OT.Tamper\_Resistance**

##### ***Tamper resistance***

The TOE shall prevent or resist physical tampering with specified system devices and components.

#### **7.1.2 SS CD parts 2, 4 and 5 only**

#### **OT.SCD/SVD\_Auth\_Gen**

##### ***Authorised SCD/SVD generation***

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

#### **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 shall practically occur only once and shall not be reconstructable from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible.

#### **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 an electronic signature creation with the SCD.

#### **7.1.3 SS CD parts 3 and 6 only**

#### **OT.SCD\_Auth\_Imp**

##### ***Authorised SCD import***

The TOE shall provide security features to ensure that authorised users only may invoke the import of the SCD.

#### **7.1.4 SS CD part 4 only**

#### **OT.TOE\_SSCD\_Auth**

##### ***Authentication proof as SS CD***

The TOE shall hold unique identity and authentication data as SS CD and provide security mechanisms to identify and to authenticate itself as SS CD.

## **OT.TOE\_TC\_SVD\_Exp**

### ***TOE trusted channel for SVD export***

The TOE shall provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA. The TOE shall enable the CGA to detect alteration of the SVD exported by the TOE.

## **7.1.5 SSCD parts 5 and 6 only**

## **OT.TOE\_TC\_VAD\_Imp**

### ***Trusted channel of TOE for VAD import***

The TOE shall provide a trusted channel for the protection of the confidentiality and integrity of the VAD received from the HID as needed by the authentication method employed.

#### ***Application Note:***

This security objective for the TOE is partly covering OE.HID\_VAD from the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI). While OE.HID\_VAD in the core PP requires only the operational environment to protect VAD, this ST requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID\_TC\_VAD\_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE\_TC\_VAD\_Imp. Therefore this ST re-assigns partly the VAD protection from the operational environment as described by OE.HID\_VAD to the TOE as described by OT.TOE\_TC\_VAD\_Imp and leaves only the necessary functionality by the HID.

## **OT.TOE\_TC\_DTBS\_Imp**

### ***Trusted channel of TOE for DTBS import***

The TOE shall provide a trusted channel to the SCA to detect alteration of the DTBS/R received from the SCA. The TOE shall not generate electronic signatures with the SCD for altered DTBS.

## **7.1.6 Additional Security Objectives for the TOE**

## **OT.Identification**

### ***Identification of the TOE***

The TOE must provide means to store Initialisation36 and Pre-Personalisation Data in its non volatile memory. The Initialisation Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the electronic document. The storage of the Pre-Personalisation data includes writing of the Personalisation Agent Key(s).

## **OT.Authentication\_Secure**

### ***Secure authentication mechanisms***

The TOE provides strong mechanism to authenticate external users/entity and mechanisms to establish a strong trusted channel with an external IT entity. The authentication protocols rely on cryptographic schemes that are based on either symmetric or asymmetric cryptography. The TOE uses freshly generated random number in the authentication

mechanism in order to avoid replay attacks. The authentication protocols ensure that the cryptogram cannot be forged without the knowledge of the authentication key, and that they cannot be reconstructed from the authentication cryptograms. The trusted channel ensures integrity, authenticity, and confidentiality of the data using strong encryption techniques. The trusted channel ensures protection against deletion, and modification of commands. Moreover, the TOE ensures the key its uses are genuine by enforcing an access control over the authentication keys update, in order to ensure that only entitled entities can change key values. These mechanisms provided by the electronic document's chip are protected against attacks with high attack potential.

Note: The natural person may authenticate itself to the TOE via the VERIFY PIN command.

#### **Protection against Abuse of Functionality:**

The TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE, (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

#### **Protection against Information Leakage:**

The TOE must provide protection against disclosure of confidential User Data or/and TSF-data stored and/or processed by the travel document

- o by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines,
- o by forcing a malfunction of the TOE and/or
- o by a physical manipulation of the TOE.

#### **Protection against Malfunctions:**

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation have not been proven or tested. This is to prevent functional errors in the TOE. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature. The following TOE security objectives address the aspects of identified threats to be countered involving TOE's environment.

#### **Protection against Physical Tampering:**

The TOE must provide protection of confidentiality and integrity of the User Data, the TSF-data and the electronic document's Embedded Software by means of

- o measuring through galvanic contacts representing a direct physical probing on the chip's surface except on pads being bonded (using standard tools for measuring voltage and current) or
- o measuring not using galvanic contacts, but other types of physical interaction between electrical charges (using tools used in solid-state physics research and IC failure analysis),
- o manipulation of the hardware and its security functionality, as well as
- o controlled manipulation of memory contents (User Data, TSF-data) with a prior
- o reverse-engineering to understand the design and its properties and functionality.

## **OT.Key\_Lifecycle\_Security**

### ***Life cycle security of the keys stored in the TOE***

The TOE shall detect flaws during the initialization, Personalization and operational usage. The TOE shall provide safe destruction techniques for the keys (other than the SCD) it stores in case of erasure, re-import or re-generation.

#### **OT.Keys\_Secrecy**

##### ***Secrecy of Keys***

The secrecy of the keys (other than the SCD) stored in the TOE is reasonably assured against attacks with a high attack potential.

#### **OT.TOE\_AuthKey\_Unique**

##### ***Uniqueness of the TOE authentication key(s)***

The TOE shall ensure the cryptographic quality of the asymmetric authentication key pair used for the TOE authentication. The private key used for TOE authentication can practically occur only once and cannot be reconstructed from the public key. In that context 'practically occur once' means that the probability of equal TOE authentication key is negligible low.

#### **OT.Lifecycle\_Management**

##### ***Management of the life cycle***

The TOE provides a life cycle management enabling to separate its life cycle in two main phases. The first one (phase 6) is the one during which the TOE is under the sole control of the Personalization Agent. The following operation may be realized:

- o The SCD, SVD and keys may be created, generated, imported or erased
- o The PINs/PUK (s) may be created and loaded
- o SVD and public keys may be exported Once performed, the Personalization Agent switches the TOE in phase 7. This transition is irreversible leaving the TOE under the sole control of the R.Sigy and R.Admin according to the TOE specification and security rules set by the Personalization Agent.

#### **OT.eServices**

##### ***Provision of eServices***

The TOE provides the following mechanisms:

- o decrypt encryption decipherment keys using asymmetric mechanisms;
- o digital authentication: authentication of the TOE (on behalf of the TOE holder) using an asymmetric private key;

Moreover, the TOE ensures these keys remain genuine by enforcing an access control over the update of these keys, in order to ensure that only entitled entities can change them.

These mechanisms provided by the electronic document's chip are protected against attacks with high attack potential.

#### **OT.AC\_Pers\_EAC**

##### ***Personalization of the Electronic Document***

The TOE must ensure that user data and TSF-Data that are permanently stored in the TOE can be written by authorized personalization agents only, with the following exception: an Authentication Terminal may also write or modify user data according to its effective

authorization. The effective authorization is determined by the electronic document during Terminal Authentication.

## **OT.Tracing**

### ***Tracing electronic document***

The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the electronic document remotely through establishing or listening to a communication via the contactless interface of the TOE without knowledge of the correct values of shared passwords (PACE passwords) in advance.

## **OT.ADMIN\_Configuration**

### ***Protection of the TOE administration***

In user phase, the TOE must ensure the administration actions are only authorized for Administrator. The TOE must control the access to its sensitive information and its functions and must provide the means to secure exchanges using cryptographic functions. The TOE must also ensure that any subject who is being authenticated as Administrator is only allowed Create or Delete Files in Use Phase.

## **OT.Key\_Usage\_Counter**

### ***Configuration of Key Usage Counter***

The TOE must protect the key usage through OT.Key\_Usage\_Counter that support a Key Usage Counter which should be decremented by one each time the key is used. Once the counter is depleted, the key should become unusable.

## **7.2 Security Objectives for the Operational Environment**

### **7.2.1 All SSCD parts**

#### **OE.SVD\_Auth**

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

#### **OE.CGA\_QCert**

##### ***Generation of qualified certificates***

The CGA shall generate a qualified certificate that includes (amongst others): a the name of the signatory controlling the TOE; b the SVD matching the SCD stored in the TOE and being under sole control of the signatory; c the advanced signature of the CSP.

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

#### **OE.DTBS\_Intend**

##### ***SCA sends data intended to be signed***

The signatory shall use a trustworthy SCA that:

- o generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE;
- o sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE;
- o attaches the signature produced by the TOE to the data or provides it separately.

## **OE.Signatory**

### ***Security obligation of the signatory***

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

## **7.2.2 SSCD parts 2, 3 and 4 only**

## **OE.HID\_VAD**

### ***Protection of the VAD***

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

## **OE.DTBS\_Protect**

### ***SCA protects the data intended to be signed***

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

## **7.2.3 SSCD parts 2, 3, 5 and 6 only**

## **OE.SSCD\_Prov\_Service**

### ***Authentic SSCD provided by SSCD-provisioning service***

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

## **7.2.4 SSCD parts 3 and 6 only**

## **OE.SCD/SVD\_Auth\_Gen**

### ***Authorised SCD/SVD generation***

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

## **OE.SCD\_Secrecy**

### ***SCD Secrecy***



The CSP shall protect the confidentiality of the SCD during generation and export to the TOE. The CSP shall not use the SCD for creation of any signature and shall irreversibly delete the SCD in the operational environment after export to the TOE.

#### **OE.SCD\_Unique**

##### ***Uniqueness of the signature creation data***

The CSP shall ensure the cryptographic quality of the SCD/SVD pair, which is generated in the environment, for the qualified or advanced electronic signature. The SCD used for signature creation shall practically occur only once, i.e. the probability of equal SCDs shall be negligible, and the SCD shall not be reconstructable from the SVD.

#### **OE.SCD\_SVD\_Corresp**

##### ***Correspondence between SVD and SCD***

The CSP shall ensure the correspondence between the SVD and the SCD generated by the CSP. This includes the correspondence between the SVD sent to the CGA and the SCD exported to the TOE of the signatory identified in the SVD certificate.

### **7.2.5 SSSCD part 4 only**

#### **OE.Dev\_Prov\_Service**

##### ***Authentic SSSCD provided by SSSCD Provisioning Service***

The SSSCD Provisioning Service handles authentic devices that implement the TOE, prepares the TOE for proof as SSSCD to external entities, personalizes the TOE for the legitimate user as signatory, links the identity of the TOE as SSSCD with the identity of the legitimate user, and delivers the TOE to the signatory.

#### **OE.CGA\_TC\_SVD\_Imp**

##### ***CGA trusted channel for SVD import***

The CGA shall detect alteration of the SVD imported from the TOE with the claimed identity of the SSSCD.

#### **OE.CGA\_SSSCD\_Auth**

##### ***Pre-initialization of the TOE for SSSCD authentication***

The CSP shall check by means of the CGA whether the device presented for application of a (qualified) certificate holds unique identification as SSSCD, successfully proved this identity as SSSCD to the CGA, and whether this identity is linked to the legitimate holder of the device as applicant for the certificate.

### **7.2.6 SSSCD parts 5 and 6 only**

#### **OE.HID\_TC\_VAD\_Exp**

##### ***Trusted channel of HID for VAD export***

The HID provides the human interface for user authentication. The HID will ensure confidentiality and integrity of the VAD as needed by the authentication method employed including export to the TOE by means of a trusted channel.

*Application Note:*

This security objective for the TOE is partly covering OE.HID\_VAD from the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI). While OE.HID\_VAD in the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI) requires only the operational environment to protect VAD, this ST requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID\_TC\_VAD\_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE\_TC\_VAD\_Exp. Therefore this ST re-assigns partly the VAD protection from the operational environment as described by OE.HID\_VAD to the TOE as described by OT.TOE\_TC\_VAD\_Exp and leaves only the necessary functionality by the HID.

### **OE.SCA\_TC\_DTBS\_Exp**

#### ***Trusted channel of SCA for DTBS export***

The SCA provides a trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS/R cannot be altered undetected in transit between the SCA and the TOE.

*Application Note:*

This security objective for the TOE is partly covering OE.DTBS\_Protect from the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI). While OE.DTBS\_Protect in the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI) requires only the operational environment to protect DTBS, this ST requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA\_TC\_DTBS\_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE\_TC\_DTBS\_Exp. Therefore this ST re-assigns partly the DTBS protection from the operational environment as described by OE.DTBS\_Protect to the TOE as described by OT.TOE\_TC\_DTBS\_Exp and leaves only the necessary functionality by the SCA.

## **7.2.7 Additional Security Objectives for the Operational Environment**

### **OE.LinkSCD\_QualifiedCertificate**

#### ***Link between SCD stored in the TOE and the relevant qualified certificate***

The Role in charge of creating and updating the SCD (Personalization Agent, R.Admin), or the trusted IT entity involved in the updating process (CSP) shall ensure an unambiguous link between the (qualified) certificate(s) and the corresponding SCD(s). This link might be figured out by a PKCS#15 structure, an XML structure, an identifier linking the file containing the (qualified) certificate or the URL hosting them to the SCD(s) stored in the TOE. In particular, it implies this link is updated, each time the SCD(s) is created, imported, erased or generated.

### **OE.AuthKey\_Transfer**

#### ***Secure transfer of authentication key(s) to the TOE***

The entity in charge of generating the authentication keys to be loaded in the TOE shall ensure the confidentiality of the key(s) transferred to the TOE.

#### **OE.AuthKey\_Unique**

##### ***Uniqueness of the authentication key(s)***

The entity in charge of generating the authentication keys to be loaded in the TOE shall ensure the cryptographic quality of the authentication key(s). The authentication key used for authentication can practically occur only once and, in case of a TOE authentication key cannot be reconstructed from its public portion. In that context 'practically occur once' means that the probability of equal keys is negligible low.

#### **OE.TOE\_PublicKeyAuth\_Transfer**

##### ***Secure transfer of public authentication key(s) of the TOE***

The entity in charge of generating the authentication certificate from the TOE's authentication public key generated in the TOE shall ensure the authenticity of this data when transferred from the TOE. This may be achieved through operational measures.

#### **OE.Terminal\_Authentication**

##### ***AuthenticationKey pairs needed for Terminal Authentication***

The electronic document issuer shall establish a public key infrastructure for the card verifiable certificates used for Terminal Authentication. For this aim, the electronic document issuer shall run a Country Verifying Certification Authority. The instances of the PKI shall fulfill the requirements and rules of the corresponding certificate policy. The electronic document issuer shall make the CVCA certificate available to the personalization agent or the manufacturer.

#### **OE.Legislative\_Compliance**

##### ***Issuing of the electronic document***

The electronic document Issuer must issue the electronic document and approve it using the terminals complying with all applicable laws and regulations.

#### **OE.Passive\_Auth\_Sign**

##### ***Authentication of electronic document by Signature***

The electronic document Issuer has to establish the necessary public key infrastructure as follows: the Issuer CA acting on behalf and according to the policy of the electronic document Issuer must (i) generate a cryptographically secure Issuer CA Key Pair, (ii) ensure the secrecy of the Issuer CA Private Key and issue certificate for its Sub-CA in a secure operational environment (if needed), and (iii) publish its certificate. Hereby authenticity and integrity of these certificates are being maintained. An Issuer CA acting in accordance with the Issuer CA policy must generate digital seals protecting the content of electronic document in a secure operational environment only.

The Issuer CA must issue its certificates exclusively to the rightful organizations (and must sign exclusively correct digital seals to be stored on electronic document).

## **OE.Personalization**

### ***Personalization of electronic document***

The electronic document Issuer must ensure that the Personalization Agents acting on his behalf (i) store the corresponding data in the electronic document (electronic Personalization) for the electronic document holder, (ii) write the document details data, (iii) write the initial TSF data, (iv) sign the digital seal protecting the content of the electronic document.

## **OE.Terminal**

### ***Terminal operating***

The terminal operators must operate their terminals as follows:

- o The related terminals are used by terminal operators and by electronic document holders.
- o The related terminals implement the terminal parts of the PACE protocol and check the digital seal generated by the Issuer CA included in the electronic document and protecting its content. The BAT shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
- o The related terminals securely store the Issuer CA certificate in order to be able to verify the digital seals generated by the Issuer CA and included in the electronic document to protect its content (integrity and authenticity of the data stored in the electronic document).
- o The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords or the PIN, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE.

## **OE.Electronic\_Document\_Holder**

### ***Electronic document holder Obligations***

The electronic document holder may reveal, if necessary, his or her verification values of the PACE password or the PIN to an authorized person or device who definitely act according to respective regulations and are trustworthy.

## **7.3 Security Objectives Rationale**

### **7.3.1 Threats**

#### **7.3.1.1 Threats drawn from the Protection Profiles**

**T.SCD\_Divulg** addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the [Directive], bullet (18). This threat is countered by

- o OE.SCD\_Secrecy, which assures the secrecy of the SCD in the CSP environment, and

- o OT.SCD\_Secrecy, which assures the secrecy of the SCD during use by the TOE for signature creation. Furthermore, generation and/or import of SCD known by an attacker is countered by OE.SCD/SVD\_Auth\_Gen, which ensures that only authorised SCD generation in the environment is possible, and OT.SCD\_Auth\_Imp, which ensures that only authorised SCD import is possible.

**T.SCD\_Derive** 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.

- o OT.SCD/SVD\_Auth\_Gen counters this threat by implementing cryptographically secure generation of the SCD/SVD pair.
- o OT.Sig\_Secure ensures cryptographically secure electronic signatures.
- o OE.SCD\_Unique counters this threat by implementing cryptographically secure generation of the SCD/SVD pair.

**T.Hack\_Phys** 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 resisting tampering attacks. OT.Keys\_Secrecy preserves the secrecy of all the authentication and eServices keys stored in the TOE.

**T.SVD\_Forgery** deals with the forgery of the SVD exported by the TOE to the CGA for certificate generation. T.SVD\_Forgery is addressed by

- o 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
- o OE.SVD\_Auth that ensures the integrity of the SVD exported by the TOE to the CGA.
- o OE.SCD\_SVD\_Corresp, which ensures correspondence between SVD and SCD.
- o Additionally T.SVD\_Forgery is addressed by OT.TOE\_TC\_SVD\_Exp, which ensures that the TOE sends the SVD in a verifiable form through a trusted channel to the CGA, as well as by OE.CGA\_TC\_SVD\_Imp, which provides verification of SVD authenticity by the CGA.

**T.SigF\_Misuse** addresses the threat of misuse of the TOE signature creation function to create SDO by others than the signatory to create an electronic signature on data for which the signatory has not expressed the intent to sign, as required by ([Directive], Annex III, paragraph 1, bullet (c) or new [eIDAS\_Regulation], Article 26, bullet (a)). OT.Lifecycle\_Security (Lifecycle security) requires the TOE to detect flaws during the initialization, personalization and operational usage including secure destruction of the SCD, which may be initiated by the signatory. OT.Sigy\_SigF (Signature creation function for the legitimate signatory only) ensures that the TOE provides the signature creation function for the legitimate signatory only. OE.DTBS\_Intend (Data intended to be signed) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign and OE.DTBS\_Protect counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE. OT.DTBS\_Integrity\_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. If the SCA provides a human interface for user

authentication, OE.HID\_VAD (Protection of the VAD) provides confidentiality and integrity of the VAD as needed by the authentication method employed. OE.Signatory ensures that the signatory checks that an SCD stored in the SSCD when received from an SSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the signatory becomes control over the SSCD. OE.Signatory ensures also that the signatory keeps their VAD confidential. OT.Lifecycle\_Management ensures that when the TOE is under the Personalization Agent control, it cannot be misused to sign on behalf of the legitimate Signatory.

The combination of OT.TOE\_TC\_DTBS\_Imp (Trusted channel of TOE for DTBS) and OE.SCA\_TC\_DTBS\_Exp (Trusted channel of SCA for DTBS) counters the undetected manipulation of the DTBS during the transmission from the SCA to the TOE.

If the SCA provides a human interface for user authentication, OE.HID\_TC\_VAD\_Exp (Trusted channel of HID for VAD) requires the HID to protect the confidentiality and the integrity of the VAD as needed by the authentication method employed. The HID and the TOE will protect the VAD by a trusted channel between HID and TOE according to OE.HID\_TC\_VAD\_Exp (Trusted channel of HID for VAD) and OT.TOE\_TC\_VAD\_Imp (Trusted channel of TOE for VAD).

**T.DTBS\_Forgery** addresses the threat arising from modifications of the data sent as input to the TOE's signature creation function that does not represent the DTBS as presented to the signatory and for which the signature has expressed its intent to sign. The TOE IT environment addresses T.DTBS\_Forgery by the means of OE.DTBS\_Intend, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE, and by means of OE.DTBS\_Protect, which ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE. The TOE counters this threat by the means of OT.DTBS\_Integrity\_TOE by ensuring the integrity of the DTBS/R inside the TOE.

The threat T.DTBS\_Forgery is addressed by the security objectives OT.TOE\_TC\_DTBS\_Imp (Trusted channel of TOE for DTBS) and OE.SCA\_TC\_DTBS\_Exp (Trusted channel of SCA for DTBS), which ensure that the DTBS/R is sent through a trusted channel and cannot be altered undetected in transit between the SCA and the TOE.

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

### 7.3.1.2 Additional Threats

**T.Key\_Divulg** addresses the threat against the (1) authentication key of the TOE, (2) the authentication keys of entities and (3) the eServices keys stored in the TOE due to storage and copying of key(s) outside the TOE. This threat is countered by OT.Keys\_Secrecy which

assures the secrecy of the keys stored and used by the TOE. OE.AuthKey\_Transfer ensures the confidentiality of the authentication keys transferred to the TOE. OT.Key\_Lifecycle\_Security (Lifecycle security) ensures the secrecy of the keys stored in the TOE during the whole life of the TOE.

**T.Key\_Derive** deals with attacks on authentication and eServices keys via public known data produced or received by the TOE (public key, authentication cryptogram,...). This threat is countered by OE.AuthKey\_Unique (in case of import) and OT.TOE\_AuthKey\_Unique (in case of TOE's authentication key generation) that provides cryptographic secure generation of the keys. OT.Authentication\_Secure ensures secure authentication cryptograms.

**T.TOE\_PublicAuthKey\_Forgery** deals with the forgery of the TOE's public key used for authentication exported by the TOE to an entitled entity for the generation of the certificate. This is addressed by OE.TOE\_PublicKeyAuth\_Transfer which ensures the authenticity of the TOE's public key for authentication.

**T.Authentication\_Replay** deals with the threats when an attacker retrieves an authentication cryptogram presented to the TOE by an entity and presents it again to the TOE in order to grant some rights and gain access to some data on the TOE. This threat is addressed by OT.Authentication\_Secure that ensures the authentication cryptogram can not be replayed as they rely on random data internally generated by the TOE.

**T.Counterfeit** addresses the attack of an unauthorized copy or reproduction of the genuine electronic document. This attack is countered by the proof of the chip's authenticity, as aimed by OT.Authentication\_Secure using a Chip Authentication key pair that is generated within the issuing PKI branch, as aimed by OE.AuthKey\_Transfer, OE.AuthKey\_Unique, OE.TOE\_PublicKeyAuth\_Transfer.

**T.Sensitive\_Data** is countered by the TOE-Objective OT.Authentication\_Secure, that requires that read access to sensitive user data is only granted to Authentication Terminals with corresponding access rights. Furthermore, it is required that the confidentiality of the data is ensured during contactless transmission. The objective OE.Terminal\_Authentication requires the electronic document issuer to provide the public key infrastructure (PKI) to generate and distribute the card verifiable certificates needed by the electronic document to securely authenticate the Authentication Terminal.

**T.Abuse-Func** addresses attacks of misusing TOE's functionality to manipulate or to disclosure the stored User- or TSF-data as well as to disable or to bypass the soft-coded security functionality. The security objective OT.Authentication\_Secure ensures that the usage of functions having not to be used in the operational phase is effectively prevented.

**T.Eavesdropping** addresses listening to the contactless communication between the TOE and a BAT or an Authentication Terminal in order to gain access to transferred user data.

This threat is countered by the security objective OT.Authentication\_Secure through a trusted channel based on PACE or EAC Authentication

**T.Forgery** addresses the fraudulent, complete or partial alteration of user data and/or TSF-Data stored on the TOE, and/or exchanged between the TOE and the terminal. The threat T.Forgery addresses the fraudulent, complete or partial alteration of the User Data or/and TSF-data stored on the TOE or/and exchanged between the TOE and the terminal. The security objective OT.AC\_Pers\_EAC requires the TOE to limit the write access for the travel document to the trustworthy Personalization Agent (cf. OE.Personalization). The TOE will protect the integrity and authenticity of the stored and exchanged User Data or/and TSF-data as aimed by the security objective OT.Authentication\_Secure. This objective contribute also to protecting integrity of the User Data or/and TSF-data stored on the TOE. A terminal operator operating his terminals according to OE.Terminal and performing the digital seal verification as aimed by OE.Passive\_Auth\_Sign will be able to effectively verify integrity and authenticity of the data received from the TOE.

**T.Information\_Leakage** is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objective OT.Authentication\_Secure.

**T.Malfunction** is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objective OT.Authentication\_Secure.

**T.Phys-Tamper** is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objective OT.Authentication\_Secure.

**T.Skimming** addresses accessing the user data (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contactless interface. This threat is countered by the security objective OT.Authentication\_Secure through the PACE authentication. The objective OE.Electronic\_Document\_Holder ensures that a PACE session can only be established either by the travel document holder itself or by an authorised person or device, and, hence, cannot be captured by an attacker. Additionally, the threat is also addressed by OT.Authentication\_Secure that demands a trusted channel based on Chip Authentication, and requires that read access to sensitive user data is only granted to Authentication Terminals with corresponding access rights. Moreover, OE.Terminal\_Authentication requires the electronic document issuer to provide the corresponding PKI.

**T.Tracing** addresses gathering TOE tracing data identifying it remotely by establishing or listening to a communication via the contactless interface of the TOE, whereby the attacker does not a priori know the correct values of the PACE password. This threat is directly countered by security objectives OT.Tracing (no gathering TOE tracing data) and



OE.Electronic\_Document\_Holder (the attacker does not a priori know the correct values of the shared passwords).

**T.ADMIN\_Configuration** The threat T.ADMIN\_Configuration "Tampering attempt of the TOE during administration" addresses attacks in Operational use phase. The attacker trying to access to unauthorized TOE functions, trying to access or to modify sensitive information exchanged between the TOE and the Administration system or trying to Create or Delete EF files in Use Phase. Protection of the TOE during this phases is directly addressed by OT.ADMIN\_Configuration "Protection of the TOE administration".

**T.Key\_Access** The threat T.Key\_Access addresses the threat of access to the internal secret cryptographic keys of the TOE. The TOE protects the key usage through OT.Key\_Usage\_Counter "Configuration of Key Usage Counter" that support a Key Usage Counter that is decremented by one each time the key is used. Once the counter is depleted, the key becomes unusable. In the case of CA key, the Key Usage Counter will be reset to the maximum usage if the CA key is re-generated in USE phase.

### 7.3.2 **Organizational Security Policies**

#### 7.3.2.1 Security Policies drawn from the Protection Profiles

**P.CSP\_QCert** 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

- o OT.Lifecycle\_Security, which requires the TOE to detect flaws during the initialization, personalization and operational usage;
- o OT.SCD\_SVD\_Corresp, which requires to ensure the correspondence between the SVD and the SCD during their generation;
- o OE.SCD/SVD\_Auth\_Gen, which ensures that the SCD/SVD generation can be invoked by authorised users only;
- o OT.SCD\_Auth\_Imp which ensures that authorised users only may invoke the import of the SCD;
- o OE.SCD\_SVD\_Corresp, which requires the CSP to ensure the correspondence between the SVD and the SCD during their generation, and
- o 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. According to OT.TOE\_SSCD\_Auth the copies of the TOE will hold unique identity and authentication data as SSCD and provide security mechanisms enabling the CGA to identify and to authenticate the TOE as SSCD to prove this identity as SSCD to the CGA. The OE.CGA\_SSCD\_Auth ensures that the SP checks the proof of the device presented of the applicant that it is a SSCD.

**P.QSign** provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate. OT.Sigy\_SigF ensures signatory's sole control of the SCD by requiring the TOE

to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others. OT.Sig\_Secure ensures that the TOE creates electronic signatures, which cannot be forged without knowledge of the SCD through robust encryption techniques. OE.CGA\_QCert addresses the requirement of qualified or non-qualified electronic certificates building a base for the electronic signature. OE.DTBS\_Intend ensures that the SCA provides only those DTBS to the TOE, which the signatory intends to sign.

