

ID-A v1.1 on ID-One Cosmo X

Public Security Target



Issue : 3

DOCUMENT REVISION HISTORY			
Issue	Date (mm/dd/yyyy)	Author	Purpose
1	05/04/2026	IN Smart Identity	Initial version
2	05/05/2026	IN Smart Identity	AGD versions updated in §2
3	05/19/2026	IN Smart Identity	TOE version and AGD versions updated Note added for Hashing operation in FCS_COP.1

Table of contents

TABLE OF CONTENTS.....	3
TABLE OF FIGURES	6
TABLE OF TABLES.....	7
1 SECURITY TARGET INTRODUCTION.....	8
1.1 INTRODUCTION.....	8
1.2 ST REFERENCE	8
1.3 TOE REFERENCE.....	9
2 TECHNICAL TERMS, ABBREVIATION AND ASSOCIATED REFERENCES	11
2.1 TECHNICAL TERMS	11
2.2 ABBREVIATION.....	16
2.3 ASSOCIATED REFERENCES	18
3 TOE OVERVIEW.....	22
3.1 TOE DESCRIPTION	23
3.1.1 <i>Physical Scope</i>	24
3.1.2 <i>Logical Scope</i>	25
3.2 REQUIRED NON-TOE HARDWARE/SOFTWARE/FIRMWARE	26
3.3 TOE USAGE AND MAJOR SECURITY FEATURES	26
3.3.1 <i>Authentication mechanisms</i>	28
3.3.2 <i>Cryptographic operations</i>	28
3.3.3 <i>Trusted Channel function</i>	28
3.3.4 <i>Access Control function</i>	28
3.3.5 <i>Data Storage function</i>	28
3.3.6 <i>Integrity function</i>	29
3.3.7 <i>Electronic Services</i>	29
3.3.8 <i>Keys and PINs management</i>	29
3.3.9 <i>Single Sign on feature (SSO)</i>	29
3.3.10 <i>Features from the Platform</i>	29
4 LIFE CYCLE	30
4.1.1 <i>Development Environment</i>	30
4.1.2 <i>Production Environment</i>	31
4.1.3 <i>Preparation Environment</i>	38
4.1.4 <i>Operational Environment</i>	38
5 CONFORMANCE CLAIMS.....	39
5.1 CC CONFORMANCE	39
5.2 PP CLAIMS	39
5.3 PACKAGE CLAIM	39
5.4 CONFORMANCE RATIONALE	39
5.4.1 <i>Security Problem Definition</i>	39
5.4.2 <i>Security Objectives</i>	40
5.4.3 <i>Assumptions</i>	41
5.4.4 <i>Security Objectives</i>	42
5.4.5 <i>Security functional requirement</i>	42
5.4.6 <i>Security Assurance Requirements</i>	45
5.4.7 <i>Threats</i>	45
5.4.8 <i>Organisational Security Policy</i>	45
5.4.9 <i>Additional functionalities impacts on the TOE</i>	45

6	SECURITY PROBLEM DEFINITION	46
6.1	ASSETS.....	46
6.1.1	<i>Primary Assets drawn from the protection profiles.....</i>	46
6.1.2	<i>Primary Assets related to EAC2</i>	46
6.2	USERS / SUBJECTS.....	48
6.2.1	<i>Subjects drawn from the protection profiles.....</i>	48
6.2.2	<i>Additional Users/Subjects</i>	48
6.2.3	<i>Threat agents</i>	50
6.3	THREATS.....	50
6.3.1	<i>Threats drawn from the protection profiles</i>	50
6.3.2	<i>Threats related to EAC2.....</i>	51
6.3.3	<i>Added Threats</i>	53
6.4	ORGANISATIONAL SECURITY POLICIES	53
6.4.1	<i>OSPs drawn from the protection profiles.....</i>	53
6.4.2	<i>OSP related to EAC2.....</i>	54
6.4.3	<i>Added OSP</i>	55
6.5	ASSUMPTIONS	56
6.5.1	<i>All SSCD parts.....</i>	56
6.5.2	<i>Parts 3 and 6 only.....</i>	56
7	SECURITY OBJECTIVES	57
7.1	SECURITY OBJECTIVES FOR THE TOE	57
7.1.1	<i>All SSCD parts.....</i>	57
7.1.2	<i>SSCD parts 2, 4 and 5 only</i>	58
7.1.3	<i>SSCD parts 3 and 6 only</i>	58
7.1.4	<i>SSCD part 4 only.....</i>	58
7.1.5	<i>SSCD parts 5 and 6 only</i>	59
7.1.6	<i>Additional Security Objectives for the TOE</i>	59
7.2	SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT	63
7.2.1	<i>All SSCD parts.....</i>	63
7.2.2	<i>SSCD parts 2, 3 and 4 only</i>	63
7.2.3	<i>SSCD part 2, 3, 5 and 6 only.....</i>	64
7.2.4	<i>SSCD parts 3 and 6 only</i>	64
7.2.5	<i>SSCD part 4 only.....</i>	64
7.2.6	<i>SSCD parts 5 and 6 only</i>	65
7.2.7	<i>Additional Security Objectives for the Operational Environment.....</i>	66
7.3	SECURITY OBJECTIVES RATIONALE.....	68
7.3.1	<i>Threats.....</i>	68
7.3.2	<i>Organisational Security Policies</i>	71
7.3.3	<i>Assumptions</i>	75
7.3.4	<i>SPD and Security Objectives</i>	75
8	SECURITY REQUIREMENTS	83
8.1	SECURITY FUNCTIONAL REQUIREMENTS	83
8.1.1	<i>All SSCD parts.....</i>	83
8.1.2	<i>SSCD parts 2, 4 and 5 only</i>	103
8.1.3	<i>SSCD parts 3 and 6 only</i>	106
8.1.4	<i>SSCD part 4 only.....</i>	108
8.1.5	<i>SSCD parts 5 and 6 only</i>	109
8.1.6	<i>Additional SFRs.....</i>	109
8.2	SECURITY ASSURANCE REQUIREMENTS.....	118
8.3	SECURITY REQUIREMENTS RATIONALE	118
8.3.1	<i>Objectives</i>	118
8.3.2	<i>Rationale tables of Security Objectives and SFRs.....</i>	126
8.3.3	<i>Dependencies</i>	137
8.3.4	<i>Rationale for the Security Assurance Requirements</i>	142
8.3.5	<i>AVA_VAN.5 Advanced methodical vulnerability analysis</i>	142

8.3.6	<i>ALC_DVS.2 Sufficiency of security measures</i>	<i>142</i>
8.3.7	<i>ALC_FLR.3 Systematic flaw remediation</i>	<i>143</i>
9	TOE SUMMARY SPECIFICATION	144
9.1	TOE SUMMARY SPECIFICATION	144
9.1.1	<i>Chip security functionalities</i>	<i>144</i>
9.1.2	<i>Platform security functionalities.....</i>	<i>144</i>
9.1.3	<i>Application security functionalities.....</i>	<i>144</i>
9.2	SFRs AND TSS.....	149
9.2.1	<i>SFRs and TSS - Rationale</i>	<i>149</i>
9.2.2	<i>Association tables of SFRs and TSS</i>	<i>159</i>

Table of figures

Figure 1 TOE's Physical form factor and interfaces.....	24
Figure 2: TOE Logical scope	26
Figure 3 Life cycle Overview	30

Table of tables

Table 1 TOE Configurations.....	10
Table 2 Applet Internal Versions.....	10
Table 3 Ports and Interfaces	24
Table 4 TOE Guidance	25
Table 5 Option 1: Both Platform and Applet packages are loaded at IC Manufacturer site	31
Table 6 Option 2: Both Platform and Applet packages are loaded at CC-audited INSI or IDEMIA sites or non-CC-audited INSI sites or External sites	32
Table 7 Option 3(a): Platform package is loaded at IC Manufacturer site and Applet package is loaded at CC-audited INSI or IDEMIA sites or non-CC-audited INSI sites or External sites through GP Mechanism	33
Table 8 Platform package is loaded at IC Manufacturer site and 3b (i) Applet package is loaded through resident application using LSK format and 3b (ii) DUMP Package is loaded through resident application using DSK Secret Live Key - at CC-audited INSI or IDEMIA sites or non-CC- audited INSI sites or External sites	34
Table 9 Option 3(c): Platform package is loaded at IC Manufacturer site and Applet package in plain format is loaded at CC-audited INSI sites only	34
Table 10 Option 4(a): Platform package is loaded at CC-audited INSI or IDEMIA sites or non-CC- audited INSI sites or External sites and Applet package is loaded at CC-audited INSI or IDEMIA sites or non-CC-audited INSI sites or External sites through GP Mechanism	35
Table 11 Platform package is loaded at CC-audited INSI or IDEMIA sites or non-CC-audited INSI sites or External sites and 4b (i) Applet package is loaded through Resident application using LSK format and 4b (ii) DUMP Package is loaded through resident application using DSK Secret Live Key - at CC-audited INSI or IDEMIA sites or non-CC-audited INSI sites or External sites	37
Table 12 Option 4(c): Platform package is loaded at CC-audited INSI or IDEMIA sites or non-CC- audited INSI sites or External sites and Applet package in plain format is loaded at CC-audited INSI sites only	37
Table 13 PP SPDs vs. ST	40
Table 14 PP Security Objectives vs. ST	41
Table 15 PP SFRs vs. ST	44
Table 16 Threats and Security Objectives - Coverage	77
Table 17 Security Objectives and Threats - Coverage	78
Table 18 OSPs and Security Objectives - Coverage	79
Table 19 Security Objectives and OSPs - Coverage	81
Table 20 Assumptions and Security Objectives for the Operational Environment - Coverage.....	82
Table 21 Security Objectives for the Operational Environment and Assumptions - Coverage.....	82
Table 22 Supported Elliptic Curves and certified scope validity	103
Table 23 Security Objectives and SFRs - Coverage	130
Table 24 SFRs and Security Objectives	137
Table 25 SFRs Dependencies.....	141
Table 26 SARs Dependencies	142
Table 27 SFRs and TSS - Coverage.....	161
Table 28 TSS and SFRs - Coverage.....	163

1 Security Target Introduction

1.1 Introduction

This document is the Security Target for the ID-A v1.1 application installed on the ID-One Cosmo X platform. The ID-A v1.1 application is an INSI Java Card application designed to provide identification, authentication and advanced signature creation functionality for national ID cards, health cards and corporate cards and electronic seal functionality.