**P.Sigy\_SSCD** requires the TOE to meet (Annex III of the [Directive] or Article 26 of new [eIDAS\_Regulation]). This is ensured as follows:

- o OE.SCD\_Unique meets the (paragraph 1 bullet (a) of the [Directive], Annex III or bullet (a) of new [eIDAS\_Regulation], Article 26), by the requirements that the SCD used for signature creation can practically occur only once;
- o OT.SCD\_Unique meets Annex III, by the requirements that the SCD used for signature creation can practically occur only once;
- o OT.SCD\_Unique, OT.SCD\_Secrecy and OT.Sig\_Secure meet the requirement in Annex III by the requirements to ensure secrecy of the SCD;
- o OT.EMSEC\_Design and OT.Tamper\_Resistance address specific objectives to ensure secrecy of the SCD against specific attacks;
- o OT.SCD\_Auth\_Imp, which limits SCD import to authorised users only;
- o OE.SCD\_Secrecy, which ensures the confidentiality of the SCD during generation and export to the TOE, and deletes the SCD after export to the TOE. The CSP does not use the SCD for signature creation;
- o OT.SCD\_Secrecy and OT.Sig\_Secure meet the requirement in in paragraph 1(b) of Annex III by the requirements to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE; — OT.SCD/SVD\_Auth\_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only, and
- o OT.Sigy\_SigF meets the requirement in Annex III by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others;
- o OT.DTBS\_Integrity\_TOE meets the requirements in paragraph 2 of Annex III as the TOE shall not alter the DTBS/R. Annex III requires that a 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
- o OT.Lifecycle\_Security requiring the TOE to detect flaws during the initialization, personalization and operational usage;
- o OE.SCD/SVD\_Auth\_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only;
- o OT.Sigy\_SigF, which requires the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others.
- o OE.SSCD\_Prov\_Service ensures that the signatory obtains an authentic copy of the TOE, initialized and personalized SSCD from an SSCD-provisioning service.

- o OE.Dev\_Prov\_Service ensures that the legitimate user obtains a TOE sample as an authentic, initialized and personalized TOE from an SSCD Provisioning Service through the TOE delivery procedure. If the TOE implements SCD generated under control of the SSCD Provisioning Service the legitimate user receives the TOE as SSCD. If the TOE is delivered to the legitimate user without SCD In the operational phase he or she applies for the (qualified) certificate as the Device holder and legitimate user of the TOE. The CSP will use the TOE security feature (addressed by the security objectives OT.TOE\_SSCD\_Auth and OT.TOE\_TC\_SVD\_Exp) to check whether the device presented is a SSCD linked to the applicant as required by OE.CGA\_SSCD\_Auth and the received SVD is sent by this SSCD as required by OE.CGA\_TC\_SVD\_Imp. Thus the obligation of the SSCD provision service for the first SCD/SVD pair is complemented in an appropriate way by the CSP for the SCD/SVD pair generated outside the secure preparation environment.

**P.Sig\_Non-Repud** deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in their certificate valid at the time of signature creation. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, which ensures the aspects of signatory's sole control over and responsibility for the electronic signatures created with the TOE. OE.SSCD\_Prov\_Service ensures that the signatory obtains an authentic copy of the TOE, initialized and personalized as SSCD from the SSCD-provisioning service. OE.SCD/SVD\_Auth\_Gen, OE.SCD\_Secrecy and OE.SCD\_Unique ensure the security of the SCD in the CSP environment. OE.SCD\_Secrecy ensures the confidentiality of the SCD during generation, during and after export to the TOE. The CSP does not use the SCD for creation of any signature and deletes the SCD irreversibly after export to the TOE. OE.SCD\_Unique provides that the signatory's SCD can practically occur just once. OE.SCD\_SVD\_Corresp ensures that the SVD in the certificate of the signatory corresponds to the SCD that is implemented in the copy of the TOE of 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 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). OT.Sigy\_SigF provides that only the signatory may use the TOE for signature creation. As prerequisite OE.Signatory ensures that the signatory keeps their VAD confidential. OE.DTBS\_Intend, OE.DTBS\_Protect and OT.DTBS\_Integrity\_TOE ensure that the TOE creates electronic signatures only for those DTBS/R, which the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig\_Secure ensure that only this SCD may create a valid electronic signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE OT.Lifecycle\_Security (Lifecycle security), OT.SCD\_Secrecy (Secrecy of the signature creation data), OT.EMSEC\_Design (Provide physical emanations security), OT.Tamper\_ID (Tamper detection) and OT.Tamper\_Resistance (Tamper resistance) protect the SCD against any compromise. The TOE security feature addressed by the security objectives OT.TOE\_SSCD\_Auth and OT.TOE\_TC\_SVD\_Exp supported by OE.Dev\_Prov\_Service enables the verification whether the device presented by the applicant is a SSCD as required

by OE.CGA\_SSCD\_Auth and the received SVD is sent by the device holding the corresponding SCD as required by OE.CGA\_TC\_SVD\_Imp. OE.DTBS\_Intend (SCA sends data intended to be signed), OE.DTBS\_Protect OT.DTBS\_Integrity\_TOE (DTBS/R integrity inside the TOE) ensure that the TOE generates electronic signatures only for a DTBS/R that the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig\_Secure ensure that only this SCD may create a valid electronic signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE OT.Lifecycle\_Security (Lifecycle security), OT.SCD\_Secrecy (Secrecy of the signature creation data), OT.EMSEC\_Design (Provide physical emanations security), OT.Tamper\_ID (Tamper detection) and OT.Tamper\_Resistance (Tamper resistance) protect the SCD against any compromise. OT.LifeCycle\_Management ensures that when the TOE is under the Personalization Agent control, it can not be misused to sign on behalf of the legitimate Signatory. OE.LinkSCD\_QualifiedCertificate ensure the SCA always uses the SCD it intends to, in order to create a digital signature. OE.LinkSCD\_QualifiedCertificate ensures that the SCA can unambiguously sort out within the TOE file structure the SCD matching any (qualified) certificate it has chosen and intends to use.

The confidentiality of VAD is protected during the transmission between the HI device and TOE according to OE.HID\_TC\_VAD\_Exp (Trusted channel of HID for VAD) and OT.TOE\_TC\_VAD\_Imp (Trusted channel of TOE for VAD).

OE.DTBS\_Intend (SCA sends data intended to be signed), OT.DTBS\_Integrity\_TOE (DTBS/R integrity inside the TOE), OE.SCA\_TC\_DTBS\_Exp (Trusted channel of SCA for DTBS) and OT.TOE\_TC\_DTBS\_Imp (Trusted channel of TOE for DTBS) ensure that the TOE generates electronic signatures only for a DTBS/R that the signatory has decided to sign as DTBS.

### 7.3.2.2 Additional Security Policies

**P.LinkSCD\_QualifiedCertificate** ensures that the SCA can unambiguously find within the TOE File structure the SCD matching a (qualified) certificate it has chosen to perform an electronic signature. It is addressed by OE.LinkSCD\_QualifiedCertificate that ensures an unambiguous link between each (qualified) certificate and the matching SCD loaded in the TOE.

**P.TOE\_PublicAuthKey\_Cert** ensures that each private key(s) of the TOE for authentication matches the public key stored within the relevant certificate issued by an entitled entity. The authentication public key is exported thanks to OE.TOE\_PublicKeyAuth\_Transfer.

**P.eServices** ensures that the TOE provides secure eServices functionalities. It is addressed by OT.eServices.

**P.EAC\_Terminal** addresses the requirement for Authentication Terminals to implement the terminal parts of the protocols needed to executed EAC according to its specification in [TR-03110-1] and [TR-03110-3], and to store (static keys) or generate (temporary keys and nonces) the needed related credentials. This is enforced by OE.AuthKey\_Transfer, OE.AuthKey\_Unique and OE.TOE\_PublicKeyAuth\_Transfer which require Chip Authentication and Restricted Identity keys to be correctly generated and stored, by

OE.Terminal\_Authentication for the PKI needed for Terminal Authentication, and by OE.Terminal which covers the PACE protocol and the digital seal verification.

**P.Terminal\_PKI** is enforced by establishing the receiving PKI branch as aimed by the objective OE.Terminal\_Authentication

**P.Card\_PKI** is enforced by establishing the issuing PKI branch as aimed by the objective OE.Passive\_Auth\_Sign (for the digital seal verification).

**P.Pre-Operational** is enforced by the following security objectives: OT.Identification is affine to the OSP's property 'traceability before the operational phase'; OT.AC\_Pers\_EAC and OE.Personalization together enforce the OSP's properties 'correctness of the User- and the TSF-data stored' and 'authorisation of Personalisation Agents'; OE.Legislative\_Compliance is affine to the OSP's property 'compliance with laws and regulations'.

**P.Terminal** is obviously enforced by the objective OE.Terminal, whereby the one-to-one mapping between the related properties is applicable

**P.Trustworthy\_PKI** is enforced by OE.Passive\_Auth\_Sign (for Issuer CA, issuing PKI branch).

**P.Manufact** The OSP P.Manufact "Manufacturing of the electronic document's chip" requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalisation Data as being fulfilled by OT.Identification.

### 7.3.3 Assumptions

#### 7.3.3.1 All SSCD parts

**A.CGA** establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by OE.CGA\_QCert (Generation of qualified certificates), which ensures the generation of qualified certificates, and by OE.SVD\_Auth (Authenticity of the SVD), which ensures the protection of the integrity of the received SVD and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

**A.SCA** establishes the trustworthiness of the SCA with respect to generation of DTBS/R. This is addressed by OE.DTBS\_Intend (Data intended to be signed) which ensures that the SCA generates the DTBS/R of the data that have been presented to the signatory as DTBS and

which the signatory intends to sign in a form which is appropriate for being signed by the TOE.

### 7.3.3.2 Parts 3 and 6 only

**A.CSP** establishes several security aspects concerning handling of SCD and SVD by the CSP. That the SCD/SVD generation device can only be used by authorised users is addressed by OE.SCD/SVD\_Auth\_Gen (Authorised SCD/SVD Generation), that the generated SCD is unique and cannot be derived by the SVD is addressed by OE.SCD\_Unique (Uniqueness of the signature creation data), that SCD and SVD correspond to each other is addressed by OE.SCD\_SVD\_Corresp (Correspondence between SVD and SCD), and that the SCD are kept confidential, are not used for signature generation in the environment and are deleted in the environment once exported to the TOE is addressed by OE.SCD\_Secrecy (SCD Secrecy).

### 7.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
<a href="#">T.SCD_Divulg</a>	<a href="#">OT.SCD_Secrecy</a> , <a href="#">OT.SCD_Auth_Imp</a> , <a href="#">OE.SCD/SVD_Auth_Gen</a> , <a href="#">OE.SCD_Secrecy</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.SCD_Derive</a>	<a href="#">OT.SCD/SVD_Auth_Gen</a> , <a href="#">OT.Sig_Secure</a> , <a href="#">OE.SCD_Unique</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Hack_Phys</a>	<a href="#">OT.SCD_Secrecy</a> , <a href="#">OT.EMSEC_Design</a> , <a href="#">OT.Tamper_ID</a> , <a href="#">OT.Tamper_Resistance</a> , <a href="#">OT.Keys_Secrecy</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.SVD_Forgery</a>	<a href="#">OT.SCD_SVD_Corresp</a> , <a href="#">OE.SVD_Auth</a> , <a href="#">OE.SCD_SVD_Corresp</a> , <a href="#">OT.TOE_TC_SVD_Exp</a> , <a href="#">OE.CGA_TC_SVD_Imp</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.SigF_Misuse</a>	<a href="#">OT.Lifecycle_Security</a> , <a href="#">OT.Sigy_SigF</a> , <a href="#">OT.DTBS_Integrity_TOE</a> , <a href="#">OE.Signatory</a> , <a href="#">OE.DTBS_Intend</a> , <a href="#">OE.HID_VAD</a> , <a href="#">OE.DTBS_Protect</a> , <a href="#">OT.Lifecycle_Management</a> , <a href="#">OT.TOE_TC_VAD_Imp</a> , <a href="#">OT.TOE_TC_DTBS_Imp</a> , <a href="#">OE.HID_TC_VAD_Exp</a> , <a href="#">OE.SCA_TC_DTBS_Exp</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.DTBS_Forgery</a>	<a href="#">OT.DTBS_Integrity_TOE</a> , <a href="#">OE.DTBS_Intend</a> , <a href="#">OE.DTBS_Protect</a> , <a href="#">OT.TOE_TC_DTBS_Imp</a> , <a href="#">OE.SCA_TC_DTBS_Exp</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Sig_Forgery</a>	<a href="#">OT.SCD_Unique</a> , <a href="#">OT.Sig_Secure</a> , <a href="#">OE.CGA_QCert</a> , <a href="#">OE.SCD_Unique</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Key_Divulg</a>	<a href="#">OT.Key_Lifecycle_Security</a> , <a href="#">OT.Keys_Secrecy</a> , <a href="#">OE.AuthKey_Transfer</a>	<a href="#">Section 7.3.1</a>

<a href="#">T.Key Derive</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OT.TOE AuthKey Unique</a> , <a href="#">OE.AuthKey Unique</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.TOE PublicKeyAuth Forgery</a>	<a href="#">OE.TOE PublicKeyAuth Transfer</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Authentication Replay</a>	<a href="#">OT.Authentication Secure</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Counterfeit</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OE.AuthKey Transfer</a> , <a href="#">OE.AuthKey Unique</a> , <a href="#">OE.TOE PublicKeyAuth Transfer</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Sensitive Data</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OE.Terminal Authentication</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Abuse-Func</a>	<a href="#">OT.Authentication Secure</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Eavesdropping</a>	<a href="#">OT.Authentication Secure</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Forgery</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OT.AC Pers EAC</a> , <a href="#">OE.Passive Auth Sign</a> , <a href="#">OE.Personalization</a> , <a href="#">OE.Terminal</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Information Leakage</a>	<a href="#">OT.Authentication Secure</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Malfunction</a>	<a href="#">OT.Authentication Secure</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Phys-Tamper</a>	<a href="#">OT.Authentication Secure</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Skimming</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OE.Terminal Authentication</a> , <a href="#">OE.Electronic Document Holder</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Tracing</a>	<a href="#">OT.Tracing</a> , <a href="#">OE.Electronic Document Holder</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.ADMIN Configuration</a>	<a href="#">OT.ADMIN Configuration</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Key Access</a>	<a href="#">OT.Key Usage Counter</a>	<a href="#">Section 7.3.1</a>

**Table 16 Threats and Security Objectives - Coverage**

<b>Security Objectives</b>	<b>Threats</b>
<a href="#">OT.Lifecycle Security</a>	<a href="#">T.SigF Misuse</a>
<a href="#">OT.SCD Secrecy</a>	<a href="#">T.SCD Divulg</a> , <a href="#">T.Hack Phys</a>
<a href="#">OT.Sig Secure</a>	<a href="#">T.SCD Derive</a> , <a href="#">T.Sig Forgery</a>
<a href="#">OT.Sigy SigF</a>	<a href="#">T.SigF Misuse</a>
<a href="#">OT.DTBS Integrity TOE</a>	<a href="#">T.SigF Misuse</a> , <a href="#">T.DTBS Forgery</a>
<a href="#">OT.EMSEC Design</a>	<a href="#">T.Hack Phys</a>
<a href="#">OT.Tamper ID</a>	<a href="#">T.Hack Phys</a>
<a href="#">OT.Tamper Resistance</a>	<a href="#">T.Hack Phys</a>

<a href="#">OT.SCD/SVD Auth Gen</a>	<a href="#">T.SCD Derive</a>
<a href="#">OT.SCD Unique</a>	<a href="#">T.Sig Forgery</a>
<a href="#">OT.SCD SVD Corresp</a>	<a href="#">T.SVD Forgery</a>
<a href="#">OT.SCD Auth Imp</a>	<a href="#">T.SCD Divulg</a>
<a href="#">OT.TOE SSCD Auth</a>	
<a href="#">OT.TOE TC SVD Exp</a>	<a href="#">T.SVD Forgery</a>
<a href="#">OT.TOE TC VAD Imp</a>	<a href="#">T.SigF Misuse</a>
<a href="#">OT.TOE TC DTBS Imp</a>	<a href="#">T.SigF Misuse, T.DTBS Forgery</a>
<a href="#">OT.Identification</a>	
<a href="#">OT.Authentication Secure</a>	<a href="#">T.Key Derive, T.Authentication Replay, T.Counterfeit, T.Sensitive Data, T.Abuse-Func, T.Eavesdropping, T.Forgery, T.Information Leakage, T.Malfunction, T.Phys-Tamper, T.Skimming</a>
<a href="#">OT.Key Lifecycle Security</a>	<a href="#">T.Key Divulg</a>
<a href="#">OT.Keys Secrecy</a>	<a href="#">T.Hack Phys, T.Key Divulg</a>
<a href="#">OT.TOE AuthKey Unique</a>	<a href="#">T.Key Derive</a>
<a href="#">OT.Lifecycle Management</a>	<a href="#">T.SigF Misuse</a>
<a href="#">OT.eServices</a>	
<a href="#">OT.AC Pers EAC</a>	<a href="#">T.Forgery</a>
<a href="#">OT.Tracing</a>	<a href="#">T.Tracing</a>
<a href="#">OT.ADMIN Configuration</a>	<a href="#">T.ADMIN Configuration</a>
<a href="#">OT.Key Usage Counter</a>	<a href="#">T.Key Access</a>
<a href="#">OE.SVD Auth</a>	<a href="#">T.SVD Forgery</a>
<a href="#">OE.CGA QCert</a>	<a href="#">T.Sig Forgery</a>
<a href="#">OE.DTBS Intend</a>	<a href="#">T.SigF Misuse, T.DTBS Forgery</a>
<a href="#">OE.Signatory</a>	<a href="#">T.SigF Misuse</a>
<a href="#">OE.HID VAD</a>	<a href="#">T.SigF Misuse</a>
<a href="#">OE.DTBS Protect</a>	<a href="#">T.SigF Misuse, T.DTBS Forgery</a>
<a href="#">OE.SSCD Prov Service</a>	
<a href="#">OE.SCD/SVD Auth Gen</a>	<a href="#">T.SCD Divulg</a>
<a href="#">OE.SCD Secrecy</a>	<a href="#">T.SCD Divulg</a>
<a href="#">OE.SCD Unique</a>	<a href="#">T.SCD Derive, T.Sig Forgery</a>
<a href="#">OE.SCD SVD Corresp</a>	<a href="#">T.SVD Forgery</a>



<a href="#">OE.Dev Prov Service</a>	
<a href="#">OE.CGA TC SVD Imp</a>	<a href="#">T.SVD Forgery</a>
<a href="#">OE.CGA SSCD Auth</a>	
<a href="#">OE.HID TC VAD Exp</a>	<a href="#">T.SigF Misuse</a>
<a href="#">OE.SCA TC DTBS Exp</a>	<a href="#">T.SigF Misuse, T.DTBS Forgery</a>
<a href="#">OE.LinkSCD QualifiedCertificate</a>	
<a href="#">OE.AuthKey Transfer</a>	<a href="#">T.Key Divulg, T.Counterfeit</a>
<a href="#">OE.AuthKey Unique</a>	<a href="#">T.Key Derive, T.Counterfeit</a>
<a href="#">OE.TOE PublicKeyAuth Transfer</a>	<a href="#">T.TOE PublicAuthKey Forgery, T.Counterfeit</a>
<a href="#">OE.Terminal Authentication</a>	<a href="#">T.Sensitive Data, T.Skimming</a>
<a href="#">OE.Legislative Compliance</a>	
<a href="#">OE.Passive Auth Sign</a>	<a href="#">T.Forgery</a>
<a href="#">OE.Personalization</a>	<a href="#">T.Forgery</a>
<a href="#">OE.Terminal</a>	<a href="#">T.Forgery</a>
<a href="#">OE.Electronic Document Holder</a>	<a href="#">T.Skimming, T.Tracing</a>

**Table 17 Security Objectives and Threats - Coverage**

Organisational Security Policies	Security Objectives	Rationale
<a href="#">P.CSP_QCert</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.SCD SVD Corresp</a> , <a href="#">OE.CGA_QCert</a> , <a href="#">OT.SCD Auth Imp</a> , <a href="#">OE.SCD/SVD Auth Gen</a> , <a href="#">OE.SCD SVD Corresp</a> , <a href="#">OT.TOE SSCD Auth</a> , <a href="#">OE.CGA SSCD Auth</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.QSign</a>	<a href="#">OT.Sig Secure</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OE.CGA_QCert</a> , <a href="#">OE.DTBS Intend</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.Sigy_SSCD</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.SCD/SVD Auth Gen</a> , <a href="#">OT.SCD Unique</a> , <a href="#">OT.SCD Secrecy</a> , <a href="#">OT.Sig Secure</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OT.DTBS Integrity TOE</a> , <a href="#">OT.EMSEC Design</a> , <a href="#">OT.Tamper Resistance</a> , <a href="#">OT.SCD Auth Imp</a> , <a href="#">OE.SCD/SVD Auth Gen</a> , <a href="#">OE.SCD Secrecy</a> , <a href="#">OE.SCD Unique</a> , <a href="#">OT.TOE SSCD Auth</a> , <a href="#">OT.TOE TC SVD Exp</a> , <a href="#">OE.Dev Prov Service</a> , <a href="#">OE.CGA TC SVD Imp</a> , <a href="#">OE.CGA SSCD Auth</a> , <a href="#">OE.SSCD Prov Service</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.Sig Non-Repud</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.SCD Unique</a> , <a href="#">OT.SCD SVD Corresp</a> , <a href="#">OT.SCD Secrecy</a> , <a href="#">OT.Sig Secure</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OT.DTBS Integrity TOE</a> , <a href="#">OT.EMSEC Design</a> , <a href="#">OT.Tamper ID</a> , <a href="#">OT.Tamper Resistance</a> , <a href="#">OE.CGA_QCert</a> , <a href="#">OE.SVD Auth</a> , <a href="#">OE.DTBS Intend</a> , <a href="#">OE.Signatory</a> , <a href="#">OE.SCD/SVD Auth Gen</a> , <a href="#">OE.SCD Secrecy</a> , <a href="#">OE.SCD Unique</a> , <a href="#">OE.SCD SVD Corresp</a> , <a href="#">OT.TOE SSCD Auth</a> , <a href="#">OT.TOE TC SVD Exp</a> , <a href="#">OE.Dev Prov Service</a> , <a href="#">OE.CGA TC SVD Imp</a> , <a href="#">OE.CGA SSCD Auth</a> , <a href="#">OE.DTBS Protect</a> , <a href="#">OE.LinkSCD QualifiedCertificate</a> , <a href="#">OT.TOE TC VAD Imp</a> ,	<a href="#">Section 7.3.2</a>

	<a href="#">OT.TOE_TC_DTBS_Imp</a> , <a href="#">OE.HID_TC_VAD_Exp</a> , <a href="#">OE.SCA_TC_DTBS_Exp</a> , <a href="#">OE.SSCD_Prov_Service</a>	
<a href="#">P.LinkSCD_QualifiedCertificate</a>	<a href="#">OE.LinkSCD_QualifiedCertificate</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.TOE_PublicAuthKey_Cert</a>	<a href="#">OE.TOE_PublicKeyAuth_Transfer</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.eServices</a>	<a href="#">OT.eServices</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.EAC_Terminal</a>	<a href="#">OE.Terminal</a> , <a href="#">OE.Terminal_Authentication</a> , <a href="#">OE.AuthKey_Transfer</a> , <a href="#">OE.AuthKey_Unique</a> , <a href="#">OE.TOE_PublicKeyAuth_Transfer</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.Terminal_PKI</a>	<a href="#">OE.Terminal_Authentication</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.Card_PKI</a>	<a href="#">OE.Passive_Auth_Sign</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.Pre-Operational</a>	<a href="#">OT.AC_Pers_EAC</a> , <a href="#">OE.Personalization</a> , <a href="#">OE.Legislative_Compliance</a> , <a href="#">OT.Identification</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.Terminal</a>	<a href="#">OE.Terminal</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.Trustworthy_PKI</a>	<a href="#">OE.Passive_Auth_Sign</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.Manufact</a>	<a href="#">OT.Identification</a>	<a href="#">Section 7.3.2</a>

**Table 18 OSPs and Security Objectives - Coverage**

<b>Security Objectives</b>	<b>Organisational Security Policies</b>
<a href="#">OT.Lifecycle_Security</a>	<a href="#">P.CSP_QCert</a> , <a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OT.SCD_Secrecy</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OT.Sig_Secure</a>	<a href="#">P.QSign</a> , <a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OT.Sigy_SigF</a>	<a href="#">P.QSign</a> , <a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OT.DTBS_Integrity_TOE</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OT.EMSEC_Design</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OT.Tamper_ID</a>	<a href="#">P.Sig_Non-Repud</a>
<a href="#">OT.Tamper_Resistance</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OT.SCD/SVD_Auth_Gen</a>	<a href="#">P.Sigy_SSCD</a>
<a href="#">OT.SCD_Unique</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OT.SCD_SVD_Corresp</a>	<a href="#">P.CSP_QCert</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OT.SCD_Auth_Imp</a>	<a href="#">P.CSP_QCert</a> , <a href="#">P.Sigy_SSCD</a>

<a href="#">OT.TOE_SSCD_Auth</a>	<a href="#">P.CSP_QCert</a> , <a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OT.TOE_TC_SVD_Exp</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OT.TOE_TC_VAD_Imp</a>	<a href="#">P.Sig_Non-Repud</a>
<a href="#">OT.TOE_TC_DTBS_Imp</a>	<a href="#">P.Sig_Non-Repud</a>
<a href="#">OT.Identification</a>	<a href="#">P.Pre-Operational</a> , <a href="#">P.Manufact</a>
<a href="#">OT.Authentication_Secure</a>	
<a href="#">OT.Key_Lifecycle_Security</a>	
<a href="#">OT.Keys_Secrecy</a>	
<a href="#">OT.TOE_AuthKey_Unique</a>	
<a href="#">OT.Lifecycle_Management</a>	
<a href="#">OT.eServices</a>	<a href="#">P.eServices</a>
<a href="#">OT.AC_Pers_EAC</a>	<a href="#">P.Pre-Operational</a>
<a href="#">OT.Tracing</a>	
<a href="#">OT.ADMIN_Configuration</a>	
<a href="#">OT.Key_Usage_Counter</a>	
<a href="#">OE.SVD_Auth</a>	<a href="#">P.Sig_Non-Repud</a>
<a href="#">OE.CGA_QCert</a>	<a href="#">P.CSP_QCert</a> , <a href="#">P.QSign</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OE.DTBS_Intend</a>	<a href="#">P.QSign</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OE.Signatory</a>	<a href="#">P.Sig_Non-Repud</a>
<a href="#">OE.HID_VAD</a>	
<a href="#">OE.DTBS_Protect</a>	<a href="#">P.Sig_Non-Repud</a>
<a href="#">OE.SSCD_Prov_Service</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OE.SCD/SVD_Auth_Gen</a>	<a href="#">P.CSP_QCert</a> , <a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OE.SCD_Secrecy</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OE.SCD_Unique</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OE.SCD_SVD_Corresp</a>	<a href="#">P.CSP_QCert</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OE.Dev_Prov_Service</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OE.CGA_TC_SVD_Imp</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OE.CGA_SSCD_Auth</a>	<a href="#">P.CSP_QCert</a> , <a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>
<a href="#">OE.HID_TC_VAD_Exp</a>	<a href="#">P.Sig_Non-Repud</a>
<a href="#">OE.SCA_TC_DTBS_Exp</a>	<a href="#">P.Sig_Non-Repud</a>

<a href="#">OE.LinkSCD_QualifiedCertificate</a>	<a href="#">P.Sig_Non-Repud</a> , <a href="#">P.LinkSCD_QualifiedCertificate</a>
<a href="#">OE.AuthKey_Transfer</a>	<a href="#">P.EAC_Terminal</a>
<a href="#">OE.AuthKey_Unique</a>	<a href="#">P.EAC_Terminal</a>
<a href="#">OE.TOE_PublicKeyAuth_Transfer</a>	<a href="#">P.TOE_PublicAuthKey_Cert</a> , <a href="#">P.EAC_Terminal</a>
<a href="#">OE.Terminal_Authentication</a>	<a href="#">P.EAC_Terminal</a> , <a href="#">P.Terminal_PKI</a>
<a href="#">OE.Legislative_Compliance</a>	<a href="#">P.Pre-Operational</a>
<a href="#">OE.Passive_Auth_Sign</a>	<a href="#">P.Card_PKI</a> , <a href="#">P.Trustworthy_PKI</a>
<a href="#">OE.Personalization</a>	<a href="#">P.Pre-Operational</a>
<a href="#">OE.Terminal</a>	<a href="#">P.EAC_Terminal</a> , <a href="#">P.Terminal</a>
<a href="#">OE.Electronic_Document_Holder</a>	

**Table 19 Security Objectives and OSPs - Coverage**

<b>Assumptions</b>	<b>Security Objectives for the Operational Environment</b>	<b>Rationale</b>
<a href="#">A.CGA</a>	<a href="#">OE.CGA_QCert</a> , <a href="#">OE.SVD_Auth</a>	<a href="#">Section 7.3.3</a>
<a href="#">A.SCA</a>	<a href="#">OE.DTBS_Intend</a>	<a href="#">Section 7.3.3</a>
<a href="#">A.CSP</a>	<a href="#">OE.SCD/SVD_Auth_Gen</a> , <a href="#">OE.SCD_Secrecy</a> , <a href="#">OE.SCD_Unique</a> , <a href="#">OE.SCD_SVD_Corresp</a>	<a href="#">Section 7.3.3</a>

**Table 20 Assumptions and Security Objectives for the Operational Environment - Coverage**

<b>Security Objectives for the Operational Environment</b>	<b>Assumptions</b>
<a href="#">OE.SVD_Auth</a>	<a href="#">A.CGA</a>
<a href="#">OE.CGA_QCert</a>	<a href="#">A.CGA</a>
<a href="#">OE.DTBS_Intend</a>	<a href="#">A.SCA</a>
<a href="#">OE.Signatory</a>	
<a href="#">OE.HID_VAD</a>	
<a href="#">OE.DTBS_Protect</a>	
<a href="#">OE.SSCD_Prov_Service</a>	
<a href="#">OE.SCD/SVD_Auth_Gen</a>	<a href="#">A.CSP</a>
<a href="#">OE.SCD_Secrecy</a>	<a href="#">A.CSP</a>
<a href="#">OE.SCD_Unique</a>	<a href="#">A.CSP</a>
<a href="#">OE.SCD_SVD_Corresp</a>	<a href="#">A.CSP</a>
<a href="#">OE.Dev_Prov_Service</a>	

<a href="#">OE.CGA_TC_SVD_Imp</a>	
<a href="#">OE.CGA_SSCD_Auth</a>	
<a href="#">OE.HID_TC_VAD_Exp</a>	
<a href="#">OE.SCA_TC_DTBS_Exp</a>	
<a href="#">OE.LinkSCD_QualifiedCertificate</a>	
<a href="#">OE.AuthKey_Transfer</a>	
<a href="#">OE.AuthKey_Unique</a>	
<a href="#">OE.TOE_PublicKeyAuth_Transfer</a>	
<a href="#">OE.Terminal_Authentication</a>	
<a href="#">OE.Legislative_Compliance</a>	
<a href="#">OE.Passive_Auth_Sign</a>	
<a href="#">OE.Personalization</a>	
<a href="#">OE.Terminal</a>	
<a href="#">OE.Electronic_Document_Holder</a>	

**Table 21 Security Objectives for the Operational Environment and Assumptions - Coverage**

## 8 Extended Requirements

---

### 8.1 Extended Families

#### 8.1.1 Extended Family FPT\_EMS - TOE Emanation

##### 8.1.1.1 Description

The additional family FPT\_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT\_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation.

##### 8.1.1.2 Extended Components

###### Extended Component FPT\_EMS.1

Family behavior:

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT\_EMS.1 TOE Emanation has two constituents:

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

Management: FPT\_EMS.1

There are no management activities foreseen.

Audit: FPT\_EMS.1

There are no actions identified that shall be auditable if **FAU\_GEN** (*Security audit data generation*) is included in a PP or ST using FPT\_EMS.1.

*Definition*

**FPT\_EMS.1 TOE Emanation**

**FPT\_EMS.1.1** The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

**FPT\_EMS.1.2** The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

Hierarchical to: No other components.

Dependencies: No dependencies.

**8.1.2 Extended Family FMT\_LIM - Limited capabilities**

**8.1.2.1 Description**

The family FMT\_LIM describes the functional requirements for the test features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing abuse of functions by limiting the capabilities of the functions and by limiting their availability.

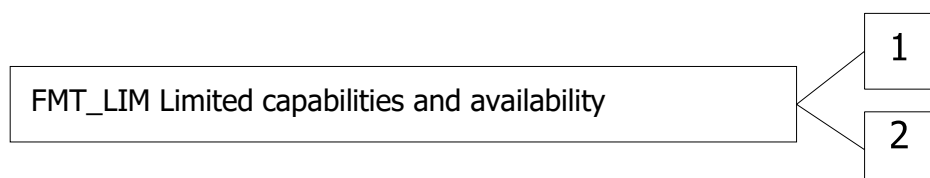
**8.1.2.2 Extended Components**

**Extended Component FMT LIM.1**

Family behavior:

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note, that FDP\_ACF restricts access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component levelling:



**FMT\_LIM.1** Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.



FMT\_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT\_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.

Management: FMT\_LIM.1, FMT\_LIM.2  
There are no management activities foreseen.

Audit: FMT\_LIM.1, FMT\_LIM.2  
There are no actions defined to be auditable.

*Definition*

**FMT\_LIM.1 Limited capabilities**

**FMT\_LIM.1.1** The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT\_LIM.2)' the following policy is enforced [assignment: Limited capability and availability policy]

Hierarchical to: No other components

Dependencies: FMT\_LIM.2 Limited availability.

**Extended Component FMT LIM.2**

*Definition*

**FMT\_LIM.2 Limited availability**

**FMT\_LIM.2.1** The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT\_LIM.1)' the following policy is enforced [assignment: Limited capability and availability policy]

Hierarchical to: No other components

Dependencies: FMT\_LIM.1 Limited availability.

**8.1.3 Extended Family FIA\_API - Authentication Proof of Identity**

**8.1.3.1 Description**

To describe the IT security functional requirements of the TOE a sensitive family (FIA\_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification

by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

**Application note 10:** The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA\_API in the style of the Common Criteria part 2 (cf. [3], chapter 'Explicitly stated IT security requirements (APE\_SRE)') from a TOE point of view.

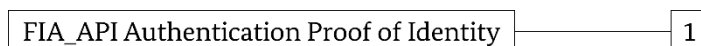
### 8.1.3.2 Extended Components

#### Extended Component FIA\_API.1

Family behavior:

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

Component levelling:



Management FIA\_API.1

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

Audit:

FIA\_API.1

There are no actions defined to be auditable.

*Definition*

#### **FIA\_API.1 Authentication Proof of Identity**

**FIA\_API.1.1** The TSF shall provide a [assignment: *authentication mechanism* ] to prove the identity of the [assignment: *authorized user or role* ].

Hierarchical to: No other components

Dependencies: No dependencies.

### 8.1.4 Extended Family FCS\_RND - Generation of random numbers

#### 8.1.4.1 Description

This family defines quality requirements for the generation of random numbers intended to be used for cryptographic purposes.

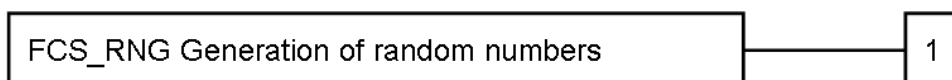
#### 8.1.4.2 Extended Components

##### Extended Component FCS\_RND.1

Family behavior:

This family defines requirements for the generation random number where the random numbers are intended to be used for cryptographic purposes.

Component levelling:



Management: FCS\_RND.1

There are no management activities foreseen.

Audit: FCS\_RND.1

There are no actions defined to be auditable.

*Definition*

##### **FCS\_RND.1 Quality metric for random numbers**

**FCS\_RND.1.1** The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric* ].

Hierarchical to: No other components.

Dependencies: No dependencies.

## 9 Security Requirements

---

### 9.1 Security Functional Requirements

This section describes the requirements imposed on the TOE in order to achieve the security objectives laid down in the previous chapter. In some of the functional requirements below, the [Editorially Refined] tag has been used to signify a small change in the requirement, to adhere to proper English grammar, or to make it more understandable to the reader.

#### 9.1.1 Security Attributes

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

Subject or object the security attribute is associated with	Security Attribute type	Value of the security attribute
S.User	Role	R.Admin, R.Sigy
S.User	SCD/SVD Management	Authorized, Not authorized
SCD	SCD Operational	Yes, No
SCD	SCD Identifier	Arbitrary value

##### 9.1.1.1 SCD/SVD Management

###### In phase 6

S.Admin is the personalization agent, and as such always has the attribute "SCD/SVD Management" set to "Authorized". Furthermore in that phase, the TOE allows the SCD to be imported or generated.

###### In phase 7

In this phase, the TOE only supports SCD/SVD generation. The access condition for SCD/SVD generation is granted if the User is successfully authenticated as S.Admin. If this condition is fulfilled, the attribute "SCD/SVD management" is set to "authorized", otherwise it is set to "not authorized".

##### 9.1.1.2 SCD Operational

###### In phase 6

The attribute "SCD operational" is always set to "No".

###### In phase 7

The attribute "SCD operational" is set to "yes" as soon as the subject is authenticated as S.Signatory, using the RAD.

## 9.1.2 All SSCD parts

### 9.1.2.1 Protection of the TSF (FPT)

#### FPT\_EMS.1 TOE Emanation

**FPT\_EMS.1.1** The TOE shall not emit **side channel emissions** in excess of **limits specified by the state-of-the-art attacks on smart card IC** enabling access to **SCD** and **RAD**.

**FPT\_EMS.1.2** The TSF shall ensure **all users** are unable to use the following interface **external contact emanations** to gain access to **RAD** and **SCD**.

#### FPT\_FLS.1 Failure with preservation of secure state

**FPT\_FLS.1.1** The TSF shall preserve a secure state when the following types of failures occur:

- o **self-test according to FPT\_TST fails**
- o **security violation detected by [ST\_PTF] with FAU\_ARP.1.**

#### FPT\_PHP.1 Passive detection of physical attack

**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.

#### FPT\_PHP.3 Resistance to physical attack

**FPT\_PHP.3.1** The TSF shall resist **physical manipulation and physical probing** to the **TSF** by responding automatically such that the SFRs are always enforced.

### FPT\_TST.1 TSF testing

**FPT\_TST.1.1** The TSF shall run a suite of self tests **during initial start-up** to demonstrate the correct operation of **the TSF**.

**FPT\_TST.1.2** The TSF shall provide authorised users with the capability to verify the integrity of **TSF data**.

**FPT\_TST.1.3** The TSF shall provide authorised users with the capability to verify the integrity of **TSF**.

#### 9.1.2.2 Security management (FMT)

### FMT\_SMR.1 Security roles

**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.

### FMT\_SMF.1 Specification of Management Functions

**FMT\_SMF.1.1** The TSF shall be capable of performing the following management functions:

- **Creation and modification of RAD,**
- **Enabling the signature creation function,**
- **Modification of the security attribute SCD/SVD management, SCD operational,**
- **Change the default value of the security attribute SCD Identifier,**
- **SCD/SVD Generation,**
- **SCD import,**
- **Unblock of RAD,**
- **Initialisation, change, resume, and unblock of PIN and PUK,**
- **Erase of PIN and RAD,**
- **Reinitialisation of PIN,**
- **Create and Delete File in Use Phase.**

**FMT\_MOF.1 Management of security functions behaviour**

**FMT\_MOF.1.1** The TSF shall restrict the ability to **enable** the functions **signature creation function** to **R.Sigy**.

**FMT\_MSA.1/Admin Management of security attributes**

**FMT\_MSA.1.1/Admin** The TSF shall enforce the **SCD/SVD Generation SFP and SCD Import SFP** to restrict the ability to **modify** the security attributes **SCD/SVD management** to **R.Admin**.

**FMT\_MSA.1/Signatory Management of security attributes**

**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**.

**FMT\_MSA.2 Secure security attributes**

**FMT\_MSA.2.1** The TSF shall ensure that only secure values are accepted for

- o **SCD/SVD Management**
- o **SCD operational**.

**FMT\_MSA.3 Static attribute initialisation**

**FMT\_MSA.3.1** The TSF shall enforce the **SCD/SVD Generation SFP, SVD Transfer SFP, SCD Import SFP and 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 **authorized identified role** to specify alternative initial values to override the default values when an object or information is created.

*Application Note:*

The authorized identified roles are defined in the following table depending on the TOE lifecycle phase

<b>Security attribute</b>	<b>Phase</b>	<b>Authorized identified roles</b>
SCD/SVD Management	6&7	R.Admin

<b>FMT_MSA.4 Security attribute value inheritance</b>
---

**FMT\_MSA.4.1** The TSF shall use the following rules to set the value of security attributes:

- o **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**
- o **If S.Admin imports SCD while S.Sigy is not currently authenticated, the security attribute "SCD operational" of the SCD shall be set to "no" after import of the SCD as a single operation.**
- o **If S.Admin imports SCD while S.Sigy is currently authenticated, the security attribute "SCD operational" of the SCD shall be set to "yes" after import of the SCD as a single operation**

*Application Note:*

Third point doesn't apply as SCD import is only possible in phase 6 where the role R.Sigy doesn't exist

<b>FMT_MTD.1/Admin Management of TSF data</b>
---

**FMT\_MTD.1.1/Admin** The TSF shall restrict the ability to **[Operation]** the **[TSF Data]** to **Admin**

<b>Operation</b>	<b>TSF Data</b>
<b>Create</b>	<b>RAD, File in Use Phase</b>
<b>Modify</b>	<b>The Chip Authentication key parameters to be used during key generation in USE phase</b>
<b>Read</b>	<b>The Chip Authentication key parameters to be used during key generation in USE phase, Proof that a key has been on board generated</b>
<b>Delete</b>	<b>File in Use Phase</b>
<b>Invalidate</b>	<b>Invalidate one of the Chip Authentication key in USE phase or set the secondary key as being the primary key</b>



## FMT\_MTD.1/Signatory Management of TSF data

**FMT\_MTD.1.1/Signatory** The TSF shall restrict the ability to **modify and none** the **RAD** to **R.Sigy**.

*Application Note:*

This requirement applies only to the RAD belonging to S.Sigy.

### 9.1.2.3 Identification and authentication (FIA)

## FIA\_UID.1 Timing of identification

**FIA\_UID.1.1** The TSF shall allow

- o **self-test according to FPT\_TST.1,**
- o **establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP\_ITC.1/SVD,**
- o **establishing a trusted channel between the CSP and the TOE by means of TSF required by FTP\_ITC.1/SCD**

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.

## FIA\_AFL.1/RAD Authentication failure handling

**FIA\_AFL.1.1/RAD** The TSF shall detect when **an administrator configurable positive integer within 1 and 15** unsuccessful authentication attempts occur related to **consecutive failed authentication attempts**.

**FIA\_AFL.1.2/RAD** When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **block RAD**.

*Application Note:*

These SFRs apply to R.Sigy and R.Admin using the PUK to authenticate itself.

## FIA\_UAU.1 Timing of authentication

**FIA\_UAU.1.1** The TSF shall allow

- a) **self-test according to FPT\_TST.1,**

- b) **identification of the user by means of TSF required by FIA\_UID.1,**
- c) **establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP\_ITC.1/SVD**

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.

#### 9.1.2.4 User data protection (FDP)

##### **FDP\_SDI.2/DTBS Stored data integrity monitoring and action**

**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

- o **prohibit the use of the altered data**
- o **inform the S.Sigy about integrity error.**

*Application Note:*

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

##### **FDP\_SDI.2/Persistent Stored data integrity monitoring and action**

**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

- o **prohibit the use of the altered data**
- o **inform the S.Sigy about integrity error.**

*Application Note:*

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

- SCD
- RAD
- Keys

### FDP\_RIP.1 Subset residual information protection

**FDP\_RIP.1.1** The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **SCD, RAD, VAD, Keys, PIN, PUK, Session keys and related data.**

### FDP\_ACC.1/Signature\_Creation Subset access control

**FDP\_ACC.1.1/Signature\_Creation** The TSF shall enforce the **Signature Creation SFP** on

- o **subjects: S.User,**
- o **objects: DTBS/R, SCD,**
- o **operations: signature creation.**

### FDP\_ACF.1/Signature\_Creation Security attribute based access control

**FDP\_ACF.1.1/Signature\_Creation** The TSF shall enforce the **Signature Creation SFP** to objects based on the following:

- o **the user S.User is associated with the security attribute "Role" and**
- o **the SCD with the security attribute "SCD Operational".**

**FDP\_ACF.1.2/Signature\_Creation** 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 electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "yes".**

**FDP\_ACF.1.3/Signature\_Creation** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

**FDP\_ACF.1.4/Signature\_Creation** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **S.User is not allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no".**

#### 9.1.2.5 Cryptographic support (FCS)

**FCS\_COP.1/Sign Cryptographic operation**

**FCS\_COP.1.1/Sign** The TSF shall perform **Signature Computation** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key Size(s)]** that meet the following: **[Standard]**

Algorithms	Key size(s)	Standard
Signature Computation with Off-Card Hashing: RSA and ECDSA	RSA-1024, 1536, 2048, 3072 and 4096 bits with PKCS#1 v1.5 and PKCS#1-PSS EC-DSA over elliptic curves of size of 192, 224, 256, 320, 384, 512 and 521 bits SHA-1, 224, 256, 384 and 512	[PKCS#1], [ANSIX9.62]
Signature Computation with On-Card Hashing: ECDSA only	EC-DSA over elliptic curves of size of 192, 224, 256, 320, 384, 512 and 521 SHA-1, 256 and 384	[ANSIX9.62]

**FCS\_CKM.4 Cryptographic key destruction**

**FCS\_CKM.4.1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting the buffer containing the key with zero** that meets the following: **none**.

*Application Note:*

This SFR applies to all keys, whether it is the SCD, the SVD or another one. The cryptographic key SCD will be destroyed before the SCD is re-imported or re-generated into the TOE.

**9.1.3 SSCD parts 2, 4 and 5 only**

**9.1.3.1 Cryptographic support (FCS)**

**FCS\_CKM.1/SCD/SVD\_Generation Cryptographic key generation**

**FCS\_CKM.1.1/SCD/SVD\_Generation [Editorially Refined]** The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm **[cryptographic key generation algorithm]** and specified cryptographic key sizes **[cryptographic key sizes]** that meet the following: **[list of standards]**

**The assignments of the cryptographic operations are described in the table below:**

key generation algorithm	key sizes	list of standards
Key pair over Elliptic Curve	Any elliptic curve from 192 bits up to 521 with prime field p	[IEEE]
RSA Key generation	1024, 1536, 2048, 3072 and 4096 bits	[ANSIX9.31]

### 9.1.3.2 User data protection (FDP)

#### FDP\_ACC.1/SVD\_Transfer Subset access control

**FDP\_ACC.1.1/SVD\_Transfer** The TSF shall enforce the **SVD Transfer SFP** on

- o **subjects: S.User;**
- o **objects: SVD;**
- o **operations: export.**

*Application Note:*

Note that here S.User can be either R.Sigy or R.Admin depending on the personalization done.

#### FDP\_ACF.1/SVD\_Transfer Security attribute based access control

**FDP\_ACF.1.1/SVD\_Transfer** The TSF shall enforce the **SVD Transfer SFP** to objects based on the following:

- o **the S.User is associated with the security attribute Role,**
- o **the SVD.**

**FDP\_ACF.1.2/SVD\_Transfer** 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.**

**FDP\_ACF.1.3/SVD\_Transfer** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

**FDP\_ACF.1.4/SVD\_Transfer** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none.**

*Application Note:*

For this operation, S.User is S.Admin.

In phase 6, S.Admin is the “personalization agent” and is always allowed to export the SVD.

In phase 7, S.Admin is the subject allowed to export the SVD.

#### **FDP\_ACC.1/SCD/SVD\_Generation Subset access control**

**FDP\_ACC.1.1/SCD/SVD\_Generation** The TSF shall enforce the **SCD/SVD Generation SFP** on

- o **subjects: S.User,**
- o **objects: SCD, SVD,**
- o **operations: generation of SCD/SVD pair.**

#### **FDP\_ACF.1/SCD/SVD\_Generation Security attribute based access control**

**FDP\_ACF.1.1/SCD/SVD\_Generation** 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** 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 "authorised" is allowed to generate SCD/SVD pair.**

**FDP\_ACF.1.3/SCD/SVD\_Generation** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

**FDP\_ACF.1.4/SCD/SVD\_Generation** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **S.User with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair.**

*Application Note:*

In phase 7, the S.user can become S.admin after authentication as S.Signatory combined with an Authentication Terminal (TA\_CMT) or Administration Terminal.

#### 9.1.4 *SSCD parts 3 and 6 only*

##### 9.1.4.1 Trusted path/channels (FTP)

###### **FTP\_ITC.1/SCD Inter-TSF trusted channel**

**FTP\_ITC.1.1/SCD** The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

**FTP\_ITC.1.2/SCD** The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

**FTP\_ITC.1.3/SCD** The TSF shall initiate communication via the trusted channel for

- o **Data exchange integrity according to FDP\_UCT.1/SCD**
- o **None.**

##### 9.1.4.2 User data protection (FDP)

###### **FDP\_UCT.1/SCD Basic data exchange confidentiality**

**FDP\_UCT.1.1/SCD [Editorially Refined]** The TSF shall enforce the **SCD Import SFP** to **receive SCD** in a manner protected from unauthorised disclosure.

###### **FDP\_ITC.1/SCD Import of user data without security attributes**

**FDP\_ITC.1.1/SCD** The TSF shall enforce the **SCD Import SFP** when importing user data, controlled under the SFP, from outside of the TOE.

**FDP\_ITC.1.2/SCD [Editorially Refined]** The TSF shall ignore any security attributes associated with the **SCD** when imported from outside the TOE.

**FDP\_ITC.1.3/SCD** The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **SCD shall be sent by an authorized CSP.**

*Application Note:*

This SFR only applies in phase 6.

The TOE interacts with a CSP through a SCD/SVD generation application to import the SCD. Authorized CSP is able to establish a trusted channel with the TOE for SCD transfer as required by FTP\_ITC.1.3/SCD.

The authorized CSP is the «Personalization Agent».

#### **FDP\_ACC.1/SCD\_Import Subset access control**

**FDP\_ACC.1.1/SCD\_Import** The TSF shall enforce the **SCD Import SFP** on

- o **subjects: S.User,**
- o **objects: SCD,**
- o **operations: import of SCD.**

#### **FDP\_ACF.1/SCD\_Import Security attribute based access control**

**FDP\_ACF.1.1/SCD\_Import** The TSF shall enforce the **SCD Import SFP** to objects based on the following: **the S.User is associated with the security attribute "SCD/SVD Management"**.

**FDP\_ACF.1.2/SCD\_Import** 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 "authorised" is allowed to import SCD.**

**FDP\_ACF.1.3/SCD\_Import** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

**FDP\_ACF.1.4/SCD\_Import** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **S.User with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to import SCD.**

*Application Note:*

For this operation, S.User is S.Admin.

In phase 6, S.Admin is the "Personalization Agent" and always has the security attribute "SCD/SVD Management" set to "authorized".

In phase 7, SCD import is not allowed.



### 9.1.5 SSCD part 4 only

#### 9.1.5.1 Trusted path/channels (FTP)

##### **FTP\_ITC.1/SVD Inter-TSF trusted channel**

**FTP\_ITC.1.1/SVD [Editorially Refined]** The TSF shall provide a communication channel between itself and another trusted IT product **CGA** that is logically distinct from other communication channels and provides ensured identification of its end points and protection of the channel data from modification or disclosure.

**FTP\_ITC.1.2/SVD** The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

**FTP\_ITC.1.3/SVD [Editorially Refined]** The TSF **or the CGA shall** initiate communication via the trusted channel for

- o **data Authentication with Identity of Guarantor according to FIA\_API.1 and FDP\_DAU.2/SVD**
- o **None.**

#### 9.1.5.2 User data protection (FDP)

##### **FDP\_DAU.2/SVD Data Authentication with Identity of Guarantor**

**FDP\_DAU.2.1/SVD** The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **SVD**.

**FDP\_DAU.2.2/SVD** The TSF shall provide **CGA** with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

#### 9.1.5.3 Identification and authentication (FIA)

##### **FIA\_API.1 Authentication Proof of Identity**

**FIA\_API.1.1** The TSF shall provide an **authentication mechanism** to prove the identity of the **SSCD**.

*Application Note:*

The authentication mechanism is achieved as follows:

- In phase 6: GP authentication

- In phase 6 & 7: an outgoing MAC

## 9.1.6 SSCD parts 5 and 6 only

### 9.1.6.1 User data protection (FDP)

#### FDP\_UIT.1/DTBS Data exchange integrity

**FDP\_UIT.1.1/DTBS** The TSF shall enforce the **Signature Creation SFP** to **receive** user data in a manner protected from **modification and insertion** errors.

**FDP\_UIT.1.2/DTBS** The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred.

### 9.1.6.2 Trusted path/channels (FTP)

#### FTP\_ITC.1/VAD Inter-TSF trusted channel

**FTP\_ITC.1.1/VAD [Editorially Refined]** The TSF shall provide a communication channel between itself and another trusted IT product **HID** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

**FTP\_ITC.1.2/VAD [Editorially Refined]** The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

**FTP\_ITC.1.3/VAD [Editorially Refined]** The TSF **or the HID** shall initiate communication via the trusted channel for:

- **User authentication according to FIA\_UAU.1**
- **Assignment: None**

#### FTP\_ITC.1/DTBS Inter-TSF trusted channel

**FTP\_ITC.1.1/DTBS [Editorially Refined]** The TSF shall provide a communication channel between itself and another trusted IT product **SCA** that is logically distinct from other

communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

**FTP\_ITC.1.2/DTBS [Editorially Refined]** The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

**FTP\_ITC.1.3/DTBS [Editorially Refined]** The TSF **or the SCA** shall initiate communication via the trusted channel for

- o **signature creation**
- o **Assignment: None.**

### 9.1.7 Additional SFRs

#### FCS\_RND.1 Quality metric for random numbers

**FCS\_RND.1.1** The TSF shall provide a mechanism to generate random numbers that meet **FCS\_RNG.1 Quality metric for random numbers of [ST\_PTF]**.

#### FCS\_CKM.1/DH\_PACE Cryptographic key generation

**FCS\_CKM.1.1/DH\_PACE** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[cryptographic key generation algorithm]** and specified cryptographic key sizes **[cryptographic key sizes]** that meet the following: **[standard]**

Cryptographic Key Generation Algorithm	Cryptographic Key Sizes	Standard
ECDH compliant to [ISO_15946]	192 bits to 521 bits	Based on ECDH protocol compliant to [TR-03111]

#### FCS\_CKM.1/Session Keys Cryptographic key generation

**FCS\_CKM.1.1/Session Keys [Editorially Refined]** The TSF shall generate session keys in accordance with a specified cryptographic key generation algorithm **key derivation function** and specified cryptographic key sizes

- o **DES keys of 112 bits**
- o **AES keys of 128, 192 and 256 bits**

that meet the following: **[TR-03110-3], [GP2.3], [SCP03]**.

## FCS\_COP.1/GP Secret Data Protection Cryptographic operation

**FCS\_COP.1.1/GP Secret Data Protection** The TSF shall perform **GP secret data encryption** in accordance with a specified cryptographic algorithm

- o **SCP02**
- o **SCP03 using AES**

and cryptographic key sizes

- o **128 bits**
- o **128, 192 and 256 bits**

that meet the following:

- o **[GP2.3]**
- o **[SCP03].**

*Application Note:*

The type of algorithm used by the TOE depends on the configuration set during the javacard open platform Personalization (For more details see [AGD\_PRE\_PLT]). The applet provides this service via the platform, it doesn't own and cannot access the keys used to protect secret data. Their import/generation and destruction are managed by the platform.

## FCS\_COP.1/SM in Confidentiality Cryptographic operation

**FCS\_COP.1.1/SM in Confidentiality** The TSF shall perform **Secure messaging in confidentiality** in accordance with a specified cryptographic algorithm

- o **Encryption with TDES EDE in CBC mode**
- o **Encryption with AES in CBC mode**

and cryptographic key sizes

- o **128 bits**
- o **128 bits, 192 bits and 256 bits**

that meet the following:

- o **[GP2.3] and [TR-03110-3]**
- o **[SCP03] and [TR-03110-3].**

*Application Note:*

This algorithm is used during secure Messaging to ensure confidentiality of incoming and outgoing data.

**FCS\_COP.1/SM in Integrity Cryptographic operation**

**FCS\_COP.1.1/SM in Integrity** The TSF shall perform **Secure messaging in integrity and authenticity** in accordance with a specified cryptographic algorithm

- o **Retail MAC: MAC algorithm 3 with padding method 2 and DES block Cipher**
- o **CMAC**

and cryptographic key sizes

- o **128 bits**
- o **128 bits, 192 bits and 256 bits**

that meet the following:

- o **[GP2.3] and, [TR-03110-3]**
- o **[SCP03] and [TR-03110-3].**

*Application Note:*

This algorithm is used during secure Messaging to ensure integrity and authenticity of incoming and outgoing data.

**FCS\_COP.1/Digital Auth Cryptographic operation**

**FCS\_COP.1.1/Digital Auth** The TSF shall perform **Digital Authentication** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key Size(s)]** that meet the following: **[Standard]**

Algorithm	Key Size(s)	Standard
<b>Digital authentication with Off-Card Hashing: RSA and ECDSA</b>	<b>RSA-1024, 1536, 2048, 3072 and 4096 bits with PKCS#1 v1.5 and PKCS#1-PSS EC-DNA over elliptic curves of size of-192, 224, 256, 320, 384, 512 and 521 bits SHA-1, 224, 256, 384 and 512</b>	<b>[PKCS#1], [ANSIX9.62]</b>
<b>Digital authentication with On-Card Hashing: ECDSA only</b>	<b>EC-DNA over elliptic curves of size of 192, 224, 256, 320, 384, 512 and 521 SHA-1, 256 and 384</b>	<b>[ANSIX9.62]</b>

**FCS\_COP.1/Enc Key Decipherment Cryptographic operation**

**FCS\_COP.1.1/Enc Key Decipherment** The TSF shall perform **Encryption Key Decipherment** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key Size(s)]** that meet the following: **[Standard]**

Algorithm	Key Size(s)	Standard
Encryption key decipherment: RSA	RSA-1024, 1536, 2048, 3072 and 4096 bits with PKCS#1 OAEP, using SHA-1, 224, 256, 384 and 512	[PKCS#1]
Encryption key decipherment: EC-DH	EC-DH over elliptic curves of size of 192, 224, 256, 320, 384, 512 and 521, using SHA-1, 224, 256, 384 and 512	[ANSIX9.62]

**FCS\_COP.1/SIG\_VER Cryptographic operation**

**FCS\_COP.1.1/SIG\_VER** The TSF shall perform **digital signature verification** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key Size(s)]** that meet the following: **[Standard]**

Algorithm	Key Size(s)	Standard
EC-DSA with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	Elliptic curves of size of 192 to 512 bits	[TR-03110-3]
RSA PKCS#1 v1.5 & v2.1 PSS with SHA-1, SHA-256,SHA-512	1024, 1536, 2048, 3072 and 4096 bits	[TR-03110-3]

**FDP\_ACC.1/TRM Subset access control**

**FDP\_ACC.1.1/TRM** The TSF shall enforce the **Access Control SFP** on **terminals gaining access User data stored in the TOE (including sensitive user data)**.