The ID-A application can be used to create advanced or qualified signature and electronic seal in the sense of **[eIDAS]** in its Qualified Signature Creation Device (QSCD) configuration defined in this security target and complies to the Identification Authentication Signature for European Citizen Card IAS ECC v2 specification **[IAS-ECC]**.

ID-One Cosmo X is an INSI Global Platform Java Card solution, which is Common Criteria EAL 6+ certified on top of the Infineon SLC37 security controller.

This ST has been conceived to prepare a Common Criteria evaluation following the “compositional approach” described in **[COMP]**. This approach consists in starting from a Platform that has been independently certified, and performing an evaluation of the composite product resulting from embedding an application into it, using some of the results from the evaluation of the Cosmo X open platform certified by the ANSSI.

This Security Target describes:

1. The Target of Evaluation (TOE)
2. The assets to be protected, the threats (T) to be countered by the TOE itself during the usage of the TOE,
3. The organizational security policies (OSP), and the assumptions (A),
4. The security objectives (OT) for the TOE and its environment (OE),
5. The security functional requirements (SFR) for the TOE and its IT environment,
6. The TOE security assurance requirements (SAR), and
7. The TOE Summary specification (TSS).

1.2 ST Reference

Title	ID-A v1.1 on Cosmo X – Public Security Target
ST Identification	FQR 151007-418
Revision	Ed 3
CC Version	2022 R1
Assurance Level	EAL5 augmented with ALC_DVS.2, AVA_VAN.5 and ALC_FLR.3
ITSEF	BrightSight
Certification Body	TrustCB – Netherlands
Compliant to Protection Profiles	[PP-SSCD2], [PP-SSCD3], [PP-SSCD4] [PP-SSCD5] [PP-SSCD6]

1.3 TOE Reference

TOE Commercial Name	ID-A v1.1 on ID-One Cosmo X
TOE version	v1.1.1
Applet Code Versions	See Table 1 below
Applet Internal Versions	See Table 2 below
Platform Name	ID-One Cosmo X
Platform Certificate	[PTF_CERT]
IC Certificate Reference	BSI_DSZ-CC-1107-V6-2025

The following table defines the TOE configurations, depending on the source code compilation and build options:

Configurations of the ID-A applet	Description	Content of the config (package/cap files)	SAAAAR + version + config code
Config 1	ID-A Applet without support for Asymmetric Role and Device Authentication	SAAAAR + version of Package + config of ID-A Package {config 1}	419261FF 01010000 0101
		SAAAAR + version of package + config of Common Package	417641FF 01000000 0201
Config 2	ID-A Applet with support for Asymmetric Role and Device Authentication	SAAAAR + version of Package + config of ID-A Package {config 2}	419261FF 01010000 0201
		SAAAAR + version of Package + config of Common Package	417641FF 01000000 0201
Config 3	ID-A Applet without support for Asymmetric Role and Device Authentication and with functional biometric authentication	SAAAAR + version of Package + config of ID-A Package {config 3}	419261FF 01010000 0101
		SAAAAR + version of Package + config of Common Package	417641FF 01000000 0301
Config 4	ID-A Applet with support for Asymmetric Role and Device Authentication and with functional biometric authentication	SAAAAR + version of Package + config of ID-A Package {config 4}	419261FF 01010000 0201
		SAAAAR + version of Package + config of Common Package	417641FF 01000000 0301
Config 5	ID-A Applet without support for Asymmetric Role and Device Authentication and with functional biometric authentication and PIN sharing	SAAAAR + version of Package + Config of ID-A Package {config 5}	419261FF 01010000 0301
		SAAAAR + version of Package + config of Common Package + Config of Server Applet Manager Package	417641FF 01000000 0301

Table 1 TOE Configurations
Note:

The authentication by PIN bio is not part of the TOE.

In the table above, the value is composed of a "SAAAAR" code (3 first bytes in bold described below), a "version" (2 next coloured bytes) and a "config" ID (2 last coloured bytes). Not coloured bytes are padding bytes.

The "SAAAAR" is the product configuration item number and is uniquely defined as:

S	Site code	1 digit
AAAA	Article number	4 digits
R	Software Release number	1 digit

Applet Internal Versions of above Configurations are as follows:

Configurations	Returned value of DF67	
Config 1	01 04 00 14	01 01 00 08
Config 2	01 03 00 14	01 01 00 08
Config 3	01 04 00 14	01 04 00 07
Config 4	01 03 00 14	01 04 00 07
Config 5	01 05 00 14	01 04 00 07

Table 2 Applet Internal Versions

2 Technical Terms, Abbreviation and Associated References

2.1 Technical terms

Term	Definition
Administrator	<i>user who performs TOE initialization, TOE personalisation, or other TOE administrative functions</i>
Advanced electronic signature	<i>An electronic signature which meets the following requirements [DIR]:</i> <i>(i) it is uniquely linked to the signatory,</i> <i>(ii) it is capable of identifying the signatory,</i> <i>(iii) it is created using means that the signatory can maintain under his sole control,</i> <i>(iv) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.</i>
Application note	<i>Optional informative part of the ST containing sensitive supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE.</i>
Authentication	<i>Authentication defines a procedure that verifies the identity of the communication partner. The most elegant method is based on the use of so called digital signatures.</i>
Authentication data	<i>information used to verify the claimed identity of a user</i>
Card Access Number (CAN)	<i>A short password that is printed or displayed on the document. The CAN is a non-blocking password. The CAN may be static (printed on the Identification Card), semi-static (e.g. printed on a label on the Identification Card) or dynamic (randomly chosen by the Card and displayed by it using e.g. ePaper, OLED or similar technologies), see [TR-03110], sec. 3.3</i>
Certificate	<i>digital signature used as electronic attestation binding signature-verification data to a person confirming the identity of that person as legitimate signer</i>
Certificate-generation application (CGA)	<i>collection of application components that receive the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate</i>
Certificate info	<i>information associated with an SCD/SVD pair that may be stored in a secure signature creation device</i>

Term	Definition
	<i>NOTE 1: Certificate info is either</i> - a signer's public key certificate or, - one or more hash values of a signer's public key certificate together with an identifier of the hash function used to compute the hash values. <i>NOTE 2: Certificate info may contain information to allow the user to distinguish between several certificates.</i>
Certificate revocation list	<i>A list of revoked certificates issued by a certificate authority</i>
Certification service provider (CSP)	<i>entity that issues certificates or provides other services related to electronic signatures</i>
CLFDB	<i>Ciphered Load File Data Block Defined in Global Platform load encrypted applets. Decryption occurs with a GP symmetrice CLFDB key installed in the SSD or ISD.</i>
Data to be signed (DTBS)	<i>all of the electronic data to be signed including a user message and signature attributes</i>
Data to be signed or its unique representation (DTBS/R)	<i>data received by a secure signature creation device as input in a single signature creation operation</i> <i>NOTE: Examples of DTBS/R are</i> - a hash value of the data to be signed (DTBS), or - an intermediate hash value of a first part of the DTBS complemented with a remaining part of the DTBS, or - the DTBS.
ECC	<i>(Elliptic Curve Cryptography) class of procedures providing an attractive alternative for the probably most popular asymmetric procedure, the RSA algorithm.</i>
Electronic Identification, Authentication and Trust Services (eIDAS)	<i>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</i>
Hash function	<i>A function which forms the fixed-size result (the hash value) from an arbitrary amount of data (which is the input). These functions are used to generate the electronic equivalent of a fingerprint. The significant factor is that it must be impossible to generate two entries which lead to the same hash value (so called collisions) or even to generate a matching message for a defined hash value.</i>
Integrity	<i>The test on the integrity of data is carried out by checking messages for changes during the transmission by the receiver. Common test procedures employ Hash functions, MACs (Message Authentication Codes) or – with additional functionality – digital signatures.</i>