**FDP\_ACF.1/TRM Security attribute based access control**

**FDP\_ACF.1.1/TRM** The TSF shall enforce the **the Access Control SFP** to objects based on the following:

- o **Subjects: Terminal, BAT, Authentication Terminal.**
- o **Objects: User data stored in the TOE (including sensitive user data),**

- o **Security attributes: Terminal Authorization.**

**FDP\_ACF.1.2/TRM** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- o **A BAT is allowed to read data objects (except sensitive user data) specified in FDP\_ACF.1.1/TRM after successful authentication, as required by FIA\_UAU.1/PACE.**
- o **Reading, modifying, writing, or using sensitive user data protected by CAV1 and TAV1 (objects specified in FDP\_ACF.1.1/TRM) is only allowed to Authentication Terminals using the following mechanism: The TOE applies the EAC protocol (cf. FIA\_UAU.5) to determine effective authorizations of the terminal. To determine the effective authorization of a terminal, the chip must calculate a bitwise Boolean 'and' of the relative authorization contained in the CHAT of the Terminal Certificate, the referenced eService certification authority Certificate. Based on the terminal type drawn from the CHAT of the Terminal Certificate, the TOE shall grant the right to read, modify or write sensitive user data, or perform operations using these sensitive user data.**

**FDP\_ACF.1.3/TRM** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

**FDP\_ACF.1.4/TRM** The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- o **Any terminal not being a BAT or an Authentication Terminal is not allowed to read, to write, to modify, or to use any user data specified in FDP\_ACF.1.1/TRM.**
- o **In contactless, terminals not using secure messaging are not allowed to read, write, modify, or use any user data specified in FDP\_ACF.1.1/TRM.**

#### **FDP\_ACC.1/MNG\_File Subset access control**

**FDP\_ACC.1.1/MNG\_File** The TSF shall enforce the **Create and Delete\_FILE access Control SFP** on **administrator gaining access to create and delete EF file(s).**

#### **FDP\_ACF.1/MNG\_File Security attribute based access control**

**FDP\_ACF.1.1/MNG\_File** The TSF shall enforce the **the Access Control SFP** to objects based on the following:

- o **Subjects: Administrator**
- o **Objects: EF Files**
- o **Security attributes: Create File or Delete File ADMIN Access condition.**

**FDP\_ACF.1.2/MNG\_File** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- o **The Administrator successfully authenticated following FDP\_ACC.1/MNG\_File can create or delete any transparent EF under any ADF whose Create File or Delete File access condition is set to ADMIN.**

**FDP\_ACF.1.3/MNG\_File** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

**FDP\_ACF.1.4/MNG\_File** The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- o **Any subject not being authenticated as Administrator is not allowed:**
  - **To Create RAD,**
  - **Configure the size or value of the Chip Authentication key to be modified in USE phase,**
  - **Read that Proof that a key has been on board generated,**
  - **Create or Delete Files in Use Phase or**
  - **Invalidate one of the Chip Authentication key in USE phase.**

#### **FDP\_UCT.1/TRM Basic data exchange confidentiality**

**FDP\_UCT.1.1/TRM** The TSF shall enforce the **Access Control SFP to receive and transmit** user data in a manner protected from unauthorised disclosure.

#### **FDP\_UIT.1/TRM Data exchange integrity**

**FDP\_UIT.1.1/TRM** The TSF shall enforce the **Access Control SFP to transmit and receive** user data in a manner protected from **modification, deletion, insertion and replay** errors.

**FDP\_UIT.1.2/TRM** The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred.

#### **FIA\_UID.1/PACE Timing of identification**

**FIA\_UID.1.1/PACE** The TSF shall allow

- o **to establish the communication channel**
- o **to carry out the PACE Protocol (PIN, PUK, MRZ or CAN) according to [TR-03110-2] and [TR-03110-3] and/or the VERIFY PIN command**
- o **to read the Initialization Data if it is not disable by TSF**



- o **to carry out the Chip Authentication Protocol v.1 according to [TR-03110-3]**
- o **to carry out the Terminal Authentication Protocol v.1 according to [TR-03110-3]**

on behalf of the user to be performed before the user is identified.

**FIA\_UID.1.2/PACE** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

#### **FIA\_UAU.1/PACE Timing of authentication**

**FIA\_UAU.1.1/PACE** The TSF shall allow

- o **to establish the communication channel**
- o **to carry out the PACE Protocol (PIN, PUK, MRZ or CAN) according to [TR-03110-2] and [TR-03110-3] and/or the VERIFY PIN command**
- o **to read the Initialization Data if it is not disable by TSF**
- o **to identify themselves by selection of the authentication key**
- o **to carry out the Chip Authentication Protocol v.1 according to [TR-03110-3]**
- o **to carry out the Terminal Authentication Protocol v.1 according to [TR-03110-3]**

on behalf of the user to be performed before the user is authenticated.

**FIA\_UAU.1.2/PACE** The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

#### **FIA\_UAU.4/PACE Single-use authentication mechanisms**

**FIA\_UAU.4.1/PACE** The TSF shall prevent reuse of authentication data related to

- o **PACE Protocol (PIN, PUK, MRZ or CAN) according to [TR-03110-2] and [TR-03110-3].**
- o **Authentication Mechanisms based on Triple-DES or AES**
- o **Terminal Authentication Protocol v.1 according to [TR-03110-3].**

*Application Note:*

The Authentication Mechanisms based on Triple-DES or AES is the authentication process performed in phases 5 and 6.

**FIA\_UAU.5/PACE Multiple authentication mechanisms**

**FIA\_UAU.5.1/PACE** The TSF shall provide

- **PACE Protocol (PIN, PUK, MRZ or CAN) according to [TR-03110-2] and [TR-03110-3] and/or VERIFY PIN command**
- **Mean to verify the integrity and authenticity of the Chip authentication public key**
- **Secure messaging in MAC-ENC mode according to [TR-03110-3]**
- **Symmetric Authentication Mechanism based on Triple-DES or AES**
- **Terminal Authentication Protocol v.1 according to [TR-03110-3]**

to support user authentication.

**FIA\_UAU.5.2/PACE** The TSF shall authenticate any user's claimed identity according to the following rules:

- **Having successfully run the PACE protocol (PIN, PUK, MRZ or CAN), the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol.**
- **The establishment of the secure messaging with the PACE protocol is not mandatory in contact mode unless compliance to PP-SSCD5 and/or PP-SSCD6 is required, then establishment of the secure messaging with the PACE protocol becomes mandatory in both contact and contactless mode.**
- **The TOE accepts the authentication attempt as Personalization Agent by the Authentication Mechanism with Personalization Agent Key(s).**
- **After run of the Chip Authentication Protocol Version 1, the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1.**
- **The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1**
- **The TOE accepts the authentication attempt as Administrator by the Authentication Mechanism with Administrator Key(s).**

**FIA\_UAU.6/PACE Re-authenticating**

**FIA\_UAU.6.1/PACE** The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the BAT.**

**FIA\_UAU.6/EAC Re-authenticating**

**FIA\_UAU.6.1/EAC** The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful run of the Chip Authentication Protocol Version 1 shall be verified as being sent by the Inspection System.**

**FIA\_AFL.1/AUTH Authentication failure handling**

**FIA\_AFL.1.1/AUTH** The TSF shall detect when **[selection]** unsuccessful authentication attempts occur related to **[list of authentication events]**.

**FIA\_AFL.1.2/AUTH** When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **[list of actions]**

<b>Selection</b>	<b>List of Authentication Events</b>	<b>List of Actions</b>
<b>Positive integer number set to 0x0A</b>	<b>Authentication attempt involving MRZ or CAN as shared password for PACE</b>	<b>Wait for an increasing time between receiving of the terminal challenge and sending of the TSF response during the PACE authentication attempts</b>
<b>An administrator configurable positive integer linked to the PIN or PUK (respectively)</b>	<b>Consecutive failed authentication attempts using the PIN or PUK leaving a single authentication attempt</b>	<b>Suspend the PIN or the PUK</b>
<b>'1'</b>	<b>Consecutive failed authentication attempts using the suspended PIN or PUK</b>	<b>Block the PIN or the PUK</b>
<b>'1'</b>	<b>Personalization agent authentication attempt</b>	<b>slow down exponentially the next authentication</b>

**FIA\_API.1/TOE Authentication Authentication Proof of Identity**

**FIA\_API.1.1/TOE Authentication** The TSF shall provide an **authentication mechanism** to prove the identity of the **document holder**.

*Application Note:*

The TOE acts as a substitute for the Document holder, to authenticate digitally on its behalf. The authentication mechanism is triggered by the Document holder itself by presenting its PIN to the TOE.

#### FMT\_SMR.1/PACE Security roles

**FMT\_SMR.1.1/PACE** The TSF shall maintain the roles

- **Personalization Agent,**
- **Terminal,**
- **BAT,**
- **Country Verifying Certification Authority,**
- **eService certification authority,**
- **Authentication Terminal,**
- **Document holder.**

**FMT\_SMR.1.2/PACE** The TSF shall be able to associate users with roles.

#### FMT\_MTD.1/CVCA\_INI Management of TSF data

**FMT\_MTD.1.1/CVCA\_INI** The TSF shall restrict the ability to **write** the

- **initial Country Verifying Certification Authority Public Key,**
- **initial Country Verifying Certification Authority Certificate,**
- **initial Current Date**

to **the personalization agent.**

#### FMT\_MTD.1/CVCA\_UPD Management of TSF data

**FMT\_MTD.1.1/CVCA\_UPD** The TSF shall restrict the ability to **update** the

- **Country Verifying Certification Authority Public Key,**
- **Country Verifying Certification Authority Certificate,**

to **Country Verifying Certification Authority.**

#### FMT\_MTD.1/DATE Management of TSF data

**FMT\_MTD.1.1/DATE** The TSF shall restrict the ability to **modify** the **current date** to

- **Country Verifying Certification Authority,**
- **eService certification authority,**

- **Authentication Terminal.**

#### **FMT\_MTD.1/CAPK Management of TSF data**

**FMT\_MTD.1.1/CAPK** The TSF shall restrict the ability to **load or generate** the **Chip Authentication Private Key selected in Access Control SFP** to the **Personalization Agent**.

#### **FMT\_MTD.1/KEY\_READ Management of TSF data**

**FMT\_MTD.1.1/KEY\_READ** The TSF shall restrict the ability to **read** the

- **PACE passwords,**
- **Personalization Agent Keys,**
- **Chip Authentication Private Key,**
- **Administrator Key(s)**

to **none**.

#### **FMT\_MTD.1/Key\_Usage\_Counter Management of TSF data**

**FMT\_MTD.1.1/Key\_Usage\_Counter** The TSF shall restrict the ability to **configure** the **Key Usage Counter** to **Personalization Agent**.

#### **FMT\_MTD.1/Initialize\_PIN Management of TSF data**

**FMT\_MTD.1.1/Initialize\_PIN** The TSF shall restrict the ability to **write** the **PIN, PUK, MRZ and CAN, selected in Access Control SFP** to the **personalization agent**.

#### **FMT\_MTD.1/Resume\_PIN Management of TSF data**

**FMT\_MTD.1.1/Resume\_PIN** The TSF shall restrict the ability to **resume** the **suspended PIN or PUK selected in Access Control SFP** to the **electronic document presenter**.

**FMT\_MTD.1/Change\_PIN Management of TSF data**

**FMT\_MTD.1.1/Change\_PIN** The TSF shall restrict the ability to **change** the **PIN** selected in **Access Control SFP** to **the document holder (using the PUK for unblocking)**.

**FMT\_MTD.1/Unblock\_PIN Management of TSF data**

**FMT\_MTD.1.1/Unblock\_PIN** The TSF shall restrict the ability to **unblock** the **PIN** selected in **Access Control SFP** to **the document holder (using the PUK for unblocking)**.

**FMT\_MTD.1/UnblockChange\_RAD Management of TSF data**

**FMT\_MTD.1.1/UnblockChange\_RAD** The TSF shall restrict the ability to **unblock and optionally change** the **RAD** selected in **Access Control SFP** to

- **If change is required, the document holder (using the PUK for unblocking) and an Authentication Terminal (TA\_PMT) or Administration Terminal in accordance with FMT\_MTD.1/Signatory;**
- **Otherwise if only unblock is required, the document holder (using the PUK for unblocking).**

**FMT\_MTD.1/Eraser\_PIN Management of TSF data**

**FMT\_MTD.1.1/Eraser\_PIN** The TSF shall restrict the ability to **erase** the **PIN or RAD** selected in **Access Control SFP** to **an Authentication Terminal (TA\_PMT) or Administration Terminal**.

**FMT\_MTD.1/Reinitialize\_PIN Management of TSF data**

**FMT\_MTD.1.1/Reinitialize\_PIN** The TSF shall restrict the ability to **(re)initialize** the **PIN** selected in **Access Control SFP** to **the document holder (using the PUK)**.

**FMT\_MTD.1/UnblockChange\_PUK Management of TSF data**

**FMT\_MTD.1.1/UnblockChange\_PUK** The TSF shall restrict the ability to **unblock and change** the **PUK** selected in **Access Control SFP** to **an Authentication Terminal (TA\_PMT) or Administration Terminal**.

#### **FMT\_MTD.1/TOE State Management of TSF data**

**FMT\_MTD.1.1/TOE State** The TSF shall restrict the ability to **switch** the **TOE from phase 6 to phase 7** to **personalization agent**.

#### **FMT\_MTD.3 Secure TSF data**

**FMT\_MTD.3.1** The TSF shall ensure that only secure values are accepted for **TSF data of the Terminal Authentication Protocol v1 and the Access Control SFP**.

#### **FMT\_MTD.1/INI\_ENA Management of TSF data**

**FMT\_MTD.1.1/INI\_ENA** The TSF shall restrict the ability to **write** the **Initialisation Data and the Pre-personalisation Data** to **the Manufacturer**.

#### **FMT\_MTD.1/INI\_DIS Management of TSF data**

**FMT\_MTD.1.1/INI\_DIS** The TSF shall restrict the ability to **read out** the **Initialisation Data and the Pre-personalisation Data** to **the Personalisation Agent**.

#### **FMT\_LIM.1 Limited capabilities**

**FMT\_LIM.1.1** The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT\_LIM.2)' the following policy is enforced **Deploying Test Features after TOE Delivery does not allow**

- **User Data to be disclosed and manipulated,**
- **TSF data to be disclosed or manipulated,**
- **software to be reconstructed and,**
- **substantial information about construction of TSF to be gathered which may enable other attacks**

#### **FMT\_LIM.2 Limited availability**

**FMT\_LIM.2.1** The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT\_LIM.1)' the following policy is enforced **Deploying Test Features after TOE Delivery does not allow**

- **User Data to be disclosed and manipulated,**

- o **TSF data to be disclosed or manipulated,**
- o **software to be reconstructed and,**
- o **substantial information about construction of TSF to be gathered which may enable other attacks**

#### **FPT\_EMS.1/PIN-PUK-KEYS TOE Emanation**

**FPT\_EMS.1.1/PIN-PUK-KEYS** The TOE shall not emit **side channel emission** in excess of **limits specified by the state of the art attacks on smart card IC** enabling access to **PIN, PUK, Keys** and **none**.

**FPT\_EMS.1.2/PIN-PUK-KEYS** The TSF shall ensure **all users** are unable to use the following interface **external contacts emanations** to gain access to **PIN, PUK, Keys** and **none**.

#### **FTP\_ITC.1/PACE Inter-TSF trusted channel**

**FTP\_ITC.1.1/PACE [Editorially Refined]** The TSF shall provide a communication channel between itself and a **BAT** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. **The trusted channel shall be established by performing the PACE protocol according to [TR-03110-3].**

**FTP\_ITC.1.2/PACE [Editorially Refined]** The TSF shall permit **the BAT** to initiate communication via the trusted channel.

**FTP\_ITC.1.3/PACE** The TSF shall initiate communication via the trusted channel for **any data exchange between the TOE and a BAT after PACE.**



## 9.2 Security Assurance Requirements

The Evaluation Assurance Level is EAL5 augmented with AVA\_VAN.5, ALC\_FLR.1 and ALC\_DVS.2.

### 9.2.1 ADV Development

#### 9.2.1.1 ADV\_ARC Security Architecture

<b>ADV_ARC.1 Security architecture description</b>
--

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

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

**ADV\_ARC.1.3D** The developer shall provide a security architecture description of the TSF.

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

**ADV\_ARC.1.2C** The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

**ADV\_ARC.1.3C** The security architecture description shall describe how the TSF initialisation process is secure.

**ADV\_ARC.1.4C** The security architecture description shall demonstrate that the TSF protects itself from tampering.

**ADV\_ARC.1.5C** The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

**ADV\_ARC.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 9.2.1.2 ADV\_FSP Functional specification

**ADV\_FSP.5 Complete semi-formal functional specification with additional error information**

**ADV\_FSP.5.1D** The developer shall provide a functional specification.

**ADV\_FSP.5.2D** The developer shall provide a tracing from the functional specification to the SFRs.

**ADV\_FSP.5.1C** The functional specification shall completely represent the TSF.

**ADV\_FSP.5.2C** The functional specification shall describe the TSFI using a semi-formal style.

**ADV\_FSP.5.3C** The functional specification shall describe the purpose and method of use for all TSFI.

**ADV\_FSP.5.4C** The functional specification shall identify and describe all parameters associated with each TSFI.

**ADV\_FSP.5.5C** The functional specification shall describe all actions associated with each TSFI.

**ADV\_FSP.5.6C** The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

**ADV\_FSP.5.7C** The functional specification shall describe all error messages that do not result from an invocation of a TSFI.

**ADV\_FSP.5.8C** The functional specification shall provide a rationale for each error message contained in the TSF implementation yet does not result from an invocation of a TSFI.

**ADV\_FSP.5.9C** The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

**ADV\_FSP.5.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ADV\_FSP.5.2E** The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

**9.2.1.3 ADV\_IMP Implementation representation**

**ADV\_IMP.1 Implementation representation of the TSF**

**ADV\_IMP.1.1D** The developer shall make available the implementation representation for the entire TSF.

**ADV\_IMP.1.2D** The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

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

**ADV\_IMP.1.2C** The implementation representation shall be in the form used by the development personnel.

**ADV\_IMP.1.3C** The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

**ADV\_IMP.1.1E** The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

**9.2.1.4 ADV\_TDS TOE design**

## **ADV\_TDS.4 Semiformal modular design**

**ADV\_TDS.4.1D** The developer shall provide the design of the TOE.

**ADV\_TDS.4.2D** The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

**ADV\_TDS.4.1C** The design shall describe the structure of the TOE in terms of subsystems.

**ADV\_TDS.4.2C** The design shall describe the TSF in terms of modules, designating each module as SFR-enforcing, SFR-supporting, or SFR-non-interfering.

**ADV\_TDS.4.3C** The design shall identify all subsystems of the TSF.

**ADV\_TDS.4.4C** The design shall provide a semiformal description of each subsystem of the TSF, supported by informal, explanatory text where appropriate.

**ADV\_TDS.4.5C** The design shall provide a description of the interactions among all subsystems of the TSF.

**ADV\_TDS.4.6C** The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

**ADV\_TDS.4.7C** The design shall describe each SFR-enforcing and SFR-supporting module in terms of its purpose and relationship with other modules.

**ADV\_TDS.4.8C** The design shall describe each SFR-enforcing and SFR-supporting module in terms of its SFR-related interfaces, return values from those interfaces, interaction with

other modules and called SFR-related interfaces to other SFR-enforcing or SFR-supporting modules.

**ADV\_TDS.4.9C** The design shall describe each SFR-non-interfering module in terms of its purpose and interaction with other modules.

**ADV\_TDS.4.10C** The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

**ADV\_TDS.4.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ADV\_TDS.4.2E** The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

#### 9.2.1.5 ADV\_INT TSF internals

<b>ADV_INT.2 Well-structured internals</b>
--

**ADV\_INT.2.1D** The developer shall design and implement the entire TSF such that it has well-structured internals.

**ADV\_INT.2.2D** The developer shall provide an internals description and justification.

**ADV\_INT.2.1C** The justification shall describe the characteristics used to judge the meaning of "well-structured".

**ADV\_INT.2.2C** The TSF internals description shall demonstrate that the entire TSF is well-structured.

**ADV\_INT.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ADV\_INT.2.2E** The evaluator shall perform an internals analysis on the TSF.

## 9.2.2 AGD Guidance documents

### 9.2.2.1 AGD\_OPE Operational user guidance

<b>AGD_OPE.1 Operational user guidance</b>
--

**AGD\_OPE.1.1D** The developer shall provide operational user guidance.

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

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

**AGD\_OPE.1.3C** The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

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

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

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

**AGD\_OPE.1.7C** The operational user guidance shall be clear and reasonable.

**AGD\_OPE.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 9.2.2.2 AGD\_PRE Preparative procedures

**AGD\_PRE.1 Preparative procedures**

**AGD\_PRE.1.1D** The developer shall provide the TOE including its preparative procedures.

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

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

**AGD\_PRE.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**AGD\_PRE.1.2E** The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

### **9.2.3 ALC Life-cycle support**

#### **9.2.3.1 ALC\_CMC CM capabilities**



**ALC\_CMC.4 Production support, acceptance procedures and automation**

**ALC\_CMC.4.1D** The developer shall provide the TOE and a reference for the TOE.

**ALC\_CMC.4.2D** The developer shall provide the CM documentation.

**ALC\_CMC.4.3D** The developer shall use a CM system.

**ALC\_CMC.4.1C** The TOE shall be labelled with its unique reference.

**ALC\_CMC.4.2C** The CM documentation shall describe the method used to uniquely identify the configuration items.

**ALC\_CMC.4.3C** The CM system shall uniquely identify all configuration items.

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

**ALC\_CMC.4.5C** The CM system shall support the production of the TOE by automated means.

**ALC\_CMC.4.6C** The CM documentation shall include a CM plan.

**ALC\_CMC.4.7C** The CM plan shall describe how the CM system is used for the development of the TOE.

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

**ALC\_CMC.4.9C** The evidence shall demonstrate that all configuration items are being maintained under the CM system.

**ALC\_CMC.4.10C** The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

**ALC\_CMC.4.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**9.2.3.2 ALC\_CMS CM scope**

### **ALC\_CMS.5 Development tools CM coverage**

**ALC\_CMS.5.1D** The developer shall provide a configuration list for the TOE.

**ALC\_CMS.5.1C** The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.

**ALC\_CMS.5.2C** The configuration list shall uniquely identify the configuration items.

**ALC\_CMS.5.3C** For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

**ALC\_CMS.5.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### **9.2.3.3 ALC\_DEL Delivery**

### **ALC\_DEL.1 Delivery procedures**

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

**ALC\_DEL.1.2D** The developer shall use the delivery procedures.

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

**ALC\_DEL.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### **9.2.3.4 ALC\_DVS Development security**

### **ALC\_DVS.2 Sufficiency of security measures**

**ALC\_DVS.2.1D** The developer shall produce and provide development security documentation.

**ALC\_DVS.2.1C** The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the

confidentiality and integrity of the TOE design and implementation in its development environment.

**ALC\_DVS.2.2C** The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

**ALC\_DVS.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ALC\_DVS.2.2E** The evaluator shall confirm that the security measures are being applied.

#### 9.2.3.5 ALC\_FLR Flaw remediation

##### **ALC\_FLR.1 Basic flaw remediation**

**ALC\_FLR.1.1D** The developer shall document and provide flaw remediation procedures addressed to TOE developers.

**ALC\_FLR.1.1C** The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

**ALC\_FLR.1.2C** The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

**ALC\_FLR.1.3C** The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

**ALC\_FLR.1.4C** The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective action to TOE users.

**ALC\_FLR.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 9.2.3.6 ALC\_LCD Life-cycle definition

### **ALC\_LCD.1 Developer defined life-cycle model**

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

**ALC\_LCD.1.2D** The developer shall provide life-cycle definition documentation.

**ALC\_LCD.1.1C** The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

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

**ALC\_LCD.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### **9.2.3.7 ALC\_TAT Tools and techniques**

### **ALC\_TAT.2 Compliance with implementation standards**

**ALC\_TAT.2.1D** The developer shall provide the documentation identifying each development tool being used for the TOE.

**ALC\_TAT.2.2D** The developer shall document and provide the selected implementation-dependent options of each development tool.

**ALC\_TAT.2.3D** The developer shall describe and provide the implementation standards that are being applied by the developer.

**ALC\_TAT.2.1C** Each development tool used for implementation shall be well-defined.

**ALC\_TAT.2.2C** The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

**ALC\_TAT.2.3C** The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

**ALC\_TAT.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ALC\_TAT.2.2E** The evaluator shall confirm that the implementation standards have been applied.

## **9.2.4 ASE Security Target evaluation**

### **9.2.4.1 ASE\_CCL Conformance claims**

## **ASE\_CCL.1 Conformance claims**

**ASE\_CCL.1.1D** The developer shall provide a conformance claim.

**ASE\_CCL.1.2D** The developer shall provide a conformance claim rationale.

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

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

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

**ASE\_CCL.1.4C** The CC conformance claim shall be consistent with the extended components definition.

**ASE\_CCL.1.5C** The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

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

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

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

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

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

**ASE\_CCL.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### **9.2.4.2 ASE\_ECD Extended components definition**

## **ASE\_ECD.1 Extended components definition**

**ASE\_ECD.1.1D** The developer shall provide a statement of security requirements.

**ASE\_ECD.1.2D** The developer shall provide an extended components definition.

**ASE\_ECD.1.1C** The statement of security requirements shall identify all extended security requirements.

**ASE\_ECD.1.2C** The extended components definition shall define an extended component for each extended security requirement.

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

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

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

**ASE\_ECD.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ASE\_ECD.1.2E** The evaluator shall confirm that no extended component can be clearly expressed using existing components.

### **9.2.4.3 ASE\_INT ST introduction**

## **ASE\_INT.1 ST introduction**

**ASE\_INT.1.1D** The developer shall provide an ST introduction.

**ASE\_INT.1.1C** The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

**ASE\_INT.1.2C** The ST reference shall uniquely identify the ST.

**ASE\_INT.1.3C** The TOE reference shall identify the TOE.

**ASE\_INT.1.4C** The TOE overview shall summarise the usage and major security features of the TOE.

**ASE\_INT.1.5C** The TOE overview shall identify the TOE type.

**ASE\_INT.1.6C** The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

**ASE\_INT.1.7C** The TOE description shall describe the physical scope of the TOE.

**ASE\_INT.1.8C** The TOE description shall describe the logical scope of the TOE.

**ASE\_INT.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ASE\_INT.1.2E** The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

### **9.2.4.4 ASE\_OBJ Security objectives**



## ASE\_OBJ.2 Security objectives

**ASE\_OBJ.2.1D** The developer shall provide a statement of security objectives.

**ASE\_OBJ.2.2D** The developer shall provide a security objectives rationale.

**ASE\_OBJ.2.1C** The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

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

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

**ASE\_OBJ.2.4C** The security objectives rationale shall demonstrate that the security objectives counter all threats.

**ASE\_OBJ.2.5C** The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

**ASE\_OBJ.2.6C** The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

**ASE\_OBJ.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 9.2.4.5 ASE\_REQ Security requirements

## **ASE\_REQ.2 Derived security requirements**

**ASE\_REQ.2.1D** The developer shall provide a statement of security requirements.

**ASE\_REQ.2.2D** The developer shall provide a security requirements rationale.

**ASE\_REQ.2.1C** The statement of security requirements shall describe the SFRs and the SARs.

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

**ASE\_REQ.2.3C** The statement of security requirements shall identify all operations on the security requirements.

**ASE\_REQ.2.4C** All operations shall be performed correctly.

**ASE\_REQ.2.5C** Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

**ASE\_REQ.2.6C** The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

**ASE\_REQ.2.7C** The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

**ASE\_REQ.2.8C** The security requirements rationale shall explain why the SARs were chosen.

**ASE\_REQ.2.9C** The statement of security requirements shall be internally consistent.

**ASE\_REQ.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### **9.2.4.6 ASE\_SPD Security problem definition**

### ASE\_SPD.1 Security problem definition

**ASE\_APD.1.1D** The developer shall provide a security problem definition.

**ASE\_SPD.1.1C** The security problem definition shall describe the threats.

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

**ASE\_SPD.1.3C** The security problem definition shall describe the OSPs.

**ASE\_SPD.1.4C** The security problem definition shall describe the assumptions about the operational environment of the TOE.

**ASE\_SPD.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 9.2.4.7 ASE\_TSS TOE summary specification

#### ASE\_TSS.1 TOE summary specification

**ASE\_TSS.1.1D** The developer shall provide a TOE summary specification.

**ASE\_TSS.1.1C** The TOE summary specification shall describe how the TOE meets each SFR.

**ASE\_TSS.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ASE\_TSS.1.2E** The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

## 9.2.5 ATE Tests

### 9.2.5.1 ATE\_COV Coverage

#### **ATE\_COV.2 Analysis of coverage**

**ATE\_COV.2.1D** The developer shall provide an analysis of the test coverage.

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

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

**ATE\_COV.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 9.2.5.2 ATE\_DPT Depth

#### **ATE\_DPT.3 Testing: modular design**

**ATE\_DPT.3.1D** The developer shall provide the analysis of the depth of testing.

**ATE\_DPT.3.1C** The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and modules in the TOE design.

**ATE\_DPT.3.2C** The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

**ATE\_DPT.3.3C** The analysis of the depth of testing shall demonstrate that all TSF modules in the TOE design have been tested.

**ATE\_DPT.3.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 9.2.5.3 ATE\_FUN Functional tests

## **ATE\_FUN.1 Functional testing**

**ATE\_FUN.1.1D** The developer shall test the TSF and document the results.

**ATE\_FUN.1.2D** The developer shall provide test documentation.

**ATE\_FUN.1.1C** The test documentation shall consist of test plans, expected test results and actual test results.

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

**ATE\_FUN.1.3C** The expected test results shall show the anticipated outputs from a successful execution of the tests.

**ATE\_FUN.1.4C** The actual test results shall be consistent with the expected test results.

**ATE\_FUN.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### **9.2.5.4 ATE\_IND Independent testing**

## **ATE\_IND.2 Independent testing - sample**

**ATE\_IND.2.1D** The developer shall provide the TOE for testing.

**ATE\_IND.2.1C** The TOE shall be suitable for testing.

**ATE\_IND.2.2C** The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

**ATE\_IND.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ATE\_IND.2.2E** The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

**ATE\_IND.2.3E** The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

## 9.2.6 AVA Vulnerability assessment

### 9.2.6.1 AVA\_VAN Vulnerability analysis

<b>AVA_VAN.5 Advanced methodical vulnerability analysis</b>
---

**AVA\_VAN.5.1D** The developer shall provide the TOE for testing.

**AVA\_VAN.5.1C** The TOE shall be suitable for testing.

**AVA\_VAN.5.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**AVA\_VAN.5.2E** The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

**AVA\_VAN.5.3E** The evaluator shall perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

**AVA\_VAN.5.4E** The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing High attack potential.

## 9.3 Security Requirements Rationale

### 9.3.1 Objectives

#### 9.3.1.1 Security Objectives for the TOE

##### All SSCD parts

**OT.Lifecycle\_Security** is provided by the SFR as follows. The SCD import is controlled by TSF according to FDP\_ACC.1/SCD\_Import, FDP\_ACF.1/SCD\_Import and FDP\_ITC.1/SCD. The confidentiality of the SCD is protected during import according to FDP\_UCT.1/SCD in the trusted channel FTP\_ITC.1/SCD. Secure SCD/SVD generation is ensured by FCS\_CKM.1/SCD/SVD\_Generation. The SCD/SVD generation is controlled by TSF according to FDP\_ACC.1/SCD/SVD\_Generation and FDP\_ACF.1/SCD/SVD\_Generation. The SVD transfer for certificate generation is controlled by TSF according to FDP\_ACC.1/SVD\_Transfer and FDP\_ACF.1/SVD\_Transfer. The secure SCD usage is ensured cryptographically according to FCS\_COP.1/Sign. The SCD usage is controlled by access control FDP\_ACC.1/Signature\_Creation, FDP\_ACF.1/Signature\_Creation, which is based on the security attribute secure TSF management according to 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/UnblockChange\_RAD, FMT\_MTD.1/Erase\_PIN, FMT\_SMF.1 and FMT\_SMR.1. The test functions FPT\_TST.1 provides failure detection throughout the lifecycle. The SFR FCS\_CKM.4, ensures a secure SCD destruction.

**OT.SCD\_Secrecy** is provided by the security functions specified by the following SFR. FDP\_UCT.1/SCD and FTP\_ITC.1/SCD ensures the confidentiality for SCD import. FCS\_CKM.1/SCD/SVD\_Generation ensures the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD. The security functions specified by FDP\_RIP.1 and FCS\_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information. The security functions specified by FDP\_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT\_TST.1 tests the working conditions of the TOE and FPT\_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT\_FLS.1 is fault injection for differential fault analysis (DFA). SFR FPT\_EMS.1 and FPT\_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

**OT.Sig\_Secure** is provided by the cryptographic algorithms specified by FCS\_COP.1/Sign, 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 ensures self-tests ensuring correct signature creation.

**OT.Sigy\_SigF** is provided by an SFR for identification authentication and access control. FIA\_UAU.1 and FIA\_UID.1 ensure that no signature creation function can be invoked before the signatory is identified and authenticated. The security functions specified by FMT\_MTD.1/Admin and FMT\_MTD.1/Signatory manage the authentication function. SFR FIA\_AFL.1/RAD 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. The security functions specified by FDP\_ACC.1/Signature\_Creation and FDP\_ACF.1/Signature\_Creation provide access control based on the security attributes managed according to the SFR FMT\_MTD.1/Signatory, FMT\_MSA.2, FMT\_MSA.3 and FMT\_MSA.4. The SFR FMT\_SMF.1 and FMT\_SMR.1 list these management functions and the roles. These ensure that the signature process is restricted to the signatory. FMT\_MOF.1 restricts the ability to enable the signature creation function to the signatory. FMT\_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory. Furthermore, FDP\_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature creation process) and ensures that no attacker can get hold of the SCD (to create signatures outside the TOE) once SCD has been deleted by the legitimate signatory. FMT\_MTD.1/Unblock\_PIN and FMT\_MTD.1/UnblockChange\_RAD ensure the unblocking of the PIN (including the RAD) is made under the sole control of the administrator. In phase 6, the RAD may be loaded on the TOE by the Personalization Agent as defined in FMT\_SMF.1. The Personalization Agent is authenticated with a mutual authentication performed with FCS\_RND.1 and FCS\_COP.1/GP, and is authenticated with FMT\_SMR.1. During the mutual authentication, a session encryption key is agreed between the TOE and the Personalization Agent and used by the TOE to decrypt the RAD using FCS\_COP.1/GP Secret Data Protection, ensuring the confidentiality of the RAD during its transfer in phase 6. In phase 6, FMT\_MSA.1/ Signatory



guarantees that the Personalization Agent cannot sign on behalf of the signatory, ensuring the signature creation features remains under the sole control of the signatory.

**OT.DTBS\_Integrity\_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** covers that no intelligible information is emanated. This is provided by FPT\_EMS.1.1 and FPT\_EMS.1/PIN-PUK-KEYS.

**OT.Tamper\_ID** is provided by FPT\_PHP.1 by the means of passive detection of physical attacks.

**OT.Tamper\_Resistance** is provided by FPT\_PHP.3 to resist physical attacks.

#### **SSCD parts 2, 4 and 5 only**

**OT.SCD/SVD\_Auth\_Gen** addresses that generation of a SCD/SVD pair requires proper user authentication. FIA\_UAU.1 and FIA\_UID.1 provide user identification and user authentication prior to enabling access to authorized functions. The SFR FDP\_ACC.1/SCD/SVD\_Generation and FDP\_ACF.1/SCD/SVD\_Generation provide access control for the SCD/SVD generation. The security attributes of the authenticated user are provided by FMT\_MSA.1/Admin, FMT\_MSA.2, and FMT\_MSA.3 for static attribute initialization. The SFR FMT\_MSA.4 defines rules for inheritance of the security attribute "SCD operational" of the SCD.

**OT.SCD\_Unique** implements the requirement of practically unique SCD as laid down in Annex III, paragraph 1(a), which is provided by the cryptographic algorithms specified by FCS\_CKM.1/SCD/SVD\_Generation.

**OT.SCD\_SVD\_Corresp** addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS\_CKM.1/SCD/SVD\_Generation to generate corresponding SVD/SCD pairs. The security functions specified by FDP\_SDI.2/Persistent ensure that the keys are not modified, so to retain the correspondence. Moreover, the SCD Identifier allows the environment to identify the SCD and to link it with the appropriate SVD. The management functions identified by FMT\_SMF.1 and by FMT\_MSA.4 allow R.Admin to modify the default value of the security attribute SCD Identifier.

#### **SSCD parts 3 and 6 only**

**OT.SCD\_Auth\_Imp** is provided by the security functions specified by the following SFR. FIA\_UID.1 and FIA\_UAU.1 ensure that the user is identified and authenticated before SCD

can be imported. FDP\_ACC.1/SCD\_Import and FDP\_ACF.1/SCD\_Import ensure that only authorised users can import SCD.

#### **SSCD part 4 only**

**OT.TOE\_SSCD\_Auth** requires the TOE to provide security mechanisms to identify and to authenticate themselves as SSCD, which is directly provided by FIA\_API.1 (Authentication proof of identity). The SFR FIA\_UAU.1 allows establishment of the trusted channel before (human) user is authenticated.

**OT.TOE\_TC\_SVD\_Exp** requires the TOE to provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA, which is directly provided by

- o The SVD transfer for certificate generation is controlled by TSF according to FDP\_ACC.1/SVD\_Transfer and FDP\_ACF.1/SVD\_Transfer
- o FDP\_DAU.2/SVD (Data authentication with identity of guarantor), which requires the TOE to provide CGA with the ability to verify evidence of the validity of the SVD and the identity of the user that generated the evidence.
- o FTP\_ITC.1/SVD (inter-TSF trusted channel), which requires the TOE to provide a trusted channel to the CGA.

#### **SSCD parts 5 and 6 only**

**OT.TOE\_TC\_VAD\_Imp** is provided by FTP\_ITC.1/VAD to provide a trusted channel to protect the VAD provided by the HID to the TOE.

**OT.TOE\_TC\_DTBS\_Imp** is provided by FTP\_ITC.1/DTBS to provide a trusted channel to protect the DTBS provided by the SCA to the TOE and by FDP\_UIT.1/DTBS, which requires the TSF to verify the integrity of the received DTBS.

#### **Additional Security Objectives for the TOE**

**OT.Identification** The security objective OT.Identification addresses the storage of Initialisation and Pre-Personalisation Data in its non-volatile memory, whereby they also include the IC Identification Data uniquely identifying the TOE's chip. The SFR FMT\_MTD.1/INI\_ENA allows only the Manufacturer to write Initialisation and Pre-personalisation Data (including the Personalisation Agent key). The SFR FMT\_MTD.1/INI\_DIS requires the Personalisation Agent to disable access to Initialisation and Pre-personalisation Data in the life cycle phase 'operational use'. The SFRs FMT\_SMF.1 and FMT\_SMR.1/PACE support the functions and the roles related.

**OT.Authentication\_Secure** is provided by FCS\_RND.1 and FCS\_COP.1/GP for the authentication of the Personalization agent. The use of a challenge freshly generated by the TOE with FCS\_RND.1 in these authentication protocols ensures a protection against replay attacks when authenticating external entities. The security function specified by FPT\_TST.1 ensures that the security functions are performed correctly and FDP\_SDI.2/Persistent guarantees the integrity of the authentication key(s) used by the

TOE. FMT\_SMR.1 and FMT\_SMF.1 ensure the TOE can distinguish between external entities successfully authenticated (R.Admin) and can grant them dedicated rights. In case of authentication protocols involving the import of ephemeral public key on the TOE (using Card verifiable certificates), FDP\_RIP.1 ensures that the key value is not kept by the TOE after usage and then can not be reused for a replay attack. This objective ensures as well the establishment of a trusted channel following a successful mutual authentication. This trusted channel ensures authenticity, integrity and confidentiality of communication. FCS\_CKM.1/Session Keys generate session keys for the secure communication from a common secret agreed between the TOE and the external entity during the mutual authentication procedure. Any incoming command shall contain a MAC computed by the issuer with the session key agreed during the mutual authentication, so that any unauthenticated or non integer command is detected by the MAC verification performed by the TOE using FCS\_COP.1/SM in Integrity. The data exchanged through this trusted channel are also protected in confidentiality thanks to FCS\_COP.1/SM in Confidentiality, ensuring they can only be disclosed to the parties authenticated during the mutual authentication step. The encryption key is ephemeral as it is generated during the mutual authentication using a challenge freshly generated by the TOE using FCS\_RND.1, which ensures that dictionary attacks cannot be performed on encrypted data. When an integrity error is detected, or if the MAC is wrong (wrong authentication of the command issuer), the session keys (for integrity and confidentiality) are erased thanks to FCS\_CKM.4 so that they cannot be reused anymore, causing the trusted channel to be irreversibly lost. In particular, it ensures that encrypted data that may be caught by an attacker cannot be reused anymore to masquerade the TOE. In phase 6, the integrity and confidentiality of data is ensured by FCS\_COP.1/GP Secret Data Protection. The SSCD provides a proof of identity with FIA\_API.1. This objective ensures as well that any authentication key is loaded in the TOE by an authenticated user, so that only genuine keys associated to genuine users are declared to the TOE. The key import defined by FMT\_SMF.1 is protected by access control. It is protected by the proper Agent(s) authentication that cannot be bypassed to access these functions with the TSF specified by FIA\_UID.1 and FIA\_UAU.1. The agent entitled to load the authentication key is (are) authenticated with FMT\_SMR.1. Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA\_AFL.1/RAD. This objective ensures the verification of the authenticity of the TOE as a whole device. This objective is mainly achieved by FIA\_API.1/TOE Authentication using FCS\_CKM.1/DH\_PACE. CA provides an evidence of possessing the Chip Authentication Private Key (CAPK). FMT\_MTD.1/CAPK governs creating/loading CAPK, whereas FMT\_MTD.1/KEY\_READ requires making this key unreadable by users. Hence, its value remains confidential. FDP\_RIP.1 requires erasing the values of CAPK and the session keys, here for CMAC. The authentication token is calculated using FCS\_COP.1/SM in Integrity. The TOE holder provides a proof of identity with FIA\_API.1/TOE Authentication. This objective aims to explicitly protect sensitive (as opposed to common) user and TSF-Data. This is mainly achieved by enforcing (FDP\_UCT.1/TRM and FDP\_UIT.1/TRM) the access control SFPs FDP\_ACC.1/TRM and FDP\_ACF.1/TRM. A specific authorization level is achieved by terminal identification/authentication as required by the SFRs FIA\_UID.1/PACE, FIA\_UAU.1/PACE supported by FCS\_COP.1/SIG\_VER. The TA protocol uses the result of the PACE authentication (FIA\_UID.1/PACE, FIA\_UAU.1/PACE, confidentiality of the PACE passwords is ensured by FMT\_MTD.1/KEY\_READ) being, in turn, supported by FCS\_CKM.1/DH\_PACE. Since PACE can use the PIN as the shared secret, the use and management of the PIN (FIA\_AFL.1/AUTH, FMT\_MTD.1/Resume\_PIN, FMT\_MTD.1/Unblock\_PIN, FMT\_MTD.1/Initialize\_PIN, FMT\_MTD.1/Change\_PIN, FMT\_MTD.1/UnblockChange\_RAD,

FMT\_MTD.1/Erase\_PIN, FMT\_MTD.1/Reinitialize\_PIN, FMT\_MTD.1/UnblockChange\_PUK) also support to achieve this objective. FDP\_RIP.1 requires erasing the temporal values of the PIN and PUK. FIA\_UAU.4/PACE, FIA\_UAU.5/PACE, FIA\_UAU.6/PACE and FCS\_CKM.4 represent some specific properties of the used protocols. To allow for a verification of the certificate chain as required in FMT\_MTD.3, the CVCA's public key and certificate as well as the current date are written or updated by authorized identified role as required by FMT\_MTD.1/CVCA\_INI, FMT\_MTD.1/CVCA\_UPD and FMT\_MTD.1/DATE. In contactless, this objective for the data exchanged is mainly achieved by FTP\_ITC.1/PACE using FCS\_COP.1/SM in Confidentiality. A prerequisite for establishing this trusted channel is a successful Chip Authentication, cf. FIA\_API.1/TOE Authentication using FCS\_CKM.1/DH\_PACE and possessing the special properties FIA\_UAU.5/PACE, and FIA\_UAU.6/EAC. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using FIA\_UID.1/PACE, FIA\_UAU.1/PACE and FCS\_CKM.1/DH\_PACE and possessing the special properties FIA\_UAU.5/PACE, FIA\_UAU.6/PACE. CA provides an evidence of possessing the Chip Authentication Private Key (CAPK). FMT\_MTD.1/CAPK governs creating/loading CAPK, FMT\_MTD.1/KEY\_READ requires making this key unreadable by users. Thus its value remains confidential. FDP\_RIP.1 requires erasing the values of CAPK and session keys, here for KENC. The SFRs FMT\_SMF.1 and FMT\_SMR.1/PACE support the related functions and roles. This objective ensures also the authenticity of user- and TSF-Data (after Terminal- and the Chip Authentication) by enabling its verification on both the terminal-side and by an active verification by the TOE itself. This objective is mainly achieved by FTP\_ITC.1/PACE in contactless using FCS\_COP.1/SM in Integrity. A prerequisite for establishing this trusted channel is a successful Chip Authentication, cf. FIA\_API.1/TOE Authentication using FCS\_CKM.1/DH\_PACE and possessing the special properties FIA\_UAU.5/PACE, and FIA\_UAU.6/EAC. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using FIA\_UID.1/PACE, FIA\_UAU.1/PACE and FCS\_CKM.1/DH\_PACE and possessing the special properties FIA\_UAU.5/PACE, FIA\_UAU.6/PACE. CA provides an evidence of possessing the Chip Authentication Private Key (CAPK). FMT\_MTD.1/CAPK governs creating/loading CAPK, FMT\_MTD.1/KEY\_READ requires to make this key unreadable by users. Hence its value remains confidential. FDP\_RIP.1 requires to erase the values of CAPK and session keys, here for KMAC. A prerequisite for successful CA is an accomplished TA as required by FIA\_UID.1/PACE, FIA\_UAU.1/PACE supported by FCS\_COP.1/SIG\_VER. The TA protocol uses the result of the PACE authentication (FIA\_UID.1/PACE, FIA\_UAU.1/PACE) being, in turn, supported by FCS\_CKM.1/DH\_PACE. Since PACE can use the PIN as the shared secret, the use and management of the PIN (FIA\_AFL.1/AUTH, FMT\_MTD.1/Resume\_PIN, FMT\_MTD.1/Initialize\_PIN, FMT\_MTD.1/Change\_PIN, FMT\_MTD.1/Unblock\_PIN, FMT\_MTD.1/UnblockChange\_RAD, FMT\_MTD.1/Erase\_PIN, FMT\_MTD.1/Reinitialize\_PIN, FMT\_MTD.1/UnblockChange\_PUK) also support achieving this objective. FDP\_RIP.1 requires to erase the temporal values of the PIN and PUK. FIA\_UAU.4/PACE, FIA\_UAU.5/PACE, FIA\_UAU.6/EAC and FCS\_CKM.4 represent some specific required properties of the used protocols. To allow for a verification of the certificate chain as required in FMT\_MTD.3, the CVCA's public key and certificate, as well as the current date, are written or updated by authorized identified roles as required by FMT\_MTD.1/CVCA\_INI, FMT\_MTD.1/CVCA\_UPD and FMT\_MTD.1/DATE. The SFRs FMT\_SMF.1 and FMT\_SMR.1/PACE support the related functions and roles. This objective ensures the confidentiality of the user- and TSF-Data stored and, after Terminal- and Chip Authentication, of their exchange. This objective for the data stored is mainly achieved by FDP\_ACC.1/TRM and FDP\_ACF.1/TRM. Enforcement of the two previous in a protected

manner is ensured by FDP\_UCT.1/TRM and FDP\_UIT.1/TRM. A specific authorization level is achieved by terminal identification/authentication as required by the SFRs FIA\_UID.1/PACE, FIA\_UAU.1/PACE supported by FCS\_COP.1/SIG\_VER. The TA protocol uses the result of the PACE authentication (FIA\_UID.1/PACE, FIA\_UAU.1/PACE, confidentiality of the PACE passwords is ensured by FMT\_MTD.1/KEY\_READ) being, in turn, supported by FCS\_CKM.1/DH\_PACE. Since PACE can use the PIN as the shared secret, the use and management of the PIN (FIA\_AFL.1/AUTH, FMT\_MTD.1/Resume\_PIN, FMT\_MTD.1/Unblock\_PIN, FMT\_MTD.1/Change\_PIN, FMT\_MTD.1/Initialize\_PIN, FMT\_MTD.1/UnblockChange\_RAD, FMT\_MTD.1/Erase\_PIN, FMT\_MTD.1/Reinitialize\_PIN, FMT\_MTD.1/UnblockChange\_PUK) also support to achieve this objective. FDP\_RIP.1 requires erasing the temporal values of the PIN and PUK. FIA\_UAU.4/PACE, FIA\_UAU.5/PACE, FIA\_UAU.6/PACE and FCS\_CKM.4 represent some specific properties of the used protocols. To allow for a verification of the certificate chain as required in FMT\_MTD.3, the CVCA's public key and certificate as well as the current date are written or updated by authorized identified role as required by FMT\_MTD.1/CVCA\_INI, FMT\_MTD.1/CVCA\_UPD and FMT\_MTD.1/DATE. This objective for the data exchanged is mainly achieved in contactless by FTP\_ITC.1/PACE using FCS\_COP.1/SM in Confidentiality. A prerequisite for establishing this trusted channel is a successful Chip Authentication, cf. FIA\_API.1/TOE Authentication using FCS\_CKM.1/DH\_PACE and possessing the special properties FIA\_UAU.5/PACE, and FIA\_UAU.6/EAC. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using FIA\_UID.1/PACE, FIA\_UAU.1/PACE and FCS\_CKM.1/DH\_PACE and possessing the special properties FIA\_UAU.5/PACE, FIA\_UAU.6/PACE. CA provides an evidence of possessing the Chip Authentication Private Key (CAPK). FMT\_MTD.1/CAPK governs creating/loading CAPK, FMT\_MTD.1/KEY\_READ requires making this key unreadable by users. Thus its value remains confidential. FDP\_RIP.1 requires erasing the values of CAPK and session keys, here for KENC. The SFRs FMT\_SMF.1 and FMT\_SMR.1/PACE support the related functions and roles. This objective ensures the integrity of stored user- and TSF-Data and, after Terminal- and Chip Authentication, of these data exchanged (physical manipulation and unauthorized modifying). Physical manipulation is addressed by FPT\_PHP.3. Unauthorized modifying of the stored data is addressed by FDP\_ACC.1/TRM and FDP\_ACF.1/TRM. Enforcement of the two previous in a protected manner is ensured by FDP\_UCT.1/TRM and FDP\_UIT.1/TRM. A specific authorization level is achieved by terminal identification/ authentication as required by the SFRs FIA\_UID.1/PACE, FIA\_UAU.1/PACE supported by FCS\_COP.1/SIG\_VER. The TA protocol uses the result of PACE authentication (FIA\_UID.1/PACE, FIA\_UAU.1/PACE) being, in turn, supported by FCS\_CKM.1.1/DH\_PACE. Since PACE can use the PIN as the shared secret, using and management of PIN (FIA\_AFL.1/AUTH, FMT\_MTD.1/Resume\_PIN, FMT\_MTD.1/Change\_PIN, FMT\_MTD.1/Unblock\_PIN FMT\_MTD.1/Initialize\_PIN, FMT\_MTD.1/UnblockChange\_RAD, FMT\_MTD.1/Erase\_PIN, FMT\_MTD.1/Reinitialize\_PIN, FMT\_MTD.1/UnblockChange\_PUK) also support achievement of this objective. FDP\_RIP.1 requires erasing the temporal values of PIN, PUK. FIA\_UAU.4/PACE, FIA\_UAU.5/PACE and FCS\_CKM.4 represent some required specific properties of the used protocols. To allow for a verification of the certificate chain as required in FMT\_MTD.3, the CVCA's public key and certificate as well as the current date are written or update by authorized identified role as required by FMT\_MTD.1/CVCA\_INI, FMT\_MTD.1/CVCA\_UPD and FMT\_MTD.1/DATE. Unauthorized modifying of the exchanged data is addressed by FTP\_ITC.1/PACE in contactless using FCS\_COP.1/SM in integrity. A prerequisite for establishing this trusted channel is a successful Chip Authentication, cf. FIA\_API.1/TOE Authentication using FCS\_CKM.1/DH\_PACE possessing the special properties FIA\_UAU.5/PACE and

FIA\_UAU.6/EAC. As a prerequisite of this trusted channel a trusted channel established with the PACE protocol using FIA\_UID.1/PACE, FIA\_UAU.1/PACE and FCS\_CKM.1/DH\_PACE and possessing the special properties FIA\_UAU.5/PACE, FIA\_UAU.6/PACE. CA provides an evidence of possessing the Chip Authentication Private Key (CAPK). FMT\_MTD.1/CAPK governs creating/loading CAPK, and FMT\_MTD.1/KEY\_READ requires CAPK to be unreadable by users; thus its value remains confidential. FDP\_RIP.1 requires erasing the values of CAPK and session keys (here: for KMAC). The SFRs FMT\_SMF.1 and FMT\_SMR.1/PACE support related functions and roles. This objective prevents TOE's functions being not intended to be used in the operational phase from manipulating and disclosing the User- and TSF-data. This objective is achieved by FMT\_LIM.1 and FMT\_LIM.2 preventing misuse of test and other functionality of the TOE having not to be used in the TOE's operational life cycle phase. This objective protects against disclosure of confidential User- or/and TSF-data stored on / processed by the TOE. This objective is achieved

- o by FPT\_EMS.1 and FPT\_EMS.1/PIN-PUK-KEYS for measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines,
- o by FPT\_FLS.1 and FPT\_TST.1 for forcing a malfunction of the TOE, and
- o by FPT\_PHP.3 for a physical manipulation of the TOE. This objective ensures a correct operation of the TOE by preventing its operation outside the normal operating conditions. This objective is covered by FPT\_TST.1 requiring self tests to demonstrate the correct operation of the TOE and tests of authorised users to verify the integrity of the TSF-data and the embedded software (TSF code) as well as by FPT\_FLS.1 requiring entering a secure state of the TOE in case of detected failure or operating conditions possibly causing a malfunction. This objective protects of the confidentiality and integrity of the User- and TSF-data as well as embedded software stored in the TOE. This objective is completely covered by FPT\_PHP.3 in an obvious way.

**OT.Key\_Lifecycle\_Security** Secure Keys generation is ensured by FCS\_CKM.1/SCD/SVD\_Generation. The secure keys usage is ensured cryptographically according to FCS\_COP.1/Digital Auth, FCS\_COP.1/Enc Key Decipherment. Keys usage is based on the security attribute secure TSF management according to FMT\_MSA.2, FMT\_MSA.3, FMT\_SMF.1 and FMT\_SMR.1. The test functions FPT\_TST.1 provides failure detection throughout the lifecycle. The SFR FCS\_CKM.4 ensures a secure keys destruction.

**OT.Keys\_Secrecy** is provided by the security functions specified by the following SFR. FCS\_CKM.1/SCD/SVD\_Generation ensure the use of secure cryptographic algorithms for keys generation. Cryptographic quality of the asymmetric key pair(s) shall prevent disclosure of the TOE's private authentication key(s) and eServices key(s) by cryptographic attacks using the publicly known public key. The security functions specified by FDP\_RIP.1 and FCS\_CKM.4 ensure that residual information on a key(s) is destroyed after a key has been used for authentication (verification or proof) or an eServices keys has been used and that destruction of key(s) leaves no residual information. The security functions specified by FDP\_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the authentication key. 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). FPT\_EMS.1/PIN-PUK-KEYS and FPT\_PHP.3 require additional security features of the TOE to ensure the confidentiality of the key(s).

**OT.TOE\_AuthKey\_Unique** implements the requirement of practically unique TOE's authentication private key, which is provided by the cryptographic algorithms specified by FCS\_CKM.1/SCD/SVD\_Generation.

**OT.Lifecycle\_Management** ensures a correct separation of the TOE life cycle between phase 6 and 7. In phase 6, FMT\_MTD.1/TOE State ensures the TOE irreversibly switches from phase 6 to phase 7 under the sole control of the Personalization Agent. The Personalization Agent is authenticated with a mutual authentication performed with FCS\_RND.1 and FCS\_COP.1/GP Secret Data Protection and is authenticated with FMT\_SMR.1. In phase 7, FDP\_ACC.1/Signature\_Creation, FDP\_ACC.1/SVD\_Transfer, FDP\_ACC.1/SCD/SVD\_Generation, FDP\_ACC.1/SCD\_Import, FDP\_ACF.1/Signature\_Creation, FDP\_ACF.1/SVD\_Transfer, FDP\_ACF.1/SCD/SVD\_Generation, FDP\_ACF.1/SCD\_Import, FMT\_MTD.1/Unblock\_PIN, FMT\_MTD.1/UnblockChange\_RAD, FMT\_MTD.1/Erase\_PIN, FMT\_MOF.1, FMT\_MTD.1/Admin, FMT\_MTD.1/Signatory ensures the Personalization Agent does not control the TOE anymore. In phase 6, the Personalization Agent has complete control over the administrative functions of the TOE. It may import, erase, generate SCD/SVD, export SVD, manage Keys, create RAD and manage the configuration of the TOE as mandated in FMT\_SMF.1, according to the security policies defined in FDP\_ACC.1/SVD transfer, FDP\_ACC.1/SCD/SVD\_Generation, FDP\_ACC.1/SCD import, FDP\_ACF.1/SVD transfer, FDP\_ACF.1/SCD/SVD\_Generation, FDP\_ACF.1/SCD import, It may as well change TOE State (FMT\_MTD.1/TOE State). These functions are protected by the Personalization Agent authentication that cannot be bypassed to access these functions with the TSF specified by FIA\_UID.1 and FIA\_UAU.1. FMT\_MSA.1/Admin, FMT\_MSA.2, FMT\_MSA.3 ensure that the sole Personalization Agent can realize these functions.