Term	Definition
Javacard	<i>A smart card with a Javacard operation system.</i>
Legitimate user	<i>An user of a secure signature creation device who gains possession of it from an SSCD provisioning service provider and who may be authenticated by the SSCD as its signatory.</i>
MAC	<i>Message Authentication Code. Algorithm that expands the message by means of a secret key by special redundant pieces of information, which are stored or transmitted together with the message. To prevent an attacker from targeted modification of the attached redundancy requires its protection in a suitable way.</i>
Non repudiation	<i>One of the objectives in the employment of digital signatures. It describes the fact that the sender of a message is prevented from denying the preparation of the message. The problem cannot be simply solved with cryptographic routines, but the entire environment needs to be considered and respective framework conditions need to be provided by pertinent laws.</i>
Notified body	<i>An organizational entity designated by a member state of the European Union as responsible for accreditation and supervision of the evaluation process for products conforming to [PP-SSCD2], [PP-SSCD5] and for determining admissible algorithms and algorithm parameters.</i>
PACE Terminal (PCT)	<i>A technical system verifying correspondence between the stored password and the related value presented to the terminal. PCT implements the terminal's part of the PACE protocol and authenticates itself to the Card using a shared password (CAN, PIN or PUK). The PCT is not allowed reading User Data (see sec. 4.2.2 in [TR-03110]). See [TR-03110], chap. 3.3, 4.2, table 1.2 and G.2.</i>
Password Authenticated Connection Establishment (PACE)	<i>A communication establishment protocol defined in [TR-03110], sec. 4.2. The PACE Protocol is a password authenticated DiffieHellman 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>
Private key	<i>Secret key only known to the receiver of a message, which is used in asymmetric ciphers for encryption or generation of digital signatures.</i>
Pseudo random number	<i>Many cryptographic mechanisms require random numbers (e.g. in key generation). The problem, however, is that it is difficult to implement true random numbers in software. Therefore, so called pseudo random number generators are used, which then should be initialized with a real random element (the so called seed).</i>
Public Key	<i>Publicly known key in an asymmetric cipher which is used for encryption and verification of digital signatures.</i>
Public key infrastructure (PKI)	<i>Combination of hardware and software components, policies, and different procedures used to manage digital certificates.</i>
Qualified certificate	<i>public key certificate that meets the requirements laid down in Annex I and that is provided by a CSP that fulfils the requirements laid down in Annex II (the directive: 2.10) [DIR]</i>

Term	Definition
Qualified electronic signature	<i>advanced electronic signature that has been created with an SSCD with a key certified with a qualified certificate ([DIR]: 5.1).</i>
Random numbers	<i>Many cryptographic algorithms or protocols require a random element, mostly in form of a random number, which is newly generated in each case. In these cases, the security of the procedure depends in part on the suitability of these random numbers. As the generation of real random numbers within computers still imposes a problem (a source for real random events can in fact only be gained by exact observation of physical events, which is not easy to realize for software), so called pseudo random numbers are used instead.</i>
Reference authentication data (RAD)	<i>Data persistently stored by the TOE for authentication of a user as authorised for a particular role.</i>
Secure messaging	<i>Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4.</i>
Secure signature creation device (SSCD)	<i>Personalised device that meets the requirements laid down in [DIR], Annex III by being evaluated according to a security target conforming to this PP ([DIR]: 2.5 and 2.6).</i>
Signatory	<i>legitimate user of an SSCD associated with it in the certificate of the signature-verification data and who is authorized by the SSCD to operate the signature-creation function</i>
Signature attributes	<i>Additional information that is signed together with a user message.</i>
Signature creation application (SCA)	<i>Application complementing an SSCD with a user interface with the purpose to create an electronic signature. Note: A signature creation application is software consisting of a collection of application components configured to:</i> <i>present the data to be signed (DTBS) for review by the signatory,</i> <i>obtain prior to the signature process a decision by the signatory,</i> <i>if the signatory indicates by specific unambiguous input or action its intent to sign send a DTBS/R to the TOE,</i> <i>process the electronic signature generated by the SSCD as appropriate, e.g. as attachment to the DTBS.</i>
Signature creation data (SCD)	<i>private cryptographic key stored in the SSCD under exclusive control by the signatory to create an electronic signature</i>
Signature creation system (SCS)	<i>complete system that creates an electronic signature consisting of an SCA and an SSCD</i>
Signature verification data (SVD)	<i>public cryptographic key that can be used to verify an electronic signature</i>

Term	Definition
Signed data object	<i>The electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.</i>
Smart card	<i>A smart card is a chip card which contains an internal micro controller with CPU, volatile (RAM) and non-volatile (FLASH) memory, i.e. which can carry out its own calculations in contrast to a simple storage card. Sometimes a smart card has a numerical coprocessor (NPU) to execute public key algorithms efficiently. Smart cards have all of their functionality comprised on a single chip (in contrast to chip cards, which contain several chips wired to each other). There-fore, such a smart card is ideal for use in cryptography as it is almost impossible to manipulate its internal processes.</i>
SSCD provisioning service	<i>service to prepare and provide an SSCD to a subscriber and to support the signatory with certification of generated keys and administrative functions of the SSCD</i>
User	<i>entity (human user or external IT entity) outside the TOE that interacts with the TOE</i>
User Message	<i>data determined by the signatory as the correct input for signing</i>
Verification authentication data (VAD)	<i>data provided as input to a secure signature creation device for authentication by cognition</i>

2.2 Abbreviation

Acronym	Definition
ADF	<i>Application Dedicated File</i>
CA	<i>Certification authority</i>
CAD	<i>card acceptance device</i>
CAN	<i>Card Access Number</i>
CC	<i>Common Criteria</i>
CGA	<i>Certification generation application</i>
CPU	<i>Central Processing Unit</i>
CSP	<i>certification service provider</i>
DPA	<i>differential power analysis</i>
DTBS	<i>Data to be signed</i>
DTBS/R	<i>Data to be signed or its unique representation</i>
EAL	<i>Evaluation assurance level</i>
ECC	<i>Elliptic Curve Cryptography</i>
GP	<i>Global Platform</i>
HID	<i>human interface device</i>
INSI	<i>IN Smart Identity</i>
IT	<i>Information technology</i>
MAC	<i>Message Authentication Code</i>
OSP	<i>Organizational security policy</i>
PACE	<i>Password Authenticated Connection Establishment</i>
PIN	<i>Personal Identification Number</i>

Acronym	Definition
PP	<i>Protection profile</i>
PS	<i>Personalization System</i>
PUK	<i>PIN Unblocked Key</i>
RAD	<i>Reference authentication data</i>
RAM	<i>random access memory</i>
RNG	<i>random number generation</i>
SAR	<i>Security Assurance Requirements</i>
SCA	<i>Signature creation application</i>
SCD	<i>Signature creation data</i>
SCS	<i>Signature creation system</i>
SDO	<i>Security data object</i>
SF	<i>security function</i>
SFP	<i>Security function policy</i>
SFR	<i>Security functional requirement</i>
SPA	<i>simple power analysis</i>
SSCD	<i>Secure signature creation device</i>
ST	<i>Security target</i>
SVD	<i>Signature verification data</i>
TOE	<i>Target of evaluation</i>
TSF	<i>TOE security functionality</i>
VAD	<i>Verification authentication data</i>

2.3 Associated references

Reference	Description
[AGD_OPE]	FQR 151007-447 Ed 3 - AGD_OPE
[AGD_PRE]	FQR 151007-446 Ed 3 - AGD_PRE
[CC-1]	Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model, November 2022, CC:2022 revision 1 - CCMB-2022-11-001
[CC-2]	Common Criteria for information Technology Security Evaluation, Part 2: Introduction and general model, November 2022, CC:2022 revision 1 - CCMB-2022-11-002
[CC-3]	Common Criteria for information Technology Security Evaluation, Part 3: Introduction and general model, November 2022, CC:2022 revision 1 - CCMB-2022-11-003
[CC-5]	Common Criteria for information Technology Security Evaluation, Part 5: Introduction and general model, November 2022, CC:2022 revision 1 - CCMB-2022-11-005
[CC-ERRATA]	Common Criteria, Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1) – October 15, 2025, version 1.2
[CEM]	Common Methodology for Information Technology Security Evaluation , Evaluation methodology , November 2022, CEM:2022 revision 1 - CCMB-2022-11-006
[CEN-14890]	CEN/EN 14890:2013 Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services.
[COMP]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT "Composite product evaluation and certification for CC: 2022", Version 1, February 2025
[DIR]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures.
[EAC2-PP]	Common Criteria Protection Profile Profile Electronic Document implementing Extended Access Control Version 2 defined in BSI [TR-03110], BSI-CC-PP-0086, Version 1.01, May 20th, 2015, BSI
[ECCG-CM]	European Cybersecurity Certification Group - Sub-group on Cryptography Agreed Cryptographic Mechanisms – Version 2.0 – April 2025
[ECDSA]	ANSI x9.62-2005 Public Key Cryptography for the Financial Services Industry – The Elliptic Curve Digital Signature Algorithm (ECDSA)
[eIDAS]	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
[EU-IMP-2016-650]	COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation

Reference	Description
	(EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
[EU-REG-910/2014]	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-202]	National Institute of Standards and Technology. FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. 2015
[GP1]	GlobalPlatform Card Specification 2.3.1, GlobalPlatform Inc., March 2018.
[GP2]	Global Platform Card Technology, Secure Channel Protocol 03, Card Specification v 2.3 - Amendment D - Version 1.1.2 - March 2019
[IAS-ECC]	Identification Authentication Signature - European Citizen Card Technical Specifications Revision: 2.0.
[ICAO-9303]	International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – Machine Readable Passports, Version Seventh Edition, 2015 (this includes the latest supplemental for ICAO doc 9303 which also should be considered).
[IFX-ST]	IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 Security Target Lite, Infineon Technologies AG, Version 7.3, 2025-05-06
[ISO14443]	ISO/IEC 14443:2018 - Cards and security devices for personal identification — Contactless proximity objects - Part 1: Physical characteristics - Part 2: Radio frequency power and signal interface - Part 3: Initialization and anticollision - Part 4: Transmission protocol
[ISO15946]	[ISO15946-2] and [ISO15946-3]
[ISO15946-2]	ISO/IEC15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002.
[ISO15946-3]	ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002
[ISO18033-1]	ISO/IEC 18033: Information security — Encryption algorithms – Part 1: General – Edition 3 - September 2021
[ISO7816]	ISO/IEC 7816: Identification cards — Integrated circuit cards.
[ISO9797-1]	“Information technology – Security techniques: Data integrity mechanism using a cryptographic check function employing a block cipher algorithm” ISO/IEC 9797-1 (1999) , International Organization for Standardization

Reference	Description
[JCAPI]	Published by Oracle. Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.1, 2019
[JCRE]	Java Card Platform Runtime Environment Specification, Classic Edition Version 3.1, November 2019, Oracle Technology Network
[JCVM]	Java Card Platform Virtual Machine Specification, Classic Edition Version 3.1, November 2019, Oracle Technology Network
[Minidriver]	Windows Smart Card Minidriver Specification - Version 7.06 - July 1, 2009
[NIST-180-4]	NIST FIPS 180-4, Secure Hash Standard, February 2011
[NIST-800-38B]	NIST SP 800-38B - Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication, May 2005
[PACE-PP]	Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE – Common Criteria Protection Profile, BSI-CC-PP-0068-V2-2011-MA-01, Version 1.0.1, 22nd July 2014.
[PP-IC]	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014
[PP-SSCD2]	Protection profiles for secure signature creation device — Part 2: Device with key Generation, EN 419211-2:2013, CEN/TC 224, BSI-CC-PP-0059-2009-MA-02, Version 2.0.1, June 30 2016
[PP-SSCD3]	Protection profiles for secure signature creation device – Part3: Device with key import, EN 419211-3:2013, CEN/TC 224, BSI-CC-PP-0075-2012-MA-01, Version 1.0.2, 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 419211-4:2013, CEN/TC 224, BSI-CC-PP-0071-2012-MA-01, Version 1.0.1, 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 419211-5:2013, CEN/TC 224, BSI-CC-PP-0072-2012-MA-01, Version 1.0.1, 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 419211-6:2013, CEN/TC 224, BSI-CC-PP-0076-2013-MA-01, Version 1.0.4, June 30 2016
[PP-PL]	Java Card System - Open Configuration Protection Profile, Version 3.0.5, BSI-CC-PP-0099-2017
[PTF-ST]	FQR 110 A19A Ed3 - ID-One Cosmo X - Public Security Target
[PTF_CERT]	ANSSI-CC-2023/06-R01
[RSA-PKCS#1]	PKCS#1 RSA Cryptography standards v2.2 27th october 2012
[RSA-PKCS#3]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised, November 1, 1993.

Reference	Description
[TR-03110]	[TR-03110-2] and [TR-03110-3]
[TR-03110-2]	BSI: 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, 25 December 2016
[TR-03110-3]	BSI: TR-03110-3: Advanced Security Mechanisms for Machine Readable Travel Documents. Part 3 - Common Specifications, Version 2.21, 21 December 2016
[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

The TOE comprises of the INSI ID-A v1.1 Java Card PKI application installed on top of the INSI ID-One Cosmo X Global Platform Java Card operating system and the Infineon SLC37 security controller.

The ID-A v1.1 application is an INSI specific Java Card implementation designed to provide functionality for identification, authentication and advanced digital signature creation for national ID cards, health cards and corporate cards.

The ID-One Cosmo X platform has been certified Common Criteria EAL5+ on top of the Infineon SLC37 security controller **[PTF-ST]**. The Infineon SLC37 is a Common Criteria EAL6+ certified security controller.

In its Qualified Signature Creation Device (QSCD) configuration defined in this security target, ID-A v1.1 application instances can create advanced (qualified) digital signatures in the sense of **[eIDAS]**.

The ID-A v1.1 application complies to the Identification Authentication Signature for European Citizen Card IAS ECC v2 specification **[IAS-ECC]** and therefore supports authentication protocols for symmetric secure messaging ciphers AES128, AES192, AES256 and 3DES.

In addition, the ID-A v1.1 applet supports the following secure authentication protocols defined in **[TR-03110-2]** and **[TR-03110-3]**:

- PACE 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 (over contactless interface);
- Chip Authentication v2 (CAv2);
- Terminal Authentication v2 (TAv2).

The TOE addressed by this ST is a qualified electronic signature creation device QSCD/SSCD according to European Regulation 910/2014 **[EU-REG-910/2014]** and implementing act **[EU-IMP-2016-650]** with functionality covered in (a combination of) the following SSCD protection profiles:

- 1) SSCD Part 2: that performs the generation of signature keys in the device **[PP-SSCD2]**,
- 2) SSCD Part 3: that performs the import of the signature keys generated in a trusted manner outside the device **[PP-SSCD3]**,
- 3) SSCD Part 4: that specifies an extension for an SSCD with key generation (SSCD Part 2) that support establishing a trusted channel with a certificate generation application (CGA) **[PP-SSCD4]**,
- 4) SSCD Part 5: that specifies an extension for an SSCD with key generation (SSCD Part 2) that additionally supports establishing a trusted channel with a signature creation application (SCA) **[PP-SSCD5]** and
- 5) SSCD Part 6: that specifies an extension for an SSCD with key import (SSCD Part 3) that additionally supports establishing a trusted channel with a signature creation application (SCA) **[PP-SSCD6]**.

For these additional authentication protocols PACE, CAV2, TAV2

- i. additional security problem definitions,
- ii. additional security objectives and
- iii. additional SFRs have been added from **[EAC2-PP]**.

Note:

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.

3.1 TOE Description

The TOE consists of:

- The chip's circuitry and the IC dedicated software forming the Chip Platform (Hardware Platform);
- The IC embedded ID-One Cosmo X Global Platform Java Card operating system software consisting of
 - Java Card virtual machine, ensuring language-level security,
 - Java Card runtime environment, providing additional security features for Java card technology enabled devices,
 - Java card API, providing access to card's resources for the Applet,
 - Global Platform Card Manager, responsible for management of Applets on the card;
 - Crypto Library;
- ID-A v1.1 Applet along with Common package and interfaces in Server Applet Manager package;
- TOE Guidance documentation for the ID-A v1.1 application and the ID-One Cosmo X platform as specified in Table 4;
- The Global Platform Key Set (for TOE preparation by the Personalisation Agent).

The ID-A v1.1 application provides e-Services and national e-ID Applications based on Java Card. ID-A v1.1 is designed to be compliant with the IAS ECC v2 specification **[IAS-ECC]**. It provides the following services:

- 1) QSCD/SSCD containing sensitive private keys needed for generating qualified electronic signatures on behalf of the Card Holder as well as for user authentication and identification. The ID-A v1.1 application is intended to be used in the context of official and commercial services, where an electronic digital signature of the Card Holder is required and is to be certified according to **[PP-SSCD2]**, **[PP-SSCD3]**, **[PP-SSCD4]**, **[PP-SSCD5]** and **[PP-SSCD6]**,
- 2) PACE authentication as defined in **[TR-03110-2]** and **[TR-03110-3]** to ensure a trusted channel for secure communication of the TOE with a SCA and a CGA,
- 3) Extended Access Control Version 2 (EAC2) as defined in **[TR-03110-2]**. It consists of two parts: Chip Authentication Protocol Version 2 and Terminal Authentication Protocol Version 2,
- 4) Several features required by **[Minidriver]**.

3.1.1 Physical Scope

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 physical form factor (chip module or antenna inlay, etc.) into which the microchip is mounted is not part of the target of evaluation, because it does not alter nor modify any security functions of the TOE.

The TOE may be used on several physical form factors: modules within an inlay, or eCover; in a contact, contactless or dual plastic card.

The physical form factor of the TOE and its physical interfaces are depicted in Figure below. The cryptographic boundary of the module is the surface and edges of the die and associated bond pads, shown as circles in the following figure.

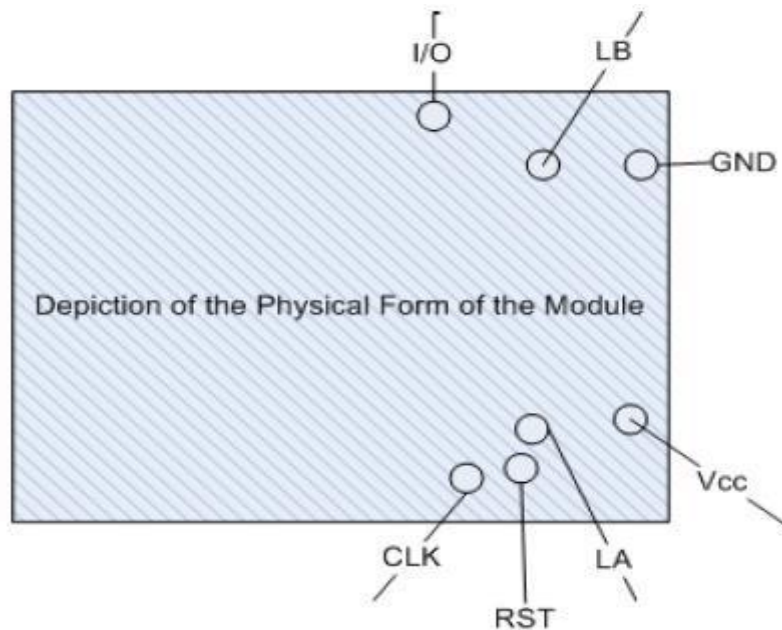


Figure 1 TOE's Physical form factor and interfaces

The contactless ports of the module require connection to an antenna. The module relies on **[ISO7816]** and **[ISO14443]** card readers and antenna connections as input/output devices.

Port	Description	Logical Interface Type
VCC, GND	ISO 7816: Supply voltage	Power (not available in contactless-only configurations)
RST	ISO 7816:Reset	Control in (not available in contactless-only configurations)
CLK	ISO 7816: Clock	Control in (not available in contactless-only configurations)
I/O	ISO 7816: Input/Output	Control in, Data in, Data out, Status out (not available in contactless-only configurations)
LA, LB	ISO 14443: Antenna	Power, Control in, Data in, Data out, Status out (Not available in Contact-only configurations)

Table 3 Ports and Interfaces

The following guidance documents will be provided for the TOE:

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

Table 4 TOE Guidance

Above mentioned documents will also be provided along with this ST Lite version and will be delivered by mail in a .pgp encrypted and signed format.