**OT.eServices** is provided by the cryptographic mechanisms specified by (1) FCS\_COP.1/Digital Auth, (2) FCS\_COP.1/Enc Key Decipherment. These requirements ensure the cryptographic robustness of these eServices. The eServices keys may be loaded, generated, and the matching public key may be exported as required by FMT\_SMF.1 and FMT\_SMR.1. These functions are protected by the proper Agent(s) authentication that cannot be bypassed to access these functions with the TSF specified by FIA\_UID.1/PACE and FIA\_UAU.1/PACE. Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA\_AFL.1/RAD.

**OT.AC\_Pers\_EAC** ensures that only the personalization agent can write user- and TSF-Data into the TOE, and that some of this data cannot be altered after personalization. This property is covered by FDP\_ACC.1/TRM and FDP\_ACF.1/TRM requiring, amongst other, an appropriate authorization level of an Authentication Terminal. This authorization level can be achieved by terminal identification/authentication as required by the SFRs FIA\_UID.1/PACE and FIA\_UAU.1/PACE. The SFRs FMT\_SMF.1 and FMT\_SMR.1/PACE support the related functions and roles. Since only an Authentication Terminal can reach the necessary authorization level, using and managing the PIN (the related SFRs are FIA\_AFL.1/AUTH, FMT\_MTD.1/Resume\_PIN, FMT\_MTD.1/Change\_PIN, FMT\_MTD.1/Unblock\_PIN, FMT\_MTD.1/Initialize\_PIN, FMT\_MTD.1/UnblockChange\_RAD,

FMT\_MTD.1/Erase\_PIN, FMT\_MTD.1/Reinitialize\_PIN, FMT\_MTD.1/UnblockChange\_PUK) also support the achievement of this objective. The justification for the SFRs FMT\_MTD.1/INI\_ENA and FMT\_MTD.1/INI\_DIS arises from the justification for OT.Identification above with respect to the pre-personalisation data. FDP\_RIP.1 requires erasing the temporal values PIN and PUK. Finally, FMT\_MTD.1/KEY\_READ ensures that cryptographic keys for EAC cannot be read by users.

**OT.Tracing** ensures that the TOE prevents gathering TOE tracing data by means of unambiguously identifying the electronic document remotely through establishing or listening to communication via the contactless-based interface of the TOE without a priori knowledge of the correct values of shared passwords (MRZ,CAN, PIN, PUK). This objective is achieved by FIA\_AFL.1/AUTH and FTP\_ITC.1/PACE

**OT.ADMIN\_Configuration** The security objective OT.ADMIN\_Configuration "Protection of the TOE administration" addresses management of the Data Configuration with key size management for the Chip Authentication of the TOE. ADMIN keys are created during pre-personalization. FMT\_MTD.1/KEY\_READ restricts the ability to read the Administrator Keys to none. FPT\_EMS.1 protects the confidentiality of Administrator Agent keys. The SFRs FMT\_SMF.1 and FMT\_SMR.1 support the functions and roles related. Symmetric authentication is managed through FCS\_COP.1/GP Secret Data Protection, FCS\_COP.1/SM in Confidentiality and FCS\_COP.1/SM in Integrity. The administration TSF data manipulation are supported by FMT\_MTD.1/Admin. It is now allowed to configure the Chip Authentication key parameters to be used during key generation in USE phase. The minimum key size that the user can generate in USE phase is controlled by the "ADMIN" role. It is also possible to change the key parameters during the key generation process. For example changing the domain parameters of an elliptic curve key. It is also possible to invalidate one of the Chip Authentication key in USE phase and to set the secondary key as being the primary key. It is also possible to create and delete EF files in Use Phase through proper File access condition been met as defined in FDP\_ACC.1/MNG\_File and FDP\_ACF.1/MNG\_File. Note: after such process, the "freed" CA key set is available for a future CA key generation.

**OT.Key\_Usage\_Counter** The security objective OT.Key\_Usage\_Counter is covered by FMT\_MTD.1/Key\_Usage\_Counter.

### 9.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
<a href="#">OT.Lifecycle Security</a>	<a href="#">FCS_CKM.1/SCD/SVD Generation</a> , <a href="#">FCS_CKM.4</a> , <a href="#">FDP_ACC.1/SCD/SVD Generation</a> , <a href="#">FDP_ACF.1/SCD/SVD Generation</a> , <a href="#">FDP_ACC.1/SVD Transfer</a> , <a href="#">FDP_ACF.1/Signature Creation</a> , <a href="#">FDP_ACC.1/Signature Creation</a> , <a href="#">FDP_ACF.1/SVD Transfer</a> , <a href="#">FMT_MOF.1</a> , <a href="#">FMT_MSA.1/Admin</a> , <a href="#">FMT_MSA.1/Signatory</a> , <a href="#">FMT_MSA.2</a> , <a href="#">FMT_MSA.3</a> , <a href="#">FMT_MSA.4</a> , <a href="#">FMT_MTD.1/Admin</a> , <a href="#">FMT_MTD.1/Signatory</a> ,	<a href="#">Section 9.3.1</a>



	<a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FPT_TST.1</a> , <a href="#">FCS_COP.1/Sign</a> , <a href="#">FDP_ACC.1/SCD_Import</a> , <a href="#">FDP_ACF.1/SCD_Import</a> , <a href="#">FDP_ITC.1/SCD</a> , <a href="#">FDP_UCT.1/SCD</a> , <a href="#">FTP_ITC.1/SCD</a> , <a href="#">FMT_MTD.1/Erase_PIN</a> , <a href="#">FMT_MTD.1/UnblockChange_RAD</a>	
<a href="#">OT.SCD_Secrecy</a>	<a href="#">FCS_CKM.1/SCD/SVD_Generation</a> , <a href="#">FCS_CKM.4</a> , <a href="#">FDP_RIP.1</a> , <a href="#">FDP_SDI.2/Persistent</a> , <a href="#">FPT_FLS.1</a> , <a href="#">FPT_PHP.3</a> , <a href="#">FPT_TST.1</a> , <a href="#">FDP_UCT.1/SCD</a> , <a href="#">FTP_ITC.1/SCD</a> , <a href="#">FPT_EMS.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Sig_Secure</a>	<a href="#">FDP_SDI.2/Persistent</a> , <a href="#">FPT_TST.1</a> , <a href="#">FCS_COP.1/Sign</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Sigy_SigF</a>	<a href="#">FDP_ACF.1/Signature_Creation</a> , <a href="#">FDP_ACC.1/Signature_Creation</a> , <a href="#">FDP_RIP.1</a> , <a href="#">FDP_SDI.2/DTBS</a> , <a href="#">FIA_AFL.1/RAD</a> , <a href="#">FIA_UAU.1</a> , <a href="#">FIA_UID.1</a> , <a href="#">FMT_MOF.1</a> , <a href="#">FMT_MSA.1/Signatory</a> , <a href="#">FMT_MSA.2</a> , <a href="#">FMT_MSA.3</a> , <a href="#">FMT_MSA.4</a> , <a href="#">FMT_MTD.1/Admin</a> , <a href="#">FMT_MTD.1/Signatory</a> , <a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FCS_COP.1/GP_Secret</a> <a href="#">Data_Protection</a> , <a href="#">FCS_RND.1</a> , <a href="#">FMT_MTD.1/Unblock_PIN</a> , <a href="#">FMT_MTD.1/UnblockChange_RAD</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.DTBS_Integrity_TOE</a>	<a href="#">FDP_SDI.2/DTBS</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.EMSEC_Design</a>	<a href="#">FPT_EMS.1/PIN-PUK-KEYS</a> , <a href="#">FPT_EMS.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Tamper_ID</a>	<a href="#">FPT_PHP.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Tamper_Resistance</a>	<a href="#">FPT_PHP.3</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.SCD/SVD_Auth_Gen</a>	<a href="#">FDP_ACC.1/SCD/SVD_Generation</a> , <a href="#">FDP_ACF.1/SCD/SVD_Generation</a> , <a href="#">FIA_UAU.1</a> , <a href="#">FIA_UID.1</a> , <a href="#">FMT_MSA.1/Admin</a> , <a href="#">FMT_MSA.2</a> , <a href="#">FMT_MSA.3</a> , <a href="#">FMT_MSA.4</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.SCD_Unique</a>	<a href="#">FCS_CKM.1/SCD/SVD_Generation</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.SCD_SVD_Corresp</a>	<a href="#">FCS_CKM.1/SCD/SVD_Generation</a> , <a href="#">FDP_SDI.2/Persistent</a> , <a href="#">FMT_MSA.4</a> , <a href="#">FMT_SMF.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.SCD_Auth_Imp</a>	<a href="#">FIA_UID.1</a> , <a href="#">FIA_UAU.1</a> , <a href="#">FDP_ACC.1/SCD_Import</a> , <a href="#">FDP_ACF.1/SCD_Import</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.TOE_SSCD_Auth</a>	<a href="#">FIA_UAU.1</a> , <a href="#">FIA_API.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.TOE_TC_SVD_Exp</a>	<a href="#">FDP_ACF.1/SVD_Transfer</a> , <a href="#">FDP_ACC.1/SVD_Transfer</a> , <a href="#">FDP_DAU.2/SVD</a> , <a href="#">FTP_ITC.1/SVD</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.TOE_TC_VAD_Imp</a>	<a href="#">FTP_ITC.1/VAD</a>	<a href="#">Section 9.3.1</a>

<a href="#">OT.TOE TC DTBS Imp</a>	<a href="#">FDP UIT.1/DTBS</a> , <a href="#">FTP ITC.1/DTBS</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Identification</a>	<a href="#">FMT SMF.1</a> , <a href="#">FMT MTD.1/INI_ENA</a> , <a href="#">FMT MTD.1/INI_DIS</a> , <a href="#">FMT SMR.1/PACE</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Authentication Secure</a>	<a href="#">FCS CKM.1/Session Keys</a> , <a href="#">FCS CKM.1/DH_PACE</a> , <a href="#">FCS COP.1/GP Secret Data Protection</a> , <a href="#">FCS COP.1/SM in Confidentiality</a> , <a href="#">FCS COP.1/SM in Integrity</a> , <a href="#">FCS COP.1/SIG_VER</a> , <a href="#">FCS RND.1</a> , <a href="#">FIA UID.1/PACE</a> , <a href="#">FIA UAU.1/PACE</a> , <a href="#">FIA UAU.4/PACE</a> , <a href="#">FIA UAU.5/PACE</a> , <a href="#">FIA UAU.6/PACE</a> , <a href="#">FIA UAU.6/EAC</a> , <a href="#">FIA AFL.1/AUTH</a> , <a href="#">FIA API.1/TOE Authentication</a> , <a href="#">FDP ACC.1/TRM</a> , <a href="#">FDP ACF.1/TRM</a> , <a href="#">FDP UCT.1/TRM</a> , <a href="#">FDP UIT.1/TRM</a> , <a href="#">FTP ITC.1/PACE</a> , <a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT MTD.1/CVCA_INI</a> , <a href="#">FMT MTD.1/CVCA_UPD</a> , <a href="#">FMT MTD.1/DATE</a> , <a href="#">FMT MTD.1/CAPK</a> , <a href="#">FMT MTD.1/KEY_READ</a> , <a href="#">FMT MTD.1/Initialize PIN</a> , <a href="#">FMT MTD.1/Resume PIN</a> , <a href="#">FMT MTD.1/Change PIN</a> , <a href="#">FMT MTD.1/Unblock PIN</a> , <a href="#">FMT MTD.1/UnblockChange_RAD</a> , <a href="#">FMT MTD.1/Erase PIN</a> , <a href="#">FMT MTD.1/Reinitialize PIN</a> , <a href="#">FMT MTD.1/UnblockChange_PUK</a> , <a href="#">FMT MTD.3</a> , <a href="#">FMT LIM.1</a> , <a href="#">FMT LIM.2</a> , <a href="#">FPT EMS.1/PIN-PUK-KEYS</a> , <a href="#">FCS CKM.4</a> , <a href="#">FDP RIP.1</a> , <a href="#">FDP SDI.2/Persistent</a> , <a href="#">FIA UID.1</a> , <a href="#">FIA UAU.1</a> , <a href="#">FIA API.1</a> , <a href="#">FMT SMR.1</a> , <a href="#">FMT SMF.1</a> , <a href="#">FPT EMS.1</a> , <a href="#">FPT FLS.1</a> , <a href="#">FPT PHP.3</a> , <a href="#">FPT TST.1</a> , <a href="#">FIA AFL.1/RAD</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Key Lifecycle Security</a>	<a href="#">FCS COP.1/Digital Auth</a> , <a href="#">FCS COP.1/Enc Key Decipherment</a> , <a href="#">FCS CKM.1/SCD/SVD Generation</a> , <a href="#">FCS CKM.4</a> , <a href="#">FMT SMR.1</a> , <a href="#">FMT SMF.1</a> , <a href="#">FMT MSA.2</a> , <a href="#">FMT MSA.3</a> , <a href="#">FPT TST.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Keys Secrecy</a>	<a href="#">FPT EMS.1/PIN-PUK-KEYS</a> , <a href="#">FCS CKM.1/SCD/SVD Generation</a> , <a href="#">FCS CKM.4</a> , <a href="#">FDP RIP.1</a> , <a href="#">FDP SDI.2/Persistent</a> , <a href="#">FPT FLS.1</a> , <a href="#">FPT PHP.3</a> , <a href="#">FPT TST.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.TOE AuthKey Unique</a>	<a href="#">FCS CKM.1/SCD/SVD Generation</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Lifecycle Management</a>	<a href="#">FCS COP.1/GP Secret Data Protection</a> , <a href="#">FCS RND.1</a> , <a href="#">FMT MTD.1/Unblock PIN</a> , <a href="#">FMT MTD.1/UnblockChange_RAD</a> , <a href="#">FMT MTD.1/Erase PIN</a> , <a href="#">FMT MTD.1/TOE</a>	<a href="#">Section 9.3.1</a>

	<a href="#">State</a> , <a href="#">FDP_ACC.1/SCD/SVD Generation</a> , <a href="#">FDP_ACF.1/SCD/SVD Generation</a> , <a href="#">FDP_ACC.1/SVD Transfer</a> , <a href="#">FDP_ACF.1/SVD Transfer</a> , <a href="#">FDP_ACC.1/SCD Import</a> , <a href="#">FDP_ACF.1/SCD Import</a> , <a href="#">FIA_UID.1</a> , <a href="#">FIA_UAU.1</a> , <a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FMT_MSA.1/Admin</a> , <a href="#">FMT_MSA.2</a> , <a href="#">FMT_MSA.3</a> , <a href="#">FMT_MTD.1/Admin</a> , <a href="#">FDP_ACC.1/Signature Creation</a> , <a href="#">FDP_ACF.1/Signature Creation</a> , <a href="#">FMT_MOF.1</a> , <a href="#">FMT_MTD.1/Signatory</a>	
<a href="#">OT.eServices</a>	<a href="#">FCS_COP.1/Digital Auth</a> , <a href="#">FCS_COP.1/Enc Key Decipherment</a> , <a href="#">FIA_UID.1/PACE</a> , <a href="#">FIA_UAU.1/PACE</a> , <a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FIA_AFL.1/RAD</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.AC Pers EAC</a>	<a href="#">FDP_ACF.1/TRM</a> , <a href="#">FDP_RIP.1</a> , <a href="#">FDP_ACC.1/TRM</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a> , <a href="#">FMT_MTD.1/Initialize PIN</a> , <a href="#">FMT_MTD.1/Resume PIN</a> , <a href="#">FMT_MTD.1/Change PIN</a> , <a href="#">FMT_MTD.1/Unblock PIN</a> , <a href="#">FMT_MTD.1/KEY READ</a> , <a href="#">FIA_UID.1/PACE</a> , <a href="#">FIA_UAU.1/PACE</a> , <a href="#">FIA_AFL.1/AUTH</a> , <a href="#">FMT_MTD.1/UnblockChange RAD</a> , <a href="#">FMT_MTD.1/Erase PIN</a> , <a href="#">FMT_MTD.1/Reinitialize PIN</a> , <a href="#">FMT_MTD.1/UnblockChange PUK</a> , <a href="#">FMT_MTD.1/INI_ENA</a> , <a href="#">FMT_MTD.1/INI_DIS</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Tracing</a>	<a href="#">FIA_AFL.1/AUTH</a> , <a href="#">FTP_ITC.1/PACE</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.ADMIN Configuration</a>	<a href="#">FMT_MTD.1/KEY READ</a> , <a href="#">FMT_MTD.1/Admin</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1</a> , <a href="#">FPT_EMS.1</a> , <a href="#">FDP_ACC.1/MNG File</a> , <a href="#">FDP_ACF.1/MNG File</a> , <a href="#">FCS_COP.1/GP Secret Data Protection</a> , <a href="#">FCS_COP.1/SM in Confidentiality</a> , <a href="#">FCS_COP.1/SM in Integrity</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Key Usage Counter</a>	<a href="#">FMT_MTD.1/Key Usage Counter</a>	<a href="#">Section 9.3.1</a>

**Table 22 Security Objectives and SFRs - Coverage**

Security Functional Requirements	Security Objectives
<a href="#">FPT_EMS.1</a>	<a href="#">OT.SCD Secrecy</a> , <a href="#">OT.EMSEC Design</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.ADMIN Configuration</a>

<a href="#">FPT_FLS.1</a>	<a href="#">OT.SCD Secrecy</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.Keys Secrecy</a>
<a href="#">FPT_PHP.1</a>	<a href="#">OT.Tamper ID</a>
<a href="#">FPT_PHP.3</a>	<a href="#">OT.SCD Secrecy</a> , <a href="#">OT.Tamper Resistance</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.Keys Secrecy</a>
<a href="#">FPT_TST.1</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.SCD Secrecy</a> , <a href="#">OT.Sig Secure</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.Key Lifecycle Security</a> , <a href="#">OT.Keys Secrecy</a>
<a href="#">FMT_SMR.1</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.Key Lifecycle Security</a> , <a href="#">OT.Lifecycle Management</a> , <a href="#">OT.eServices</a> , <a href="#">OT.ADMIN Configuration</a>
<a href="#">FMT_SMF.1</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OT.SCD SVD Corresp</a> , <a href="#">OT.Identification</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.Key Lifecycle Security</a> , <a href="#">OT.Lifecycle Management</a> , <a href="#">OT.eServices</a> , <a href="#">OT.AC Pers EAC</a> , <a href="#">OT.ADMIN Configuration</a>
<a href="#">FMT_MOF.1</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OT.Lifecycle Management</a>
<a href="#">FMT_MSA.1/Admin</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.SCD/SVD Auth Gen</a> , <a href="#">OT.Lifecycle Management</a>
<a href="#">FMT_MSA.1/Signatory</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.Sigy SigF</a>
<a href="#">FMT_MSA.2</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OT.SCD/SVD Auth Gen</a> , <a href="#">OT.Key Lifecycle Security</a> , <a href="#">OT.Lifecycle Management</a>
<a href="#">FMT_MSA.3</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OT.SCD/SVD Auth Gen</a> , <a href="#">OT.Key Lifecycle Security</a> , <a href="#">OT.Lifecycle Management</a>
<a href="#">FMT_MSA.4</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OT.SCD/SVD Auth Gen</a> , <a href="#">OT.SCD SVD Corresp</a>
<a href="#">FMT_MTD.1/Admin</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OT.Lifecycle Management</a> , <a href="#">OT.ADMIN Configuration</a>

<a href="#">FMT_MTD.1/Signatory</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OT.Lifecycle Management</a>
<a href="#">FIA_UID.1</a>	<a href="#">OT.Sigy SigF</a> , <a href="#">OT.SCD/SVD Auth Gen</a> , <a href="#">OT.SCD Auth Imp</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.Lifecycle Management</a>
<a href="#">FIA_AFL.1/RAD</a>	<a href="#">OT.Sigy SigF</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.eServices</a>
<a href="#">FIA_UAU.1</a>	<a href="#">OT.Sigy SigF</a> , <a href="#">OT.SCD/SVD Auth Gen</a> , <a href="#">OT.SCD Auth Imp</a> , <a href="#">OT.TOE SSCD Auth</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.Lifecycle Management</a>
<a href="#">FDP_SDI.2/DTBS</a>	<a href="#">OT.Sigy SigF</a> , <a href="#">OT.DTBS Integrity TOE</a>
<a href="#">FDP_SDI.2/Persistent</a>	<a href="#">OT.SCD Secrecy</a> , <a href="#">OT.Sig Secure</a> , <a href="#">OT.SCD SVD Corresp</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.Keys Secrecy</a>
<a href="#">FDP_RIP.1</a>	<a href="#">OT.SCD Secrecy</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.Keys Secrecy</a> , <a href="#">OT.AC Pers EAC</a>
<a href="#">FDP_ACC.1/Signature Creation</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OT.Lifecycle Management</a>
<a href="#">FDP_ACF.1/Signature Creation</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OT.Lifecycle Management</a>
<a href="#">FCS_COP.1/Sign</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.Sig Secure</a>
<a href="#">FCS_CKM.4</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.SCD Secrecy</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.Key Lifecycle Security</a> , <a href="#">OT.Keys Secrecy</a>
<a href="#">FCS_CKM.1/SCD/SVD Generation</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.SCD Secrecy</a> , <a href="#">OT.SCD Unique</a> , <a href="#">OT.SCD SVD Corresp</a> , <a href="#">OT.Key Lifecycle Security</a> , <a href="#">OT.Keys Secrecy</a> , <a href="#">OT.TOE AuthKey Unique</a>
<a href="#">FDP_ACC.1/SVD Transfer</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.TOE TC SVD Exp</a> , <a href="#">OT.Lifecycle Management</a>
<a href="#">FDP_ACF.1/SVD Transfer</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.TOE TC SVD Exp</a> , <a href="#">OT.Lifecycle Management</a>

<a href="#">FDP_ACC.1/SCD/SVD Generation</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.SCD/SVD Auth Gen</a> , <a href="#">OT.Lifecycle Management</a>
<a href="#">FDP_ACF.1/SCD/SVD Generation</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.SCD/SVD Auth Gen</a> , <a href="#">OT.Lifecycle Management</a>
<a href="#">FTP_ITC.1/SCD</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.SCD Secrecy</a>
<a href="#">FDP_UCT.1/SCD</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.SCD Secrecy</a>
<a href="#">FDP_ITC.1/SCD</a>	<a href="#">OT.Lifecycle Security</a>
<a href="#">FDP_ACC.1/SCD Import</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.SCD Auth Imp</a> , <a href="#">OT.Lifecycle Management</a>
<a href="#">FDP_ACF.1/SCD Import</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.SCD Auth Imp</a> , <a href="#">OT.Lifecycle Management</a>
<a href="#">FTP_ITC.1/SVD</a>	<a href="#">OT.TOE TC SVD Exp</a>
<a href="#">FDP_DAU.2/SVD</a>	<a href="#">OT.TOE TC SVD Exp</a>
<a href="#">FIA_API.1</a>	<a href="#">OT.TOE SSCD Auth</a> , <a href="#">OT.Authentication Secure</a>
<a href="#">FDP_UIT.1/DTBS</a>	<a href="#">OT.TOE TC DTBS Imp</a>
<a href="#">FTP_ITC.1/VAD</a>	<a href="#">OT.TOE TC VAD Imp</a>
<a href="#">FTP_ITC.1/DTBS</a>	<a href="#">OT.TOE TC DTBS Imp</a>
<a href="#">FCS_RND.1</a>	<a href="#">OT.SigY SigF</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.Lifecycle Management</a>
<a href="#">FCS_CKM.1/DH PACE</a>	<a href="#">OT.Authentication Secure</a>
<a href="#">FCS_CKM.1/Session Keys</a>	<a href="#">OT.Authentication Secure</a>
<a href="#">FCS_COP.1/GP Secret Data Protection</a>	<a href="#">OT.SigY SigF</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.Lifecycle Management</a> , <a href="#">OT.ADMIN Configuration</a>
<a href="#">FCS_COP.1/SM in Confidentiality</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OT.ADMIN Configuration</a>
<a href="#">FCS_COP.1/SM in Integrity</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OT.ADMIN Configuration</a>
<a href="#">FCS_COP.1/Digital Auth</a>	<a href="#">OT.Key Lifecycle Security</a> , <a href="#">OT.eServices</a>
<a href="#">FCS_COP.1/Enc Key Decipherment</a>	<a href="#">OT.Key Lifecycle Security</a> , <a href="#">OT.eServices</a>
<a href="#">FCS_COP.1/SIG VER</a>	<a href="#">OT.Authentication Secure</a>
<a href="#">FDP_ACC.1/TRM</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OT.AC Pers EAC</a>

<a href="#">FDP_ACF.1/TRM</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OT.AC Pers EAC</a>
<a href="#">FDP_ACC.1/MNG File</a>	<a href="#">OT.ADMIN Configuration</a>
<a href="#">FDP_ACF.1/MNG File</a>	<a href="#">OT.ADMIN Configuration</a>
<a href="#">FDP_UCT.1/TRM</a>	<a href="#">OT.Authentication Secure</a>
<a href="#">FDP_UIT.1/TRM</a>	<a href="#">OT.Authentication Secure</a>
<a href="#">FIA_UID.1/PACE</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OT.eServices</a> , <a href="#">OT.AC Pers EAC</a>
<a href="#">FIA_UAU.1/PACE</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OT.eServices</a> , <a href="#">OT.AC Pers EAC</a>
<a href="#">FIA_UAU.4/PACE</a>	<a href="#">OT.Authentication Secure</a>
<a href="#">FIA_UAU.5/PACE</a>	<a href="#">OT.Authentication Secure</a>
<a href="#">FIA_UAU.6/PACE</a>	<a href="#">OT.Authentication Secure</a>
<a href="#">FIA_UAU.6/EAC</a>	<a href="#">OT.Authentication Secure</a>
<a href="#">FIA_AFL.1/AUTH</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OT.AC Pers EAC</a> , <a href="#">OT.Tracing</a>
<a href="#">FIA_API.1/TOE Authentication</a>	<a href="#">OT.Authentication Secure</a>
<a href="#">FMT_SMR.1/PACE</a>	<a href="#">OT.Identification</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.AC Pers EAC</a>
<a href="#">FMT_MTD.1/CVCA INI</a>	<a href="#">OT.Authentication Secure</a>
<a href="#">FMT_MTD.1/CVCA UPD</a>	<a href="#">OT.Authentication Secure</a>
<a href="#">FMT_MTD.1/DATE</a>	<a href="#">OT.Authentication Secure</a>
<a href="#">FMT_MTD.1/CAPK</a>	<a href="#">OT.Authentication Secure</a>
<a href="#">FMT_MTD.1/KEY READ</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OT.AC Pers EAC</a> , <a href="#">OT.ADMIN Configuration</a>
<a href="#">FMT_MTD.1/Key Usage Counter</a>	<a href="#">OT.Key Usage Counter</a>
<a href="#">FMT_MTD.1/Initialize PIN</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OT.AC Pers EAC</a>
<a href="#">FMT_MTD.1/Resume PIN</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OT.AC Pers EAC</a>
<a href="#">FMT_MTD.1/Change PIN</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OT.AC Pers EAC</a>
<a href="#">FMT_MTD.1/Unblock PIN</a>	<a href="#">OT.SigF SigF</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.Lifecycle Management</a> , <a href="#">OT.AC Pers EAC</a>

<a href="#">FMT_MTD.1/UnblockChange_RAD</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.Sigy_SigF</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.Lifecycle Management</a> , <a href="#">OT.AC Pers EAC</a>
<a href="#">FMT_MTD.1/Erase_PIN</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.Lifecycle Management</a> , <a href="#">OT.AC Pers EAC</a>
<a href="#">FMT_MTD.1/Reinitialize_PIN</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OT.AC Pers EAC</a>
<a href="#">FMT_MTD.1/UnblockChange_PUK</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OT.AC Pers EAC</a>
<a href="#">FMT_MTD.1/TOE State</a>	<a href="#">OT.Lifecycle Management</a>
<a href="#">FMT_MTD.3</a>	<a href="#">OT.Authentication Secure</a>
<a href="#">FMT_MTD.1/INI_ENA</a>	<a href="#">OT.Identification</a> , <a href="#">OT.AC Pers EAC</a>
<a href="#">FMT_MTD.1/INI_DIS</a>	<a href="#">OT.Identification</a> , <a href="#">OT.AC Pers EAC</a>
<a href="#">FMT_LIM.1</a>	<a href="#">OT.Authentication Secure</a>
<a href="#">FMT_LIM.2</a>	<a href="#">OT.Authentication Secure</a>
<a href="#">FPT_EMS.1/PIN-PUK-KEYS</a>	<a href="#">OT.EMSEC Design</a> , <a href="#">OT.Authentication Secure</a> , <a href="#">OT.Keys Secrecy</a>
<a href="#">FTP_ITC.1/PACE</a>	<a href="#">OT.Authentication Secure</a> , <a href="#">OT.Tracing</a>