Platform related guidance documents are mentioned in **[PTF-ST]**.

Form factor and Delivery Preparation:

1. In accordance with the software development process of INSI, upon completion of development activities, particular applet will be uploaded into PS in CAP file format.
2. During Release for Sample as project milestone, status of the applet in PS will be changed into "Pilot version" to be used further for manufacturing samples.
3. During Software Delivery Review as the final R&D project milestone, status of the applet in PS will be changed into "Industrial release" to be used further for mass production.

Refer Life Cycle chapter of this ST for more details regarding TOE delivery as per different options.

3.1.2 Logical Scope

The ID-A v1.1 application on ID-One Cosmo X platform is an integrated circuit chip embedding:

- An Operating system providing:
 - Java Card interfaces, as specified in **[JCAPI]**,
 - Extended interfaces for targeted applications needs,
 - A card manager application compliant with the Global Platform v2.3.1 specifications **[GP1]** standard;
- An ID-A application, compliant to the IAS ECC v2 specification **[IAS-ECC]** with extensions for PACE and EAC2 in accordance with **[TR-03110-2]** and **[TR-03110-3]**;
- The Common package. For additional information about each of these parts, please refer TOE guidance;
- The Server Applet Manager package for Global PIN management.

The ID-A v1.1 Application comprises of 3 basic packages, that work together to provide the functionality defined in this Security Target. They are:

1. The ID-A Applet Package, and
2. The Common Package,
3. Server Applet Manager Package.

So, ID-A v1.1 Application will always include ID-A Applet Package, Common Package and Server Applet Manager Package.

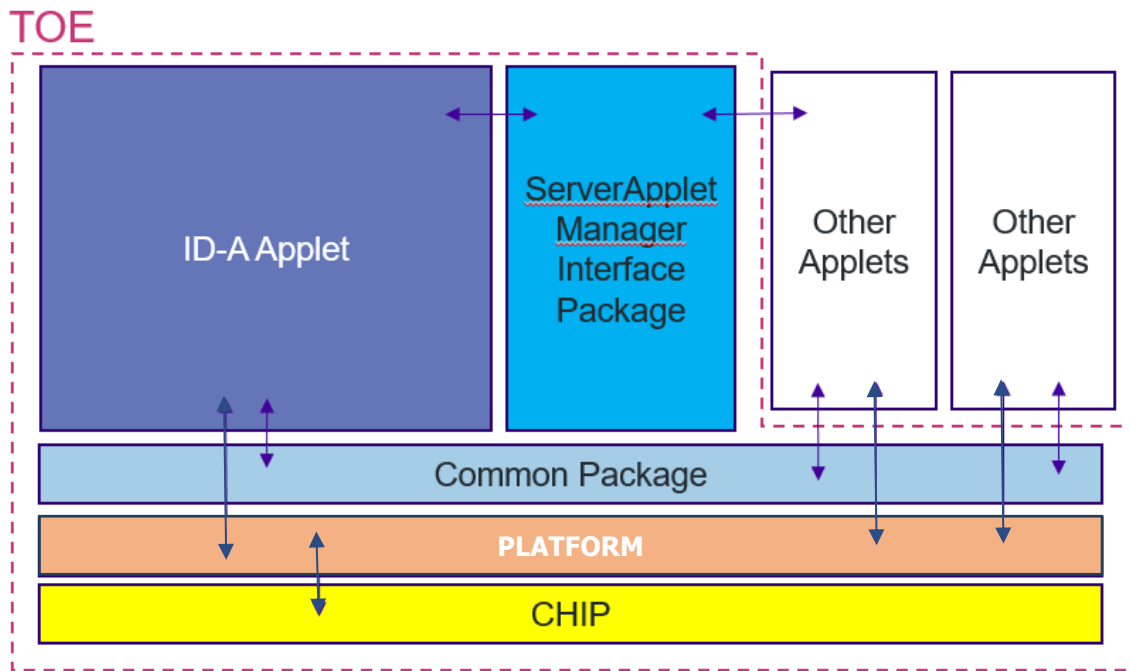


Figure 2: TOE Logical scope

3.2 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.

3.3 TOE Usage and Major Security Features

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 [EU-REG-910/2014].

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 signatures;
- authenticate the cardholder based on a PIN verification;
- authenticate one (or several) administrator(s) of the TOE, that may have special rights to administrate the SCD and SVD (generation, import), using either symmetric and/or asymmetric mechanisms, or PIN verification;
- establish trusted channel, protected in integrity and confidentiality, with Trusted IT entities such as a SCA or a CSP. It may be realized by means of symmetric and/or asymmetric mechanisms.

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

- A super Administrator (TOE_Administrator) has special rights to administrate the signature creation function and the type of cryptographic mechanisms to use;
- SCD/SVD pairs and other cryptographic objects may be generated and/or imported after issuance at any time, and in particular, they may be updated during the TOE life cycle;

- eServices features are added, enabling the cardholder to perform C/S authentication, Encryption key decipherment...;
- A complete access control over objects is ensured, whatever their type is: file or cryptographic objects (PIN, keys,...), ensuring it is not possible to bypass the access rules;
- Personalisation phase including:
 - authentication protocol,
 - access control,
 - encryption mechanism involved in key loading,
 - initialization of the data structure,
 - data loading,
 - locks management,
 - phase switching;
- All authentication protocols (symmetric and asymmetric), and secure messaging type (3DES-112, AES128/192/256);
- All supported digital signature algorithm;
- Authentication of the TOE using symmetric and asymmetric cryptography;
- All PIN management operations available after delivery point;
- Certificate management.

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

- Electronic signature application,
- Electronic health card,
- Electronic services cards.

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).

Since the TOE claims compliancy to protection profiles from EN 419 211-2 to EN 419 211-6 (Signature Protection Profiles **[PP-SSCD2]**, **[PP-SSCD3]**, **[PP-SSCD4]**, **[PP-SSCD5]** and **[PP-SSCD6]**), the TOE can (depending on the desired card profile/issuer policy) be used in the following QSCD/SSCD configurations:

- **SSCD 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]**);
- **SSCD 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;
- **SSCD 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.

The product can have two types of configurations. The first configuration is done at the generation of application code (see the five configurations in chapter 1.3). This configuration can not be changed after generation. The second SSCD_Config# is done at the personalization step of the application.

These two sets of configurations are independents. We can have config (1 to 5) with any SSCD Config#.

The TOE provides the following TOE security features mentioned hereafter.

3.3.1 Authentication mechanisms

This feature realizes the following authentication mechanisms:

- User authentication (PIN);
- External authentication (symmetric and asymmetric role authentication, Terminal Authentication v2);
- Secure messaging (symmetric and asymmetric device authentication, Chip Authentication v2);
- PACE protocol with
 - o support for ECDH in Generic and Integrated Mapping modes (PACE-GM, PACE-IM),
 - o MRZ, CAN, PIN and PUK passwords and
 - o PIN/PUK suspend and resume mechanism (over contactless interface);
- GP authentication in phase 6 (personaliser) and 7 (TOE admin);
- combined device/role authentication.

It also ensures that only authenticated terminals can get access to the user data stored on the TOE.

3.3.2 Cryptographic operations

This feature performs high level cryptographic operations (key generation, symmetric and asymmetric encryption and decryption, signature creation, destruction of cryptographic keys and random number generation). The implementation is mainly based on the Security Functionalities provided by the platform.

3.3.3 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. The TOE provides:

- Secure messaging with external applications as CGA and SCA;
- GP secure messaging in phase 6;
- PACE protocol for 3DES, AES128, AES192 and AES256 [ICAO-9303] and [IAS-ECC] secure messaging;
- TDES for encryption/decryption and MAC generation/verification
- AES128, AES192 and AES256 for encryption/decryption and MAC generation/verification;
- Chip Authentication v2 (CAv2) used to establish new session keys for secure messaging.

This feature is provided by the platform and used for secure messaging.

3.3.4 Access Control function

This feature manages the access to objects (files, directories, data and secrets) stored in the ID-A file system. It ensures secure management of secrets such as cryptographic keys. Access control is enforced by the APDU methods as specified in the interface defined in the functional specification.

3.3.5 Data Storage function

This feature manages the storage of manufacturing data, pre-personalisation data and personalisation data. This covers also the secure storage of SCD/SVD and RAD.

3.3.6 Integrity function

This feature monitors the integrity of sensitive user data and the integrity of the DTBS/R.

3.3.7 Electronic Services

The TOE supports as well several electronic services:

- C/S authentication: this feature enables to authenticate the TOE to an external entity.
- Digital signature: this feature enables the cardholder to electronically signs documents. The signature may be either advanced or qualified (compliant with **[PP-SSCD2]** and **[PP-SSCD3]**);
- Encryption key decipherment: this feature enables the cardholder 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 cardholder's computer sends the encrypted encryption key to the TOE to get the plain encryption key;
- Symmetric encryption and decryption: this feature allows the card to be used as a safe for AES keys.

3.3.8 Keys and PINs management

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

3.3.9 Single Sign on feature (SSO)

The TOE may also behave as a Single Sign on (SSO). It provides access points to any other applet willing to use authentication services based on a PIN.

3.3.10 Features from the Platform

This contains all security functionalities provided by the certified platform (IC and Java Card operation system):

- Protection against malfunctions that are caused by exposure to operating conditions that may cause a malfunction. This includes hardware resets and operation outside the specified norms;
- Protection against tampering and the stored assets can not be retrieved or altered by physical manipulation;
- Protection against physical attack and perform self tests as described in **[PTF-ST]**;
- Security domains are supported by the Java Card platform;
- Cryptographic operations: Signature generation, signature creation and secure messaging, symmetric and asymmetric encryption and decryption and key generation.

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]**.

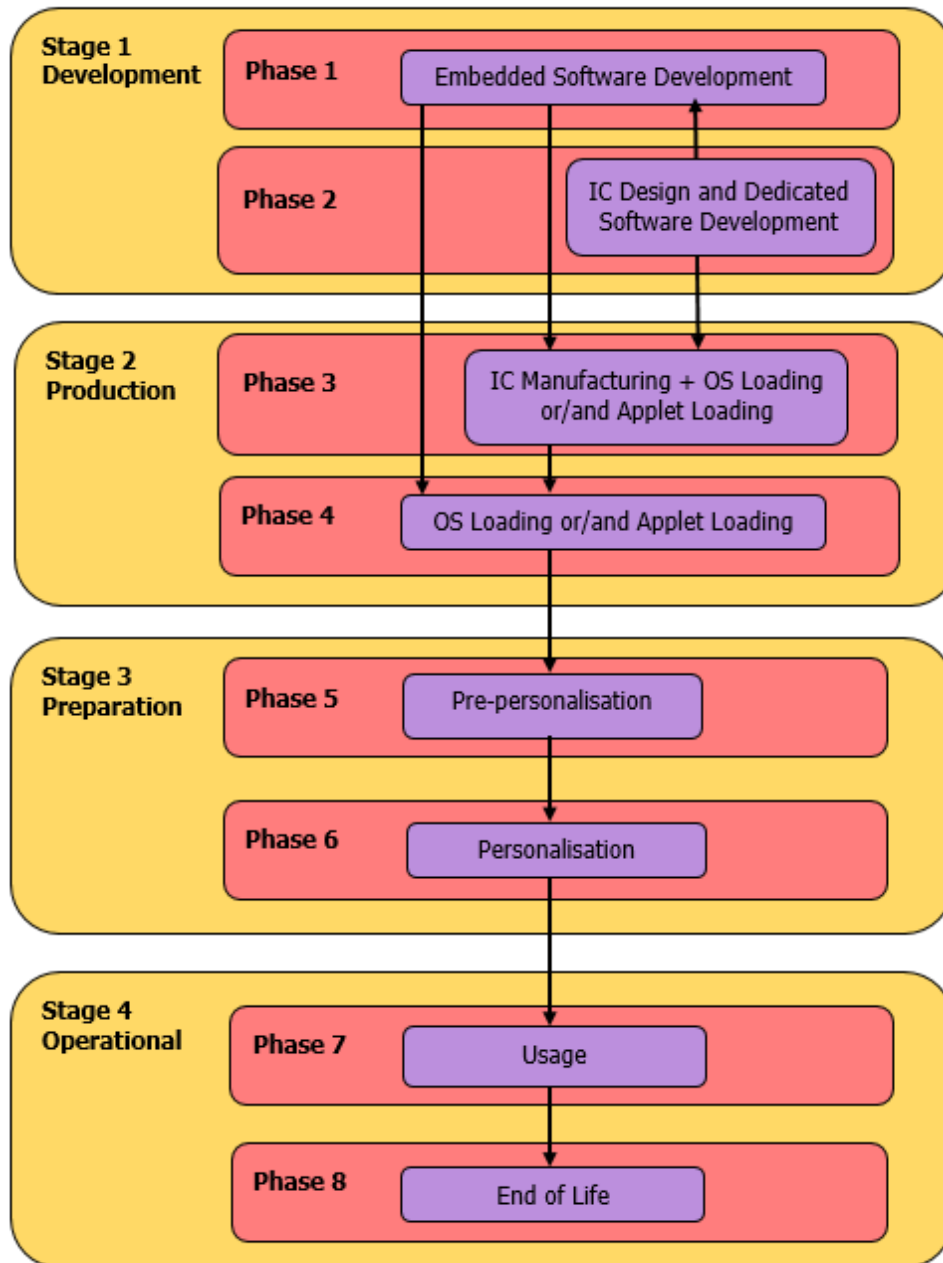


Figure 3 Life cycle Overview

4.1.1 Development Environment

In this environment, the following two phases take place:

- Phase 1: IC Embedded Software Development (Java Card Open Platform components and ID-A applet),
- 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 ID-A applet).

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
ID-A Applet Developer	INSI	MANILA and COURBEVOIE R&D sites	ALC
Embedded Software Developer (Java Card Open Platform)	INSI	Platform Developer (refer to [PTF-ST])	ALC
Redaction and Review of Documents	INSI	MANILA and COURBEVOIE R&D site	ALC
IC Developer	Infineon	IC Manufacturer (refer to [PTF-ST])	ALC

4.1.2 Production Environment

In this environment, the following two phases take place:

- Phase 3: IC Manufacturing,
- Phase 4: ID-One Cosmo X Operating System loading and ID-A v1.1 applet loading.

The ID-A Applet run time code and the Common Package and Server Applet Manager Package is integrated in FLASH of the chip together with the ID-One Cosmo X Operating System.

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

(Option 1) Both ID-One Cosmo X Platform along with ID-A v1.1 application with Common package and Server Applet Manager Package is securely delivered directly from the software developer (INSI R&D CC-audited site) to the **IC Manufacturer** (Infineon CC-audited site) to be loaded into flash. The FLASH image is always encrypted. Decryption is performed by the loader inside the IC.

TOE Delivery point:

- Here, the TOE delivery is considered after Phase 3, as soon as the loading of Java Card Platform package + Applet package (as described below) is complete.

Package	Actor	Site	Covered by
Images containing Java Card Platform OS + Applet and additional packages	IC Manufacturer	IC Manufacturer Production Plants [PTF-ST]	ALC

Table 5 Option 1: Both Platform and Applet packages are loaded at IC Manufacturer site

(Option 2) Both ID-One Cosmo X Platform along with ID-A v1.1 application with Common package and Server Applet Manager Package is securely delivered directly from the software developer (INSI R&D CC-audited site) for loading to **CC-audited INSI or IDEMIA Production sites** or **non-CC-audited INSI sites** or **External sites**.

TOE Delivery points:

- If loading of Java Card Platform package + Applet package (as described below) is done in CC-audited INSI or IDEMIA Production sites then, TOE delivery is considered after Phase 4.
- If loading of Java Card Platform package + Applet package (as described below) is done in non-CC-audited INSI Production sites or External sites then, TOE delivery is considered after Phase 3.

Package	Actor	Site	Covered by
-	-	-	-
Images containing the Java Card Platform OS + Applet and additional packages	INSI or IDEMIA Authorized Entity or External Authorized Agent	CC-audited INSI Production sites (Haarlem, Ostrava) or CC-audited IDEMIA Production sites (Shenzhen, Vitré) or non-CC-audited INSI sites or External sites	ALC or AGD

Table 6 Option 2: Both Platform and Applet packages are loaded at CC-audited INSI or IDEMIA sites or non-CC-audited INSI sites or External sites

(Option 3) Only the ID-One Cosmo X Platform is delivered to the IC Manufacturer (Infineon CC-audited sites) to be loaded.

Next, following options **(3a or 3b (i) or 3b (ii) or 3c)** can be opted for loading applets on top of the platform already loaded.

(Option 3a) ID-A v1.1 Application with Common package and Server Applet Manager Package along with the guidance documentation is securely delivered directly from the Software Developer (INSI R&D CC-audited site) to **CC-audited INSI or IDEMIA Production sites** or **non-CC-audited INSI 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 IC Manufacturer (Infineon).

TOE Delivery points:

- If loading of Applet package on top of already loaded Java Card Platform package (as described below) is done in CC-audited INSI or IDEMIA Production sites then, TOE delivery is considered after Phase 4.
- If loading of Applet package on top of already loaded Java Card Platform package (as described below) is done in non-CC-audited INSI Production sites or External sites then, TOE delivery is considered during Phase 4.

Package	Actor	Site	Covered by
Image containing only Java Card Platform OS	IC Manufacturer	IC Manufacturer Production Plants (refer to [PTF_CERT])	ALC
Applet and additional packages loaded through GP mechanism using CLFDB Key	INSI or IDEMIA Authorized Entity or External Authorized Agent	CC-audited INSI Production sites (Haarlem, Ostrava) or CC-audited IDEMIA Production sites (Shenzhen, Vitré) or non-CC-audited INSI sites or External sites	ALC or AGD

Table 7 Option 3(a): Platform package is loaded at IC Manufacturer site and Applet package is loaded at CC-audited INSI or IDEMIA sites or non-CC-audited INSI sites or External sites through GP Mechanism

(Option 3b)

- (i) ID-A v1.1 Application with Common package and Server Applet Manager Package along with the guidance documentation is securely delivered directly from the Software Developer (INSI R&D CC-audited site) to **CC-audited INSI or IDEMIA Production sites** or **non-CC-audited INSI sites** or **External sites**.
Loading of Applet in any of these sites is done through Resident Application using LSK format on top of the platform already loaded by IC Manufacturer (Infineon).
- (ii) DUMP package (including ID-A v1.1 Application with Common package data and Server Applet Manager Package) with the guidance documentation is securely delivered directly from the Software Developer (INSI R&D CC-audited site) to **CC-audited INSI or IDEMIA Production sites** or **non-CC-audited INSI sites** or **External sites**.
Loading of DUMP PACKAGES in any of these sites is done through Resident Application using DSK secret live 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 Java Card Platform package (as described below) is done in CC-audited INSI or IDEMIA Production sites then, TOE delivery is considered after Phase 4.
- If loading of Applet package /DUMP Package on top of already loaded Java Card Platform package (as described below) is done in non-CC-audited INSI Production sites or External sites then, TOE delivery is considered during Phase 4.