**Table 23 SFRs and Security Objectives**

### 9.3.3 Dependencies

#### 9.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
<a href="#">FCS_RND.1</a>	No Dependencies	
<a href="#">FCS_CKM.1/DH_PACE</a>	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	<a href="#">FCS_COP.1/SM in Confidentiality</a> , <a href="#">FCS_COP.1/SM in Integrity</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS_CKM.1/Session Keys</a>	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	<a href="#">FCS_COP.1/SM in Confidentiality</a> , <a href="#">FCS_COP.1/SM in Integrity</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS_COP.1/GP Secret Data Protection</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.1/Session Keys</a> , <a href="#">FCS_CKM.4</a>



<a href="#">FCS COP.1/SM in Confidentiality</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.1/Session Keys</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS COP.1/SM in Integrity</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.1/Session Keys</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS COP.1/Digital Auth</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.4</a> , <a href="#">FCS_CKM.1/SCD/SVD Generation</a>
<a href="#">FCS COP.1/Enc Key Decipherment</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.4</a> , <a href="#">FCS_CKM.1/SCD/SVD Generation</a>
<a href="#">FCS COP.1/SIG VER</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.4</a> , <a href="#">FCS_CKM.1/SCD/SVD Generation</a>
<a href="#">FDP ACC.1/TRM</a>	(FDP_ACF.1)	<a href="#">FDP_ACF.1/TRM</a>
<a href="#">FDP ACF.1/TRM</a>	(FDP_ACC.1) and (FMT_MSA.3)	<a href="#">FDP_ACC.1/TRM</a> , <a href="#">FMT_MSA.3</a>
<a href="#">FDP ACC.1/MNG File</a>	(FDP_ACF.1)	<a href="#">FDP_ACF.1/TRM</a>
<a href="#">FDP ACF.1/MNG File</a>	(FDP_ACC.1) and (FMT_MSA.3)	<a href="#">FDP_ACC.1/TRM</a> , <a href="#">FMT_MSA.3</a>
<a href="#">FDP UCT.1/TRM</a>	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	<a href="#">FDP_ACC.1/TRM</a> , <a href="#">FTP_ITC.1/PACE</a>
<a href="#">FDP UIT.1/TRM</a>	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	<a href="#">FDP_ACC.1/TRM</a> , <a href="#">FTP_ITC.1/PACE</a>
<a href="#">FIA UID.1/PACE</a>	No Dependencies	
<a href="#">FIA UAU.1/PACE</a>	(FIA_UID.1)	<a href="#">FIA_UID.1/PACE</a>
<a href="#">FIA UAU.4/PACE</a>	No Dependencies	
<a href="#">FIA UAU.5/PACE</a>	No Dependencies	
<a href="#">FIA UAU.6/PACE</a>	No Dependencies	
<a href="#">FIA UAU.6/EAC</a>	No Dependencies	

<a href="#">FIA AFL.1/AUTH</a>	(FIA_UAU.1)	<a href="#">FIA UAU.1/PACE</a>
<a href="#">FIA API.1/TOE Authentication</a>	No Dependencies	
<a href="#">FMT SMR.1/PACE</a>	(FIA_UID.1)	<a href="#">FIA UID.1/PACE</a>
<a href="#">FMT MTD.1/CVCA INI</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT SMF.1</a>
<a href="#">FMT MTD.1/CVCA UPD</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT SMF.1</a>
<a href="#">FMT MTD.1/DATE</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT SMF.1</a>
<a href="#">FMT MTD.1/CAPK</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT SMF.1</a>
<a href="#">FMT MTD.1/KEY READ</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT SMF.1</a>
<a href="#">FMT MTD.1/Key Usage Counter</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT SMF.1</a>
<a href="#">FMT MTD.1/Initialize PIN</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT SMF.1</a>
<a href="#">FMT MTD.1/Resume PIN</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT SMF.1</a>
<a href="#">FMT MTD.1/Change PIN</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT SMF.1</a>
<a href="#">FMT MTD.1/Unblock PIN</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT SMF.1</a>
<a href="#">FMT MTD.1/UnblockChange RAD</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT SMF.1</a>
<a href="#">FMT MTD.1/Erase PIN</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT SMF.1</a>
<a href="#">FMT MTD.1/Reinitialize PIN</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT SMF.1</a>
<a href="#">FMT MTD.1/UnblockChange PUK</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT SMF.1</a>
<a href="#">FMT MTD.1/TOE State</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT SMF.1</a>
<a href="#">FMT MTD.3</a>	(FMT_MTD.1)	<a href="#">FMT MTD.1/CVCA INI</a> , <a href="#">FMT MTD.1/CVCA UPD</a> , <a href="#">FMT MTD.1/DATE</a>
<a href="#">FMT MTD.1/INI ENA</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT SMR.1</a> , <a href="#">FMT SMF.1</a>

<a href="#">FMT_MTD.1/INI_DIS</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FMT_LIM.1</a>	(FMT_LIM.2)	<a href="#">FMT_LIM.2</a>
<a href="#">FMT_LIM.2</a>	(FMT_LIM.1)	<a href="#">FMT_LIM.1</a>
<a href="#">FPT_EMS.1/PIN-PUK-KEYS</a>	No Dependencies	
<a href="#">FTP_ITC.1/PACE</a>	No Dependencies	
<a href="#">FPT_EMS.1</a>	No Dependencies	
<a href="#">FPT_FLS.1</a>	No Dependencies	
<a href="#">FPT_PHP.1</a>	No Dependencies	
<a href="#">FPT_PHP.3</a>	No Dependencies	
<a href="#">FPT_TST.1</a>	No Dependencies	
<a href="#">FMT_SMR.1</a>	(FIA_UID.1)	<a href="#">FIA_UID.1</a>
<a href="#">FMT_SMF.1</a>	No Dependencies	
<a href="#">FMT_MOF.1</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FMT_MSA.1/Admin</a>	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FDP_ACC.1/Signature Creation</a> , <a href="#">FDP_ACC.1/SVD Transfer</a> , <a href="#">FDP_ACC.1/SCD/SVD Generation</a> , <a href="#">FDP_ACC.1/SCD Import</a>
<a href="#">FMT_MSA.1/Signatory</a>	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FDP_ACC.1/Signature Creation</a>
<a href="#">FMT_MSA.2</a>	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1</a> , <a href="#">FMT_MSA.1/Admin</a> , <a href="#">FMT_MSA.1/Signatory</a> , <a href="#">FDP_ACC.1/Signature Creation</a> , <a href="#">FDP_ACC.1/SCD/SVD Generation</a>
<a href="#">FMT_MSA.3</a>	(FMT_MSA.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1</a> , <a href="#">FMT_MSA.1/Admin</a> , <a href="#">FMT_MSA.1/Signatory</a>
<a href="#">FMT_MSA.4</a>	(FDP_ACC.1 or FDP_IFC.1)	<a href="#">FDP_ACC.1/Signature Creation</a> , <a href="#">FDP_ACC.1/SCD/SVD Generation</a>
<a href="#">FMT_MTD.1/Admin</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FMT_MTD.1/Signatory</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FIA_UID.1</a>	No Dependencies	
<a href="#">FIA_AFL.1/RAD</a>	(FIA_UAU.1)	<a href="#">FIA_UAU.1</a>

<a href="#">FIA_UAU.1</a>	(FIA_UID.1)	<a href="#">FIA_UID.1</a>
<a href="#">FDP_SDI.2/DTBS</a>	No Dependencies	
<a href="#">FDP_SDI.2/Persistent</a>	No Dependencies	
<a href="#">FDP_RIP.1</a>	No Dependencies	
<a href="#">FDP_ACC.1/Signature Creation</a>	(FDP_ACF.1)	<a href="#">FDP_ACF.1/Signature Creation</a>
<a href="#">FDP_ACF.1/Signature Creation</a>	(FDP_ACC.1) and (FMT_MSA.3)	<a href="#">FMT_MSA.3</a> , <a href="#">FDP_ACC.1/Signature Creation</a>
<a href="#">FCS_COP.1/Sign</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.4</a> , <a href="#">FCS_CKM.1/SCD/SVD Generation</a> , <a href="#">FDP_ITC.1/SCD</a>
<a href="#">FCS_CKM.4</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	<a href="#">FCS_CKM.1/SCD/SVD Generation</a> , <a href="#">FDP_ITC.1/SCD</a>
<a href="#">FCS_CKM.1/SCD/SVD Generation</a>	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	<a href="#">FCS_COP.1/Sign</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FDP_ACC.1/SVD Transfer</a>	(FDP_ACF.1)	<a href="#">FDP_ACF.1/SVD Transfer</a>
<a href="#">FDP_ACF.1/SVD Transfer</a>	(FDP_ACC.1) and (FMT_MSA.3)	<a href="#">FMT_MSA.3</a> , <a href="#">FDP_ACC.1/SVD Transfer</a>
<a href="#">FDP_ACC.1/SCD/SVD Generation</a>	(FDP_ACF.1)	<a href="#">FDP_ACF.1/SCD/SVD Generation</a>
<a href="#">FDP_ACF.1/SCD/SVD Generation</a>	(FDP_ACC.1) and (FMT_MSA.3)	<a href="#">FMT_MSA.3</a> , <a href="#">FDP_ACC.1/SCD/SVD Generation</a>
<a href="#">FTP_ITC.1/SCD</a>	No Dependencies	
<a href="#">FDP_UCT.1/SCD</a>	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	<a href="#">FTP_ITC.1/SCD</a> , <a href="#">FDP_ACC.1/SCD Import</a>
<a href="#">FDP_ITC.1/SCD</a>	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	<a href="#">FMT_MSA.3</a> , <a href="#">FDP_ACC.1/SCD Import</a>
<a href="#">FDP_ACC.1/SCD Import</a>	(FDP_ACF.1)	<a href="#">FDP_ACF.1/SCD Import</a>
<a href="#">FDP_ACF.1/SCD Import</a>	(FDP_ACC.1) and (FMT_MSA.3)	<a href="#">FMT_MSA.3</a> , <a href="#">FDP_ACC.1/SCD Import</a>
<a href="#">FTP_ITC.1/SVD</a>	No Dependencies	
<a href="#">FDP_DAU.2/SVD</a>	(FIA_UID.1)	<a href="#">FIA_UID.1</a>
<a href="#">FIA_API.1</a>	No Dependencies	

<a href="#">FDP UIT.1/DTBS</a>	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	<a href="#">FDP ACC.1/Signature Creation, FTP ITC.1/DTBS</a>
<a href="#">FTP ITC.1/VAD</a>	No Dependencies	
<a href="#">FTP ITC.1/DTBS</a>	No Dependencies	

**Table 24 SFRs Dependencies**

### 9.3.3.2 SARs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
<a href="#">ADV ARC.1</a>	(ADV_FSP.1) and (ADV_TDS.1)	<a href="#">ADV FSP.5</a> , <a href="#">ADV TDS.4</a>
<a href="#">ADV FSP.5</a>	(ADV_IMP.1) and (ADV_TDS.1)	<a href="#">ADV IMP.1</a> , <a href="#">ADV TDS.4</a>
<a href="#">ADV IMP.1</a>	(ADV_TDS.3) and (ALC_TAT.1)	<a href="#">ADV TDS.4</a> , <a href="#">ALC TAT.2</a>
<a href="#">ADV TDS.4</a>	(ADV_FSP.5)	<a href="#">ADV FSP.5</a>
<a href="#">ADV INT.2</a>	(ADV_IMP.1) and (ADV_TDS.3) and (ALC_TAT.1)	<a href="#">ADV IMP.1</a> , <a href="#">ADV TDS.4</a> , <a href="#">ALC TAT.2</a>
<a href="#">AGD OPE.1</a>	(ADV_FSP.1)	<a href="#">ADV FSP.5</a>
<a href="#">AGD PRE.1</a>	No Dependencies	
<a href="#">ALC CMC.4</a>	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	<a href="#">ALC CMS.5</a> , <a href="#">ALC DVS.2</a> , <a href="#">ALC LCD.1</a>
<a href="#">ALC CMS.5</a>	No Dependencies	
<a href="#">ALC DEL.1</a>	No Dependencies	
<a href="#">ALC DVS.2</a>	No Dependencies	
<a href="#">ALC FLR.1</a>	No Dependencies	
<a href="#">ALC LCD.1</a>	No Dependencies	
<a href="#">ALC TAT.2</a>	(ADV_IMP.1)	<a href="#">ADV IMP.1</a>
<a href="#">ASE CCL.1</a>	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	<a href="#">ASE ECD.1</a> , <a href="#">ASE INT.1</a> , <a href="#">ASE REQ.2</a>
<a href="#">ASE ECD.1</a>	No Dependencies	
<a href="#">ASE INT.1</a>	No Dependencies	
<a href="#">ASE OBJ.2</a>	(ASE_SPD.1)	<a href="#">ASE SPD.1</a>
<a href="#">ASE REQ.2</a>	(ASE_ECD.1) and (ASE_OBJ.2)	<a href="#">ASE ECD.1</a> , <a href="#">ASE OBJ.2</a>
<a href="#">ASE SPD.1</a>	No Dependencies	
<a href="#">ASE TSS.1</a>	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	<a href="#">ADV FSP.5</a> , <a href="#">ASE INT.1</a> , <a href="#">ASE REQ.2</a>

<a href="#">ATE_COV.2</a>	(ADV_FSP.2) and (ATE_FUN.1)	<a href="#">ADV_FSP.5</a> , <a href="#">ATE_FUN.1</a>
<a href="#">ATE_DPT.3</a>	(ADV_ARC.1) and (ADV_TDS.4) and (ATE_FUN.1)	<a href="#">ADV_ARC.1</a> , <a href="#">ADV_TDS.4</a> , <a href="#">ATE_FUN.1</a>
<a href="#">ATE_FUN.1</a>	(ATE_COV.1)	<a href="#">ATE_COV.2</a>
<a href="#">ATE_IND.2</a>	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	<a href="#">ADV_FSP.5</a> , <a href="#">AGD_OPE.1</a> , <a href="#">AGD_PRE.1</a> , <a href="#">ATE_COV.2</a> , <a href="#">ATE_FUN.1</a>
<a href="#">AVA_VAN.5</a>	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	<a href="#">ADV_ARC.1</a> , <a href="#">ADV_FSP.5</a> , <a href="#">ADV_IMP.1</a> , <a href="#">ADV_TDS.4</a> , <a href="#">AGD_OPE.1</a> , <a href="#">AGD_PRE.1</a> , <a href="#">ATE_DPT.3</a>

**Table 25 SARs Dependencies**

### 9.3.4 Rationale for the Security Assurance Requirements

The assurance level for this Security Target is EAL5 augmented. EAL5 allows a developer to attain a reasonably high assurance level without the need for highly specialised 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, EAL5 is appropriate for commercial products that can be applied to moderate to high security functions. Augmentation results from the selection of:

AVA\_VAN.5 Advanced methodical vulnerability analysis  
 ALC\_DVS.2 Sufficiency of security measures  
 ALC\_FLR.1 Basic flaw remediation

### 9.3.5 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 applications, i.e. the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. Insecure states shall be easy to detect and the TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD\_Secrecy, OT.Sigy\_SigF, OT.Sig\_Secure and OT.Keys\_Secrecy. This assurance requirement is achieved by the AVA\_VAN.5 component. Independent vulnerability analysis is based on highly detailed technical information. The attacker is assumed to be thoroughly familiar with the specific implementation of the TOE. The attacker is presumed to have a high level of technical sophistication.

### 9.3.6 ALC\_DVS.2 Sufficiency of security measures

In order to protect the TOE on development Phase, the component ALC\_DVS.2 was added. This latter requires security documentation justifying that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

### **9.3.7 ALC\_FLR.1 Basic flaw remediation**

The flaw remediation assurance improves a rigorous management for updating the TOE in the context of sensible market.

## 10 TOE Summary Specification

---

### 10.1 TOE Summary Specification

This section provides a summary of the security functions implemented by the TOE in order to fulfil the security functional requirements. The summary is structured in security functions. The security functionalities concerning the IC and the JC Platform are described in [ST\_PTF] and are not redefined in this security target, although they must be considered for the TOE.

The TOE inherits all the security functions provided by the underlying javacard open platform [ST\_PTF]. On top of these, it adds some supplemental security functions that are described hereafter.

#### **SF.PIN\_MGT**

This security function is involved in the management of the PINs (PIN, PUK and RAD). PINs are secret data used so that a natural person can authenticate itself to the TOE. This security function:

- o Provides all management operations on these PINs (verification, change, unblocking, unblocking and change, initialization, re-initialization) and
- o Enforces the access control policies over these operations. The natural person can authenticate itself to the TOE via the PACE protocol and/or the VERIFY PIN command. Take note that the usage of PACE protocol is mandatory only for contactless mode unless compliance to PP-SSCD5 and/or PP-SSCD6 is required, then usage of PACE protocol becomes mandatory for both contact and contactless mode. The verification process uses a velocity checking mechanism, thus a remaining try counter and a maximum error counter are defined for each PIN. If the verification fails, the try counter is decremented by one and an error status that contains the remaining attempts is returned by the application. When all available tries have failed, the PIN is suspended or blocked and can no longer be used. Note that a successful verification of the PIN resets its remaining try counter to the maximum error counter.

#### **SF.SIG**

This security function manages the signature creation service.

It enforces access control over the signature creation service:

- o In phase 6, it ensures the signature computation function is not accessible, and in particular that the personalization agent cannot sign on behalf of the Signatory.
- o In phase 7, it ensures the signature creation feature is activated only by the signatory. Also it enforces the integrity of DTBS, and ensures that R.Sigy is successfully authenticated before creating the signature.

The security function ensures the data hashing (if hash on card, or partial hashing is used), and the secure signature computation using the private key (SCD), either with RSA or EC-DSA cryptography. This security function relies on SF.PIN\_MGT to authenticate the Signatory.



## SF.AUTH

This security function manages the authentication protocols supported by the TOE. This security function supports the authentication with the personalization agent in phase 6. This authentication relies on a mutual authentication protocol authenticating

- o the TOE to the personalization agent, and
- o the personalization agent to the TOE. It relies on symmetric master key sets shared by the TOE and the personalization agent that may be DES or AES symmetric keys (depending on the type of Secure Channel Protocol – SCP). Upon successful completion of the authentication, both parties (TOE and personalization agent) generate session keys that may be used to establish a secure channel thanks to SF.SM. This secure channel allows protecting the communication between them in integrity, authenticity and confidentiality. Each symmetric master key sets is associated to an error counter, which aims at ensuring its protecting against brute force attacks. Upon each wrong authentication attempt, the authentication processing time is slowed down (exponentially). Once a successful authentication takes place, the slow down mechanisms is cancelled. In phase 7, this security function also supports the PACE protocol. This protocol is a human to machine authentication protocol allowing to
  - o authenticate a natural person to the TOE by using a PIN or
  - o prove the holder has the TOE in hand (using MRZ or CAN) and
  - o creating a secure channel between the TOE and a device used to initiate the communication. This protocol is designed to protect the secrecy of the PIN in the course of the authentication so that it can't be intercepted during the communication, or deduced through crypto analysis. Upon successful completion of PACE authentication, session keys used to establish a secure channel thanks to SF.SM are generated. This secure function also manage error counter on the credentials used to perform the authentication.
  - o Upon failure, the error counter of the credentials used to initiate the PACE authentication is decreased until it is blocked.
  - o Once blocked, a secret credential (PINs) can't be used anymore to perform a PACE protocol, while for MRZ or CAN, the PACE protocol is slowed down.
  - o Upon successful PACE authentication, the error counter of the credentials used to initiate the PACE authentication is reset to its maximum value; Last but not least, this security function also handles the suspension mechanisms protecting the PINs against Denial Of services attacks (not applicable to MRZ and CAN). When the remaining number of tries is set to '1', any attempt to perform a PACE authentication using a PIN credential will require it to be made through a secure channel generated using PACE authentication performed using the CAN.

The PACE protocol is used to establish a trusted channel with the SCA.

In phase 7, this security function also supports authentication of a natural person to the TOE by using a PIN or biometry based credential through the VERIFY command.

In phase 7, this security function also supports the Extended Access Control protocol (EAC) made up with Chip authentication (CA) and Terminal Authentication (TA). This protocol allows

- o a mutual authentication between the TOE and a remote terminal, and

- o the generation of session keys used to establish a secure channel thanks to SF.SM. This secure channel protects the communication between them in integrity, authenticity and confidentiality. This authentication is based on PKI scheme: each party (TOE and remote terminal) uses
- o an authentication private key and
- o digital certificates containing the corresponding authentication public key and linking it to the root of trust known by the other party, to authenticate itself to the other party. This security function manages the verification and processing of the certificates received from the remote terminal (that have a specific format named Card Verifiable Certificate – CVC). In particular, this security function computes the effective authorization of the remote terminal. The Extended Access Control (EAC) protocol or GP Authentication is used to establish a trusted channel with the CGA prior to SCD/SVD generation. In phase 7, this security function also provides mechanisms to authenticate the SSCD and prove its identity (thanks to the Chip Authentication mechanism described above).

### **SF.SM**

This security function ensures the protection of communication between the TOE and an external entity. As such, this security function maintains a trusted channel between the TOE and an external entity. This security function requires the TOE and the external entity to establish first a trusted channel using an authentication supported by SF.AUTH. This security function ensures the following properties:

- o In phase 6, it ensures the confidentiality, integrity and authenticity of the private keys (including the SCD), and the PINs (including the RAD);
- o In phase 6, it ensures the integrity and authenticity of the asymmetric public key (including the SVD) when being exported to the outside
- o In phase 7, it ensures the confidentiality, integrity and authenticity of communication between the TOE and the external entity with which an authentication was performed; In phase 6, the confidentiality, integrity and authenticity of communication is ensured by symmetric cryptography. Sensitive data (such as SCD or PINs) are encrypted using a dedicated symmetric session keys for data encryption generated from the seed agreed during the authentication with the personalization agent (see SF.AUTH). On top of that, data are encrypted and signed using symmetric session keys generated from the seed agreed during the authentication with the personalization agent (see SF.AUTH). In phase 7, the confidentiality, integrity and authenticity of communication is ensured by symmetric cryptography. Data are encrypted and signed using symmetric session keys generated from the seed agreed during the Extended Access Control (EAC) or PACE protocol (see SF.AUTH). Moreover, the protection against replay attacks is ensured by the Message Authentication Code (MAC) which is computed using a dynamic ICV, incremented at each new command. This security function is also in charge of:
- o generating the session keys from the seed computed by SF.AUTH. These session keys are ephemeral and unique, as the seed is computed from random numbers generated by the TOE and the external entity.
- o destroying the session keys in case an error is detected (data not authentic or not integer), or when a command in plain text is sent.

- o providing CGA the ability to verify evidence of the validity of the SVD and the identity of the user that generated the evidence. This security function supports SF.AUTH to prove the identity of the SSCD and the TOE holder.

### **SF.KEY\_MGT**

This security function is involved in the management of the asymmetric keys (including SCDs and SVDs). It enforces access control over any management operation on the keys:

- o In phase 6, it only allows the key (including the SCD) to be loaded, generated and exported (for the public keys) by the personalization agent. It also requires the private keys to be encrypted in order to ensure their confidentiality. This security function ensures the personalization agent (1) can't use the keys it has loaded or generated. and (2) can't impersonate the associated role (in case of authentication keys), or create a signature with the SCD;
- o In phase 7, it allows managing all the keys (including the SCD) by providing generation and export of the corresponding public key. It also enforces access control policies on these operations.

This security function also ensures that after update or generation, the former key (including SCD and SVD) is securely destroyed.

### **SF.CONF**

This security function manages the configuration of the TOE in phase 6. For instance it allows the modification of the TOE State in phase 6. This security function ensures an access control over these operations. Only the successfully authenticated Personalization Agent can modify these attributes. This security function relies on SF.AUTH to authenticate the personalization agent.

### **SF.ESERVICE**

This security function enables to perform digital authentication and electronic services. It is active in phase 7. This security function offers the following services:

- o Digital authentication;
- o Decryption key decipherment; This security function relies on SF.KEY\_MGT which provides management of the keys on which these services rely.

### **SF.SAFESTATE\_MGT**

This security function ensures the TOE is always in a safe state. It monitors the integrity of the TOE, its assets and the TSF data by performing self-tests. When an unexpected event occurs (loss of power, loss of integrity, tearing,...), it ensures

- o the TOE returns in a safe state
- o all sensitive data are erased
- o the TOE returns in a restrictive secure state When a major issue is detected, the security function ensures the destruction of the TOE, so that the assets are not accessible anymore.

**SF.PHYS**

This security function protects the TOE against physical attacks, so that the integrity and confidentiality of the TOE is ensured, including keys, user data, PLC data, configuration data and TOE life cycle. It detects physical tampering, responds automatically and also controls the emanations sent out by the TOE. It furthermore prevents deploying test features after TOE delivery.

**SF.ADMIN**

This security functionality ensures that the TOE, when delivered to the Administration Agent, provides and requires authentication for data exchange.

## 10.2 SFRs and TSS

### 10.2.1 SFRs and TSS - Rationale

#### All SSCD parts

##### *Protection of the TSF (FPT)*

**FPT\_EMS.1** is met by SF.PHYS

**FPT\_FLS.1** is met by SF.SAFESTATE\_MGT

**FPT\_PHP.1** is met by SF.PHYS

**FPT\_PHP.3** is met by SF.PHYS

**FPT\_TST.1** is met by SF.SAFESTATE\_MGT

##### *Security management (FMT)*

**FMT\_SMR.1** is met by SF.PIN\_MGT and SF.AUTH

**FMT\_SMF.1** is met by SF.PIN\_MGT, SF.SIG, SF.AUTH, SF.KEY\_MGT and SF.CONF

**FMT\_MOF.1** is met by SF.SIG

**FMT\_MSA.1/Admin** is met by SF.AUTH

**FMT\_MSA.1/Signatory** is met by SF.SIG

**FMT\_MSA.2** is met by SF.SIG, SF.AUTH, SF.KEY\_MGT and SF.CONF

**FMT\_MSA.3** is met by SF.SIG, SF.AUTH, SF.KEY\_MGT and SF.CONF

**FMT\_MSA.4** is met by SF.SIG, SF.AUTH and SF.KEY\_MGT

**FMT\_MTD.1/Admin** is met by SF.ADMIN

**FMT\_MTD.1/Signatory** is met by SF.PIN\_MGT

##### *Identification and authentication (FIA)*

**FIA\_UID.1** is met by SF.PIN\_MGT, SF.SIG, SF.AUTH and SF.KEY\_MGT

**FIA\_AFL.1/RAD** is met by SF.PIN\_MGT

**FIA\_UAU.1** is met by SF.PIN\_MGT, SF.SIG, SF.AUTH and SF.KEY\_MGT

*User data protection (FDP)*

**FDP\_SDI.2/DTBS** is met by SF.SIG and SF.SAFESTATE\_MGT

**FDP\_SDI.2/Persistent** is met by SF.SAFESTATE\_MGT

**FDP\_RIP.1** is met by SF.SAFESTATE\_MGT

**FDP\_ACC.1/Signature\_Creation** is met by SF.SIG

**FDP\_ACF.1/Signature\_Creation** is met by SF.SIG

*Cryptographic support (FCS)*

**FCS\_COP.1/Sign** is met by SF.SIG

**FCS\_CKM.4** is met by SF.KEY\_MGT

**SSCD parts 2, 4 and 5 only**

*Cryptographic support (FCS)*

**FCS\_CKM.1/SCD/SVD\_Generation** is met by SF.KEY\_MGT

*User data protection (FDP)*

**FDP\_ACC.1/SVD\_Transfer** is met by SF.KEY\_MGT

**FDP\_ACF.1/SVD\_Transfer** is met by SF.KEY\_MGT

**FDP\_ACC.1/SCD/SVD\_Generation** is met by SF.KEY\_MGT

**FDP\_ACF.1/SCD/SVD\_Generation** is met by SF.KEY\_MGT

**SSCD parts 3 and 6 only**

*Trusted path/channels (FTP)*

**FTP\_ITC.1/SCD** is met by SF.AUTH and SF.SM

*User data protection (FDP)*

**FDP\_UCT.1/SCD** is met by SF.SM

**FDP\_ITC.1/SCD** is met by SF.KEY\_MGT

**FDP\_ACC.1/SCD\_Import** is met by SF.KEY\_MGT

**FDP\_ACF.1/SCD\_Import** is met by SF.KEY\_MGT

**SSCD part 4 only**

*Trusted path/channels (FTP)*

**FTP\_ITC.1/SVD** is met by SF.AUTH and SF.SM

*User data protection (FDP)*

**FDP\_DAU.2/SVD** is met by SF.SM

*Identification and authentication (FIA)*

**FIA\_API.1** is met by SF.AUTH and SF.SM

**SSCD parts 5 and 6 only**

*User data protection (FDP)*

**FDP\_UIT.1/DTBS** is met by SF.SIG

*Trusted path/channels (FTP)*

**FTP\_ITC.1/VAD** is met by SF.PIN\_MGT

**FTP\_ITC.1/DTBS** is met by SF.SM

**Additional SFRs**

**FCS\_RND.1** is met by SF.AUTH

**FCS\_CKM.1/DH\_PACE** is met by SF.AUTH

**FCS\_CKM.1/Session Keys** is met by SF.SM



**FCS\_COP.1/GP Secret Data Protection** is met by SF.AUTH and SF.SM

**FCS\_COP.1/SM in Confidentiality** is met by SF.AUTH and SF.SM

**FCS\_COP.1/SM in Integrity** is met by SF.AUTH and SF.SM

**FCS\_COP.1/Digital Auth** is met by SF.ESERVICE

**FCS\_COP.1/Enc Key Decipherment** is met by SF.ESERVICE

**FCS\_COP.1/SIG\_VER** is met by SF.AUTH and SF.SM

**FDP\_ACC.1/TRM** is met by SF.AUTH and SF.SM

**FDP\_ACF.1/TRM** is met by SF.AUTH and SF.SM

**FDP\_ACC.1/MNG\_File** is met by SF.AUTH and SF.SM

**FDP\_ACF.1/MNG\_File** is met by SF.AUTH and SF.SM

**FDP\_UCT.1/TRM** is met by SF.AUTH, SF.SM and SF.KEY\_MGT

**FDP\_UIT.1/TRM** is met by SF.SM and SF.KEY\_MGT

**FIA\_UID.1/PACE** is met by SF.PIN\_MGT, SF.AUTH and SF.SM

**FIA\_UAU.1/PACE** is met by SF.PIN\_MGT, SF.AUTH and SF.SM

**FIA\_UAU.4/PACE** is met by SF.PIN\_MGT, SF.AUTH and SF.SM

**FIA\_UAU.5/PACE** is met by SF.PIN\_MGT, SF.AUTH and SF.SM

**FIA\_UAU.6/PACE** is met by SF.AUTH and SF.SM

**FIA\_UAU.6/EAC** is met by SF.AUTH and SF.SM

**FIA\_AFL.1/AUTH** is met by SF.PIN\_MGT, SF.AUTH and SF.SM

**FIA\_API.1/TOE Authentication** is met by SF.AUTH and SF.SM

**FMT\_SMR.1/PACE** is met by SF.PIN\_MGT and SF.AUTH



**FMT\_MTD.1/CVCA\_INI** is met by SF.AUTH

**FMT\_MTD.1/CVCA\_UPD** is met by SF.AUTH

**FMT\_MTD.1/DATE** is met by SF.AUTH

**FMT\_MTD.1/CAPK** is met by SF.AUTH

**FMT\_MTD.1/KEY\_READ** is met by SF.AUTH

**FMT\_MTD.1/Key\_Usage\_Counter** is met by SF.KEY\_MGT

**FMT\_MTD.1/Initialize\_PIN** is met by SF.PIN\_MGT

**FMT\_MTD.1/Resume\_PIN** is met by SF.PIN\_MGT

**FMT\_MTD.1/Change\_PIN** is met by SF.PIN\_MGT

**FMT\_MTD.1/Unblock\_PIN** is met by SF.PIN\_MGT

**FMT\_MTD.1/UnblockChange\_RAD** is met by SF.PIN\_MGT

**FMT\_MTD.1/Erase\_PIN** is met by SF.PIN\_MGT

**FMT\_MTD.1/Reinitialize\_PIN** is met by SF.PIN\_MGT

**FMT\_MTD.1/UnblockChange\_PUK** is met by SF.PIN\_MGT

**FMT\_MTD.1/TOE State** is met by SF.CONF

**FMT\_MTD.3** is met by SF.PIN\_MGT and SF.AUTH

**FMT\_MTD.1/INI\_ENA**

- o is met by SF.AUTH that provides the authentication protocol.

**FMT\_MTD.1/INI\_DIS**

- o is met by SF.AUTH that provides the authentication protocol.

**FMT\_LIM.1** is met by SF.PHYS

**FMT\_LIM.2** is met by SF.PHYS

**FPT\_EMS.1/PIN-PUK-KEYS** is met by SF.PHYS

**FTP\_ITC.1/PACE** is met by SF.PIN\_MGT, SF.AUTH and SF.SM

### 10.2.1.1 TOE Summary Specification

**SF.PIN\_MGT** The implementation of this security function contributes to:

- o FIA\_UID.1, FIA\_UAU.1, FIA\_UID.1/PACE, FIA\_UAU.1/PACE, FIA\_UAU.4/PACE, FIA\_UAU.5/PACE that provide user identification and user authentication prior to enabling access to authorized functions.
- o FIA\_AFL.1/RAD, FIA\_AFL.1/AUTH that handle the authentication failure.
- o FMT\_SMR.1, FMT\_SMR.1/PACE that define security roles for the TOE.
- o FMT\_SMF.1.
- o FTP\_ITC.1/PACE that ensures a trusted channel between them TOE and a PACE terminal to protect the exchanged data in contactless from modification and disclosure.
- o FMT\_MTD.1/Admin, FMT\_MTD.1/Signatory, FMT\_MTD.1.1/Initialize\_PIN, FMT\_MTD.1.1/Resume\_PIN, FMT\_MTD.1/Change\_PIN, FMT\_MTD.1/Unblock\_PIN, FMT\_MTD.1.1/UnblockChange\_RAD, FMT\_MTD.1.1/Erase\_PIN, FMT\_MTD.1.1/Reinitialize\_PIN, FMT\_MTD.1.1/UnblockChange\_PUK, FMT\_MTD.3 that manage the TSFs date by defining access rules.

**SF.SIG** The implementation of this security function contributes to:

- o FCS\_COP.1/Sign that provide cryptographic operations.
- o FDP\_ACC.1/Signature\_Creation, FDP\_ACF.1/Signature\_Creation that enforce the signature creation SFP.
- o FIA\_UID.1, FIA\_UAU.1 that provide user identification and user authentication prior to enabling access to authorized functions.
- o FMT\_MSA.1/Signatory, FMT\_MSA.2, FMT\_MSA.3, FMT\_MSA.4 that manages the access right policy of the TOE.
- o FMT\_MOF.1 that ensures the management of the signature creation function.
- o FMT\_SMF.1.
- o FDP\_SDI.2/DTBS that ensures the integrity of DTBS.

**SF.AUTH** The implementation of this security function contributes to:

- o FCS\_CKM.1.1/DH\_PACE that ensures cryptographic key generation.
- o FCS\_COP.1/SM in confidentiality, FCS\_COP.1/SM in integrity, FCS\_COP.1/GP secret data protection, FCS\_RND.1, FCS\_COP.1.1/SIG\_VER that provide cryptographic operations.
- o FIA\_API.1, FIA\_API.1/TOE Authentication

- o FMT\_SMR.1, FMT\_SMR.1/PACE that define security roles for the TOE.
- o FMT\_SMF.1
- o FMT\_MSA.1/Admin, FMT\_MSA.2, FMT\_MSA.3, FMT\_MSA.4 that manages the access right policy of the TOE.
- o FTP\_ITC.1/SCD, FTP\_ITC.1/SVD, FTP\_ITC.1/PACE that ensure a trusted channel between them TOE and a Terminal to protect the exchanged data from modification and disclosure.
- o FIA\_UID.1, FIA\_UAU.1, FIA\_UID.1/PACE, FIA\_UAU.1/PACE, FIA\_UAU.4/PACE, FIA\_UAU.5/PACE, FIA\_UAU.6/PACE, FIA\_UAU.6/EAC that provide user identification and user authentication prior to enabling access to authorized functions.
- o FIA\_AFL.1/AUTH that handles the authentication failure.
- o FDP\_ACC.1/TRM, FDP\_ACF.1/TRM that ensure that only an authorized user under specific conditions can perform a dedicated operation, and in particular, that only users authenticated as authenticated terminal.
- o FDP\_UCT.1/TRM that ensures data exchange confidentiality.
- o FMT\_MTD.1.1/CVCA\_INI, FMT\_MTD.1.1/CVCA\_UPD, FMT\_MTD.1.1/DATE, FMT\_MTD.1.1/CAPK, FMT\_MTD.1.1/KEY\_READ, FMT\_MTD.3 that manage the TSFs date by defining access rules.

**SF.SM** The implementation of this security function contributes to:

- o FCS\_CKM.1/Session Keys that ensure cryptographic key generation.
- o FCS\_COP.1/SM in confidentiality, FCS\_COP.1/SM in integrity, FCS\_COP.1/GP secret data protection, FCS\_COP.1.1/SIG\_VER that provide cryptographic operations.
- o FDP\_DAU.2/SVD that ensures that exported SVD to the CGA is authenticated and unmodified.
- o FIA\_API.1, FIA\_API.1/TOE Authentication.
- o FTP\_ITC.1/SCD, FTP\_ITC.1/SVD, FTP\_ITC.1/PACE that ensure a trusted channel between them TOE and a Terminal to protect the exchanged data from modification and disclosure.
- o FIA\_UID.1/PACE, FIA\_UAU.1/PACE, FIA\_UAU.4/PACE, FIA\_UAU.5/PACE, FIA\_UAU.6/PACE, FIA\_UAU.6/EAC that provide user identification and user authentication prior to enabling access to authorized functions.
- o FIA\_AFL.1/AUTH.
- o FDP\_ACC.1/TRM, FDP\_ACF.1/TRM that ensure that only an authorized user under specific conditions can perform a dedicated operation, and in particular, that only users authenticated as authenticated terminal.
- o FDP\_UCT.1/SCD, FDP\_UCT.1/TRM that ensures data exchange confidentiality.
- o FDP\_UIT.1/TRM that ensures data exchange integrity.

**SF.KEY\_MGT** The implementation of this security function contributes to:

- o FCS\_CKM.1/SCD/SVD\_Generation that ensures cryptographic key generation.
- o FCS\_CKM.4 that manages that ensure cryptographic key destruction.
- o FDP\_ACC.1/SCD/SVD\_Generation, FDP\_ACF.1/SCD/SVD\_Generation, FDP\_ACC.1/SVD\_Transfer,

FDP\_ACF.1/SVD\_Transfer, FDP\_ACC.1/SCD\_Import, FDP\_ACF.1/SCD\_Import that ensure that only an authorized user under specific conditions can perform a dedicated operation, and in particular, that only users authenticated as administrator or signatory.

- o FDP\_ITC.1/SCD that ensures a trusted channel between them TOE and a Terminal to protect the exchanged data from modification and disclosure.
- o FIA\_UID.1, FIA\_UAU.1 that provide user identification and user authentication prior to enabling access to authorized functions.
- o FMT\_SMF.1.
- o FMT\_MSA.2, FMT\_MSA.3, FMT\_MSA.4 that manage the access right policy of the TOE.
- o FDP\_UCT.1/TRM that ensures data exchange confidentiality.
- o FDP\_UIT.1/TRM that ensures data exchange integrity.

**SF.CONF** The implementation of this security function contributes to:

- o FMT\_SMF.1.
- o FMT\_MSA.2, FMT\_MSA.3 that manage the access right policy of the TOE.
- o FMT\_MTD.1/TOE\_State that restrict the ability to switch the TOE from phase 6 to phase 7 to the personalization agent.

**SF.ESERVICE** The implementation of this security function contributes to:

- o FCS\_COP.1/Digital Auth, FCS\_COP.1/Enc Key Decipherment that provide cryptographic operations.

**SF.SAFESTATE\_MGT** The implementation of this security function contributes to:

- o FDP\_RIP.1 that ensures erasure of data in FLASH and in RAM.
- o FDP\_SDI.2/Persistent, FDP\_SDI.2/DTBS that ensure the integrity of data stored in the TOE.
- o FPT\_FLS.1 that ensure the preservation of secure state when failures occur.
- o FPT\_TST.1 that ensures the integrity of the data stored on the TOE.

**SF.PHYS** The implementation of this security function contributes to:

- o FPT\_EMS.1, FPT\_EMS.1/PIN-PUK-KEYS that ensure the TOE emanation.
- o FPT\_PHP.1, FPT\_PHP.3 that ensures the detection of physical tampering of the TOE and the resistance to it.
- o FMT\_LIM.1, FMT\_LIM.2.

### 10.2.2 Association tables of SFRs and TSS

Security Functional Requirements	TOE Summary Specification
<a href="#">FPT_EMS.1</a>	<a href="#">SF.PHYS</a>
<a href="#">FPT_FLS.1</a>	<a href="#">SF.SAFESTATE_MGT</a>

<a href="#">FPT_PHP.1</a>	<a href="#">SF.PHYS</a>
<a href="#">FPT_PHP.3</a>	<a href="#">SF.PHYS</a>
<a href="#">FPT_TST.1</a>	<a href="#">SF.SAFESTATE_MGT</a>
<a href="#">FMT_SMR.1</a>	<a href="#">SF.PIN_MGT</a> , <a href="#">SF.AUTH</a>
<a href="#">FMT_SMF.1</a>	<a href="#">SF.PIN_MGT</a> , <a href="#">SF.SIG</a> , <a href="#">SF.AUTH</a> , <a href="#">SF.KEY_MGT</a> , <a href="#">SF.CONF</a>
<a href="#">FMT_MOF.1</a>	<a href="#">SF.SIG</a>
<a href="#">FMT_MSA.1/Admin</a>	<a href="#">SF.AUTH</a>
<a href="#">FMT_MSA.1/Signatory</a>	<a href="#">SF.SIG</a>
<a href="#">FMT_MSA.2</a>	<a href="#">SF.SIG</a> , <a href="#">SF.AUTH</a> , <a href="#">SF.KEY_MGT</a> , <a href="#">SF.CONF</a>
<a href="#">FMT_MSA.3</a>	<a href="#">SF.SIG</a> , <a href="#">SF.AUTH</a> , <a href="#">SF.KEY_MGT</a> , <a href="#">SF.CONF</a>
<a href="#">FMT_MSA.4</a>	<a href="#">SF.SIG</a> , <a href="#">SF.AUTH</a> , <a href="#">SF.KEY_MGT</a>
<a href="#">FMT_MTD.1/Admin</a>	<a href="#">SF.ADMIN</a>
<a href="#">FMT_MTD.1/Signatory</a>	<a href="#">SF.PIN_MGT</a>
<a href="#">FIA_UID.1</a>	<a href="#">SF.PIN_MGT</a> , <a href="#">SF.SIG</a> , <a href="#">SF.AUTH</a> , <a href="#">SF.KEY_MGT</a>
<a href="#">FIA_AFL.1/RAD</a>	<a href="#">SF.PIN_MGT</a>
<a href="#">FIA_UAU.1</a>	<a href="#">SF.PIN_MGT</a> , <a href="#">SF.SIG</a> , <a href="#">SF.AUTH</a> , <a href="#">SF.KEY_MGT</a>
<a href="#">FDP_SDI.2/DTBS</a>	<a href="#">SF.SIG</a> , <a href="#">SF.SAFESTATE_MGT</a>
<a href="#">FDP_SDI.2/Persistent</a>	<a href="#">SF.SAFESTATE_MGT</a>
<a href="#">FDP_RIP.1</a>	<a href="#">SF.SAFESTATE_MGT</a>
<a href="#">FDP_ACC.1/Signature_Creation</a>	<a href="#">SF.SIG</a>
<a href="#">FDP_ACF.1/Signature_Creation</a>	<a href="#">SF.SIG</a>
<a href="#">FCS_COP.1/Sign</a>	<a href="#">SF.SIG</a>
<a href="#">FCS_CKM.4</a>	<a href="#">SF.KEY_MGT</a>
<a href="#">FCS_CKM.1/SCD/SVD_Generation</a>	<a href="#">SF.KEY_MGT</a>
<a href="#">FDP_ACC.1/SVD_Transfer</a>	<a href="#">SF.KEY_MGT</a>
<a href="#">FDP_ACF.1/SVD_Transfer</a>	<a href="#">SF.KEY_MGT</a>
<a href="#">FDP_ACC.1/SCD/SVD_Generation</a>	<a href="#">SF.KEY_MGT</a>
<a href="#">FDP_ACF.1/SCD/SVD_Generation</a>	<a href="#">SF.KEY_MGT</a>
<a href="#">FTP_ITC.1/SCD</a>	<a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FDP_UCT.1/SCD</a>	<a href="#">SF.SM</a>
<a href="#">FDP_ITC.1/SCD</a>	<a href="#">SF.KEY_MGT</a>
<a href="#">FDP_ACC.1/SCD_Import</a>	<a href="#">SF.KEY_MGT</a>

<a href="#">FDP_ACF.1/SCD_Import</a>	<a href="#">SF.KEY_MGT</a>
<a href="#">FTP_ITC.1/SVD</a>	<a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FDP_DAU.2/SVD</a>	<a href="#">SF.SM</a>
<a href="#">FIA_API.1</a>	<a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FDP UIT.1/DTBS</a>	<a href="#">SF.SIG</a>
<a href="#">FTP_ITC.1/VAD</a>	<a href="#">SF.PIN_MGT</a>
<a href="#">FTP_ITC.1/DTBS</a>	<a href="#">SF.SM</a>
<a href="#">FCS_RND.1</a>	<a href="#">SF.AUTH</a>
<a href="#">FCS_CKM.1/DH_PACE</a>	<a href="#">SF.AUTH</a>
<a href="#">FCS_CKM.1/Session Keys</a>	<a href="#">SF.SM</a>
<a href="#">FCS_COP.1/GP Secret Data Protection</a>	<a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FCS_COP.1/SM in Confidentiality</a>	<a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FCS_COP.1/SM in Integrity</a>	<a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FCS_COP.1/Digital Auth</a>	<a href="#">SF.ESERVICE</a>
<a href="#">FCS_COP.1/Enc Key Decipherment</a>	<a href="#">SF.ESERVICE</a>
<a href="#">FCS_COP.1/SIG_VER</a>	<a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FDP_ACC.1/TRM</a>	<a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FDP_ACF.1/TRM</a>	<a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FDP_ACC.1/MNG_File</a>	<a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FDP_ACF.1/MNG_File</a>	<a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FDP_UCT.1/TRM</a>	<a href="#">SF.AUTH</a> , <a href="#">SF.SM</a> , <a href="#">SF.KEY_MGT</a>
<a href="#">FDP UIT.1/TRM</a>	<a href="#">SF.SM</a> , <a href="#">SF.KEY_MGT</a>
<a href="#">FIA_UID.1/PACE</a>	<a href="#">SF.PIN_MGT</a> , <a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FIA_UAU.1/PACE</a>	<a href="#">SF.PIN_MGT</a> , <a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FIA_UAU.4/PACE</a>	<a href="#">SF.PIN_MGT</a> , <a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FIA_UAU.5/PACE</a>	<a href="#">SF.PIN_MGT</a> , <a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FIA_UAU.6/PACE</a>	<a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FIA_UAU.6/EAC</a>	<a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FIA_AFL.1/AUTH</a>	<a href="#">SF.PIN_MGT</a> , <a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FIA_API.1/TOE Authentication</a>	<a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>
<a href="#">FMT_SMR.1/PACE</a>	<a href="#">SF.PIN_MGT</a> , <a href="#">SF.AUTH</a>
<a href="#">FMT_MTD.1/CVCA_INI</a>	<a href="#">SF.AUTH</a>
<a href="#">FMT_MTD.1/CVCA_UPD</a>	<a href="#">SF.AUTH</a>

<a href="#">FMT_MTD.1/DATE</a>	<a href="#">SF.AUTH</a>
<a href="#">FMT_MTD.1/CAPK</a>	<a href="#">SF.AUTH</a>
<a href="#">FMT_MTD.1/KEY_READ</a>	<a href="#">SF.AUTH</a>
<a href="#">FMT_MTD.1/Key Usage Counter</a>	<a href="#">SF.KEY_MGT</a>
<a href="#">FMT_MTD.1/Initialize PIN</a>	<a href="#">SF.PIN_MGT</a>
<a href="#">FMT_MTD.1/Resume PIN</a>	<a href="#">SF.PIN_MGT</a>
<a href="#">FMT_MTD.1/Change PIN</a>	<a href="#">SF.PIN_MGT</a>
<a href="#">FMT_MTD.1/Unblock PIN</a>	<a href="#">SF.PIN_MGT</a>
<a href="#">FMT_MTD.1/UnblockChange RAD</a>	<a href="#">SF.PIN_MGT</a>
<a href="#">FMT_MTD.1/Erase PIN</a>	<a href="#">SF.PIN_MGT</a>
<a href="#">FMT_MTD.1/Reinitialize PIN</a>	<a href="#">SF.PIN_MGT</a>
<a href="#">FMT_MTD.1/UnblockChange PUK</a>	<a href="#">SF.PIN_MGT</a>
<a href="#">FMT_MTD.1/TOE State</a>	<a href="#">SF.CONF</a>
<a href="#">FMT_MTD.3</a>	<a href="#">SF.PIN_MGT</a> , <a href="#">SF.AUTH</a>
<a href="#">FMT_MTD.1/INI_ENA</a>	<a href="#">SF.AUTH</a>
<a href="#">FMT_MTD.1/INI_DIS</a>	<a href="#">SF.AUTH</a>
<a href="#">FMT_LIM.1</a>	<a href="#">SF.PHYS</a>
<a href="#">FMT_LIM.2</a>	<a href="#">SF.PHYS</a>
<a href="#">FPT_EMS.1/PIN-PUK-KEYS</a>	<a href="#">SF.PHYS</a>
<a href="#">FTP_ITC.1/PACE</a>	<a href="#">SF.PIN_MGT</a> , <a href="#">SF.AUTH</a> , <a href="#">SF.SM</a>

**Table 26 SFRs and TSS - Coverage**

<b>TOE Summary Specification</b>	<b>Security Functional Requirements</b>
<a href="#">SF.PIN_MGT</a>	<a href="#">FIA_UID.1/PACE</a> , <a href="#">FIA_UAU.1/PACE</a> , <a href="#">FIA_UAU.4/PACE</a> , <a href="#">FIA_UAU.5/PACE</a> , <a href="#">FIA_AFL.1/AUTH</a> , <a href="#">FMT_SMR.1/PACE</a> , <a href="#">FMT_MTD.1/Initialize PIN</a> , <a href="#">FMT_MTD.1/Resume PIN</a> , <a href="#">FMT_MTD.1/Change PIN</a> , <a href="#">FMT_MTD.1/Unblock PIN</a> , <a href="#">FMT_MTD.1/UnblockChange RAD</a> , <a href="#">FMT_MTD.1/Erase PIN</a> , <a href="#">FMT_MTD.1/Reinitialize PIN</a> , <a href="#">FMT_MTD.1/UnblockChange PUK</a> , <a href="#">FMT_MTD.3</a> , <a href="#">FTP_ITC.1/PACE</a> , <a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FMT_MTD.1/Signatory</a> , <a href="#">FIA_UID.1</a> , <a href="#">FIA_AFL.1/RAD</a> , <a href="#">FIA_UAU.1</a> , <a href="#">FTP_ITC.1/VAD</a>
<a href="#">SF.SIG</a>	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_MOF.1</a> , <a href="#">FMT_MSA.1/Signatory</a> , <a href="#">FMT_MSA.2</a> , <a href="#">FMT_MSA.3</a> , <a href="#">FMT_MSA.4</a> , <a href="#">FIA_UID.1</a> , <a href="#">FIA_UAU.1</a> , <a href="#">FDP_SDI.2/DTBS</a> , <a href="#">FDP_ACC.1/Signature Creation</a> , <a href="#">FDP_ACF.1/Signature Creation</a> , <a href="#">FCS_COP.1/Sign</a> , <a href="#">FDP_UIT.1/DTBS</a>

<a href="#">SF.AUTH</a>	<a href="#">FCS_RND.1</a> , <a href="#">FCS_CKM.1/DH_PACE</a> , <a href="#">FCS_COP.1/GP Secret Data Protection</a> , <a href="#">FCS_COP.1/SM in Confidentiality</a> , <a href="#">FCS_COP.1/SM in Integrity</a> , <a href="#">FCS_COP.1/SIG VER</a> , <a href="#">FDP_ACC.1/TRM</a> , <a href="#">FDP_ACF.1/TRM</a> , <a href="#">FDP_ACC.1/MNG File</a> , <a href="#">FDP_ACF.1/MNG File</a> , <a href="#">FDP_UCT.1/TRM</a> , <a href="#">FIA_UID.1/PACE</a> , <a href="#">FIA_UAU.1/PACE</a> , <a href="#">FIA_UAU.4/PACE</a> , <a href="#">FIA_UAU.5/PACE</a> , <a href="#">FIA_UAU.6/PACE</a> , <a href="#">FIA_UAU.6/EAC</a> , <a href="#">FIA_AFL.1/AUTH</a> , <a href="#">FIA_API.1/TOE Authentication</a> , <a href="#">FMT_SMR.1/PACE</a> , <a href="#">FMT_MTD.1/CVCA INI</a> , <a href="#">FMT_MTD.1/CVCA UPD</a> , <a href="#">FMT_MTD.1/DATE</a> , <a href="#">FMT_MTD.1/CAPK</a> , <a href="#">FMT_MTD.1/KEY READ</a> , <a href="#">FMT_MTD.3</a> , <a href="#">FMT_MTD.1/INI_ENA</a> , <a href="#">FMT_MTD.1/INI_DIS</a> , <a href="#">FTP_ITC.1/PACE</a> , <a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FMT_MSA.1/Admin</a> , <a href="#">FMT_MSA.2</a> , <a href="#">FMT_MSA.3</a> , <a href="#">FMT_MSA.4</a> , <a href="#">FIA_UID.1</a> , <a href="#">FIA_UAU.1</a> , <a href="#">FTP_ITC.1/SCD</a> , <a href="#">FTP_ITC.1/SVD</a> , <a href="#">FIA_API.1</a>
<a href="#">SF.SM</a>	<a href="#">FCS_CKM.1/Session Keys</a> , <a href="#">FCS_COP.1/GP Secret Data Protection</a> , <a href="#">FCS_COP.1/SM in Confidentiality</a> , <a href="#">FCS_COP.1/SM in Integrity</a> , <a href="#">FCS_COP.1/SIG VER</a> , <a href="#">FDP_ACC.1/TRM</a> , <a href="#">FDP_ACF.1/TRM</a> , <a href="#">FDP_ACC.1/MNG File</a> , <a href="#">FDP_ACF.1/MNG File</a> , <a href="#">FDP_UCT.1/TRM</a> , <a href="#">FDP_UIT.1/TRM</a> , <a href="#">FIA_UID.1/PACE</a> , <a href="#">FIA_UAU.1/PACE</a> , <a href="#">FIA_UAU.4/PACE</a> , <a href="#">FIA_UAU.5/PACE</a> , <a href="#">FIA_UAU.6/PACE</a> , <a href="#">FIA_UAU.6/EAC</a> , <a href="#">FIA_AFL.1/AUTH</a> , <a href="#">FIA_API.1/TOE Authentication</a> , <a href="#">FTP_ITC.1/PACE</a> , <a href="#">FTP_ITC.1/SCD</a> , <a href="#">FDP_UCT.1/SCD</a> , <a href="#">FTP_ITC.1/SVD</a> , <a href="#">FDP_DAU.2/SVD</a> , <a href="#">FIA_API.1</a> , <a href="#">FTP_ITC.1/DTBS</a>
<a href="#">SF.KEY_MGT</a>	<a href="#">FDP_UCT.1/TRM</a> , <a href="#">FDP_UIT.1/TRM</a> , <a href="#">FMT_MTD.1/Key Usage Counter</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FMT_MSA.2</a> , <a href="#">FMT_MSA.3</a> , <a href="#">FMT_MSA.4</a> , <a href="#">FIA_UID.1</a> , <a href="#">FIA_UAU.1</a> , <a href="#">FCS_CKM.4</a> , <a href="#">FCS_CKM.1/SCD/SVD Generation</a> , <a href="#">FDP_ACC.1/SVD Transfer</a> , <a href="#">FDP_ACF.1/SVD Transfer</a> , <a href="#">FDP_ACC.1/SCD/SVD Generation</a> , <a href="#">FDP_ACF.1/SCD/SVD Generation</a> , <a href="#">FDP_ITC.1/SCD</a> , <a href="#">FDP_ACC.1/SCD Import</a> , <a href="#">FDP_ACF.1/SCD Import</a>
<a href="#">SF.CONF</a>	<a href="#">FMT_MTD.1/TOE State</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FMT_MSA.2</a> , <a href="#">FMT_MSA.3</a>
<a href="#">SF.ESERVICE</a>	<a href="#">FCS_COP.1/Digital Auth</a> , <a href="#">FCS_COP.1/Enc Key Decipherment</a>
<a href="#">SF.SAFESTATE_MGT</a>	<a href="#">FPT_FLS.1</a> , <a href="#">FPT_TST.1</a> , <a href="#">FDP_SDI.2/DTBS</a> , <a href="#">FDP_SDI.2/Persistent</a> , <a href="#">FDP_RIP.1</a>
<a href="#">SF.PHYS</a>	<a href="#">FMT_LIM.1</a> , <a href="#">FMT_LIM.2</a> , <a href="#">FPT_EMS.1/PIN-PUK-KEYS</a> , <a href="#">FPT_EMS.1</a> , <a href="#">FPT_PHP.1</a> , <a href="#">FPT_PHP.3</a>
<a href="#">SF.ADMIN</a>	<a href="#">FMT_MTD.1/Admin</a>

**Table 27 TSS and SFRs - Coverage**