Package	Actor	Site	Covered by
Image containing only Java Card Platform OS	IC Manufacturer	IC Manufacturer Production Plants (refer to [PTF_CERT])	ALC
3b (i) Applet and additional packages loaded through Resident Application using LSK format	INSI or IDEMIA Authorized Entity or External Authorized Agent	CC-audited INSI Production sites (Haarlem, Vitré,) or CC-audited IDEMIA Production sites (Shenzhen, Vitré) or non-CC-audited INSI sites or External sites	ALC or AGD
3b (ii) DUMP PACKAGE Ciphred format [DSK Secret Live Key]	INSI or IDEMIA Authorized Entity		

Table 8 Platform package is loaded at IC Manufacturer site and 3b (i) Applet package is loaded through resident application using LSK format and 3b (ii) DUMP Package is loaded through resident application using DSK Secret Live Key - at CC-audited INSI or IDEMIA sites or non-CC-audited INSI sites or External sites

(Option 3c) ID-A v1.1 Application with Common package and Server Applet Manager Package along with the guidance documentation is securely delivered directly from the Software Developer (INSI R&D CC-audited site) to **CC-audited INSI Production sites**.

Here, there is a provision of loading the applet in plain format in **CC-audited INSI sites only**, on top of the platform already loaded by IC Manufacturer (Infineon). This applet loading in plain format is not allowed neither in non-CC-audited INSI sites nor in CC-audited IDEMIA sites nor External sites.

TOE Delivery points:

- Here, since the loading of Applet package on top of already loaded Java Card Platform package (as described below) is done Plain format in CC-audited INSI Production sites, so TOE delivery is considered after Phase 4.

Package	Actor	Site	Covered by
Image containing only Java Card Platform OS	IC Manufacturer	IC Manufacturer Production Plants (refer to [PTF_CERT])	ALC
Applet and additional packages in Plain Format	INSI Authorized Entity	CC-audited INSI Production sites (Haarlem, Vitré,)	ALC

Table 9 Option 3(c): Platform package is loaded at IC Manufacturer site and Applet package in plain format is loaded at CC-audited INSI sites only

(Option 4) Only ID-One Cosmo X Platform is securely delivered directly from the software developer (INSI R&D CC-audited site) for loading to **CC-audited INSI or IDEMIA Production sites** or **non-CC-audited INSI sites** or **External sites**.

Note: Here, when the Platform package is loaded in non-CC-audited INSI sites or External sites, then the Platform is in self-protected mode by its secure functions

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

(Option 4a) ID-A v1.1 Application with Common package and Server Applet Manager Package along with the guidance documentation is securely delivered directly from the Software Developer (INSI R&D CC-audited site) to **CC-audited INSI or IDEMIA Production sites** or **non-CC-audited INSI 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 INSI or IDEMIA Production sites** or **non-CC-audited INSI sites** or **External sites**.

TOE Delivery points:

- If loading of Applet package on top of already loaded Java Card Platform package (as described below) is done in CC-audited INSI or IDEMIA Production sites then, TOE delivery is considered after Phase 4.
- If loading of Applet package on top of already loaded Java Card Platform package (as described below) is done in non-CC-audited INSI or IDEMIA Production sites or External sites then, TOE delivery is considered during Phase 4.

Package	Actor	Site	Covered by
Image containing only Java Card Platform OS	INSI or IDEMIA Authorized Entity or External Authorized Agent	CC-audited INSI Production sites (Haarlem, Ostrava) or CC-audited IDEMIA Production sites (Shenzhen, Vitré) or non-CC-audited INSI sites or External sites	ALC or AGD
Applet and additional packages loaded through GP mechanism using CLFDB Key	INSI or IDEMIA Authorized Entity or External Authorized Agent	CC-audited INSI Production sites (Haarlem, Ostrava) or CC-audited IDEMIA Production sites (Shenzhen, Vitré) or non-CC-audited INSI sites or External sites	ALC or AGD

Table 10 Option 4(a): Platform package is loaded at CC-audited INSI or IDEMIA sites or non-CC-audited INSI sites or External sites and Applet package is loaded at CC-audited INSI or IDEMIA sites or non-CC-audited INSI sites or External sites through GP Mechanism

(Option 4b)

- (i) ID-A v1.1 Application with Common package and Server Applet Manager Package along with the guidance documentation is securely delivered directly from the Software Developer (INSI R&D CC-audited site) to **CC-audited INSI or IDEMIA Production sites** or **non-CC-audited INSI sites** or **External sites**.
Loading of Applet in any of these sites is done through Resident Application using LSK format on top of the platform already loaded by **CC-audited INSI or IDEMIA Production sites** or **non-CC-audited INSI sites** or **External sites**.
- (ii) DUMP package (including ID-A v1.1 Application with Common package data and Server Applet Manager Package) with the guidance documentation is securely delivered directly from the Software Developer (INSI R&D CC-audited site) to **CC-audited INSI or IDEMIA Production sites** or **non-CC-audited INSI sites** or **External sites**.
Loading of DUMP PACKAGES in any of these sites is done through Resident Application using DSK secret live key on top of the platform already loaded by **CC-audited INSI or IDEMIA Production sites** or **non-CC-audited INSI sites** or **External sites**.

TOE Delivery points:

- If loading of Applet package /DUMP Package on top of already loaded Java Card Platform package (as described below) is done in CC-audited INSI or IDEMIA Production sites then, TOE delivery is considered after Phase 4.
- If loading of Applet package /DUMP Package on top of already loaded Java Card Platform package (as described below) is done in non-CC-audited INSI Production sites or External sites then, TOE delivery is considered during Phase 4.

Package	Actor	Site	Covered by
Image containing only Java Card Platform OS	INSI or IDEMIA Authorized Entity or External Authorized Agent	CC-audited INSI Production sites (Haarlem, Ostrava) or CC-audited IDEMIA Production sites (Shenzhen, Vitré) or non-CC-audited INSI sites or External sites	ALC or AGD
4b (i) Applet and additional packages loaded through Resident Application using LSK format	INSI or IDEMIA Authorized Entity or External Authorized Agent	CC-audited INSI Production sites (Haarlem, Ostrava) or CC-audited IDEMIA	ALC or AGD

4b (ii) DUMP PACKAGE Ciphred format [DSK Secret Live Key]	INSI or IDEMIA Authorized Entity	Production sites (Shenzhen, Vitré) or non-CC-audited INSI sites or External sites	
--	-------------------------------------	--	--

Table 11 Platform package is loaded at CC-audited INSI or IDEMIA sites or non-CC-audited INSI sites or External sites and 4b (i) Applet package is loaded through Resident application using LSK format and 4b (ii) DUMP Package is loaded through resident application using DSK Secret Live Key - at CC-audited INSI or IDEMIA sites or non-CC-audited INSI sites or External sites

(Option 4c) ID-A v1.1 Application with Common package and Server Applet Manager Package along with the guidance documentation is securely delivered directly from the Software Developer (INSI R&D CC-audited site) to **CC-audited INSI Production sites**.

Here, there is a provision of loading the applet in plain format in **CC-audited INSI sites only**, on top of the platform already loaded by CC-audited INSI or IDEMIA Production sites or non-CC-audited INSI sites or External sites. This applet loading in plain format is not allowed in neither non-CC-audited INSI sites nor CC-audited IDEMIA sites nor External sites.

TOE Delivery points:

- Here, since the loading of Applet package on top of already loaded Java Card Platform package (as described below) is done in Plain format in CC-audited INSI Production sites, so TOE delivery is considered after Phase 4.

Package	Actor	Site	Covered by
Image containing only Java Card Platform OS	INSI or IDEMIA Authorized Entity or External Authorized Agent	CC-audited INSI Production sites (Haarlem, Ostrava) or CC-audited IDEMIA Production sites (Shenzhen, Vitré) or non-CC-audited INSI sites or External sites	ALC or AGD
Applet and additional packages in Plain Format	INSI Authorized Entity	CC-audited INSI Production sites (Shenzhen, Haarlem, Vitré, Ostrava)	ALC

Table 12 Option 4(c): Platform package is loaded at CC-audited INSI or IDEMIA sites or non-CC-audited INSI sites or External sites and Applet package in plain format is loaded at CC-audited INSI sites only

4.1.3 Preparation Environment

All along this phase, the TOE is self-protected as it requires the authentication of the personalisation agent prior to any operation. During this phase, creation of ID-A SSCD applet instance is mandatory.

This phase consists of:

- 1) SSCD ID-A applet instance creation of MF for the loaded configuration according to **[AGD_PRE]**.
- 2) Personalisation according to **[AGD_PRE]**:
 - a. RAD storage on SSCD (optional)
 - b. [OPTIONAL] Creation of SCD/SVD pair
 - i. by the TOE through the SCD/SVD generation functionality or
 - ii. by the Personalisation Agent, who loads the SCD and/or SVD into the TOE.
 - c. [OPTIONAL] export of SVD to CGA.
 - d. [OPTIONAL] storing back the obtained certificates
 - e. [OPTIONAL] depending on SSCD Config#1 or SSCD Config2#, required trusted channel cryptographic keys and mechanisms (e.g. PACE, EAC2, IAS-ECC CV certificates) for secure messaging with SCA and CGA.
- 3) Post-perso steps including: (i) ISD life-cycle management; (ii) disabling access to the Global Platform ISD (Card Manager) in order to prevent post issuance applet loading.

Application note:

Personalisation steps 2b, 2c and 2d are not mandatory in preparation phase as they may be performed in operational phase of the TOE as well. Personalisation steps 2e is optional because it is not required for the SSCD Config#3.

4.1.4 Operational Environment

The TOE in this phase is under the control of the User (Signatory and/or Administrator).

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 **[PTF_AGD2]** and **[PTF_AGD3]** tasks of **[PTF-ST]**.

5 Conformance Claims

5.1 CC Conformance

This security target claims conformance to the Common Criteria version 2022, revision 1 ([**CC-1**], [**CC-2**], [**CC-3**], [**CC-5**], [**CC-ERRATA**] and [**CEM**]).

The conformance to the Common Criteria is claimed as follows:

CC	Conformance rationale
Part 1 [CC-1]	Conformant
Part 2 [CC-2]	Conformant
Part 3 [CC-3]	Conformant
Part 5 [CC-5]	Conformant
Errata [CC-ERRATA]	Conformant
[CEM]	Conformant

The TOE also includes:

- ID-One Cosmo X Platform,
- The Infineon IC.

5.2 PP Claims

This security target claims strict conformance to the following PPs: [**PP-SSCD2**], [**PP-SSCD3**], [**PP-SSCD4**], [**PP-SSCD5**], [**PP-SSCD6**].

5.3 Package Claim

This ST is conforming to assurance package EAL5 augmented with ALC_DVS.2, AVA_VAN.5 and ALC_FLR.3 defined in CC part 5 [**CC-5**].

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 claims demonstrable conformance to the above mentioned PPs [**PP-SSCD2**], [**PP-SSCD3**], [**PP-SSCD4**], [**PP-SSCD5**], [**PP-SSCD6**]. A detailed justification is given in the following.

5.4.1 Security Problem Definition

The SPD of this ST contains the security problem definition present in [**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 as shown in the following table.

TOE SPDs	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
Assumptions						
A.CGA	x	x	x	x	x	x
A.SCA	x	x	x	x	x	x
A.CSP		x			x	x
Threats						
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
Organisational Security Policies						
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

5.4.2 Security Objectives

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:

- the security objectives OT.TOE_TC_VAD_Imp and OT.TOE_TC_DTBS_Imp from **[PP-SSCD5]** and **[PP-SSCD6]**,
- the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp from **[PP-SSCD4]**.

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
Objectives for the TOE						
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

TOE Objectives	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
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

5.4.3 Assumptions

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;

5.4.4 Security Objectives

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.HID_VAD, OE.DTBS_Protect and OE.SSCD_Prov_Service:

- this ST adapts OE.HID_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]**:

- the OE.HIP_VAD, OE.DTBS_Protect for SSCD config#2 is added,
- the OE.HIP_VAD, OE.DTBS_Protect and OE.SSCD_Prov_Service for SSCD config#3 is added.

5.4.5 Security functional requirement

The SFRs specified in this ST includes all SFRs (including the part of extended components) specified in the **[PP-SSCD2]**, **[PP-SSCD3]**, **[PP-SSCD4]**, **[PP-SSCD5]**, **[PP-SSCD6]** with following exceptions:

- in case a SFR from **[CC-2]** is also in Extended components chapter in PPs then the one from **[CC-2]** will be the reference. Details are given in section 5.4.5.1,
- in case a SFR from **[CC-2]** is also in PPs (Extended components chapter excluded) differs from each other then the one from **[CC-2]** will be the reference. Details are given in section 5.4.5.2.

Additional SFRs are added and address:

- 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.
- trusted communication with CGA from **[PP-SSCD4]**: FIA_API.1 and FDP_DAU.2/SVD, FTP_ITC.1/SVD;

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	×		×	×		×
FCS_COP.1	×	×	×	×	×	×
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/Signature_Creation	×	×	×	×	×	×

TOE SFRs	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
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/Signatory	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/Admin	x	x	x	x	x	x
FMT_MTD.1/Signatory	x	x	x	x	x	x
FPT_EMS.1fpt_emsec	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

TOE SFRs	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
FCS_RND.1						×

Table 15 PP SFRs vs. ST

5.4.5.1 PP vs CC for Extended Components

Extended Components are defined in **[PP-SSCD2]**, **[PP-SSCD3]**, **[PP-SSCD4]**, **[PP-SSCD5]**, **[PP-SSCD6]**. Some of them are now defined in **[CC-2]**. In such a case, **[CC-2]** definition is taken and applied to this TOE. List is as following:

SFR in [PP-SSCD2] , [PP-SSCD3] , [PP-SSCD4] , [PP-SSCD5] , [PP-SSCD6]	SFR in [CC-2]	Comments
FPT_EMS.1	FPT_EMS.1	
FPT_EMS.1.1	FPT_EMS.1.1	- Table creation to summarize the emissions and matching parameters
FPT_EMS.1.2	<i>Not Applicable</i>	- SFR removed
FIA_API.1	FIA_API.1	
FIA_API.1.1	FIA_API.1.1	- Light modification of the sentence - Addition of list of properties

5.4.5.2 PP vs CC for generic SFR

Table below indicates SFR present in **[PP-SSCD2]**, **[PP-SSCD3]**, **[PP-SSCD4]**, **[PP-SSCD5]**, **[PP-SSCD6]** and in **[CC-2]** with a difference on their definition or dependencies. List is as following:

SFR in [PP-SSCD2] , [PP-SSCD3] , [PP-SSCD4] , [PP-SSCD5] , [PP-SSCD6]	SFR in [CC-2]	Comments
FCS_CKM.1	FCS_CKM.1	- change in dependencies
FCS_CKM.1.1	FCS_CKM.1.1	- change in definition
FCS_CKM.4	FCS_CKM.6	- FCS_CKM.4 withdrawn and replaced by FCS_CKM.6 - New dependency compared to FCS_CKM.4
-	FCS_CKM.6.1	- New point
FCS_CKM.4.1	FCS_CKM.6.2	- Renamed and change in definition
FCS_COP.1	FCS_COP.1	- change in dependencies
FCS_COP.1.1	FCS_COP.1.1	- change in definition
FPT_PHP.1	FPT_PHP.1	
FPT_PHP.1.1	FPT_PHP.1.1	- change in definition
FPT_TST.1	FPT_TST.1	
FPT_TST.1.1	FPT_TST.1.1	- Light modification of the sentence - Addition of list of properties

5.4.6 Security Assurance Requirements

The security assurance requirements (SARs) are originally taken from SARs of part 3 **[CC-3]** according to the package conformance EAL 5 augmented with ALC_DVS.2, AVA_VAN.5 and ALC_FLR.3 (the Evaluation Assurance Level EAL5+ of the current ST exceeds the EAL4+ defined by **[PP-SSCD2]**, **[PP-SSCD3]**, **[PP-SSCD4]**, **[PP-SSCD5]**, **[PP-SSCD6]**).

5.4.7 Threats

Additional Threats not related to **[EAC2-PP]** have been added to the TOE:

- T.Authentication_Replay to cover the threats when an attacker retrieves an authentication cryptogram
- T.Key_Derive to cover the threats on the eServices_keys via public know data

To respond to the T.Authentication_Replay an additional Security Objectives not related to **[EAC2-PP]** has been added: OT.Authentication_Secure

To respond to the T.Key_Derive two additional Security Objectives not related to **[EAC2-PP]** have been added: OT.Authentication_Secure and **OT.eServices**

5.4.8 Organisational Security Policy

E services mechanisms not related to **[EAC2-PP]** have been added to the TOE to provide services:

- One Organisational Security Policy: **P.eServices** covered by OT.eServices

5.4.9 Additional functionalities impacts on the TOE

The additional functionalities (PACE authentication, Chip Authentication Protocol Version 2 and Terminal Authentication Protocol Version 2) have been added to the TOE with: (i) additional security problem definition; (ii) additional security objectives; (iii) additional SFRs. Some additions are inspired from the **[EAC2-PP]**. 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.

6 Security Problem Definition

6.1 Assets

6.1.1 *Primary Assets drawn from the protection profiles*

Following primary assets are protected by the TOE as listed below:

D.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 must be maintained.

D.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 must be maintained.

D.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 must be maintained.

6.1.2 *Primary Assets related to EAC2*

Authenticity of the Electronic Documents Chip

The authenticity of the electronic document's chip, personalised by the issuing state or organization for the electronic document holder, is used by the electronic document presenter to prove his possession of a genuine electronic document. Generic Security Property: Authenticity

Tracing Data

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

Generic Security Property: Unavailability

Sensitive User Data

User data, which have been classified as sensitive data by the electronic document issuer, e. g. sensitive biometric data. Sensitive user data are a subset of all user data, and are protected by EAC2.

Generic Security Properties: Confidentiality, Integrity, Authenticity

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 PACE terminal, or, in the case of sensitive data, by an EAC2 terminal with appropriate authorization level.

Generic Security Properties: Confidentiality, Integrity, Authenticity

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.

Generic Security Properties: Confidentiality, Integrity, Authenticity

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.

Generic Security Property: Availability

Genuineness of the TOE

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

Generic Security Property: Availability

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 sent to it.

Restricted-revealable here refers to the fact that if necessary, the electronic document holder may reveal her verification values of CAN to an authorized person, or to a device that acts according to respective regulations and is considered trustworthy.

Generic Security Properties: Confidentiality, Integrity

Secret Electronic Document Holder Authentication Data

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

Generic Security Properties: Confidentiality, Integrity

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. An example for such non-secret material is the document security object (SOD) that contains a digital signature.

Generic Security Properties: Integrity, Authenticity

TOE internal Secret Cryptographic Keys

Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.

Generic Security Properties: Confidentiality, Integrity

Application Note:

Data for electronic document holder authentication and for authorization of communication with the electronic document can be categorized as (i) reference information that are persistently stored within the TOE, and (ii) verification information for the TOE that are input by a human user during an authentication and/or authorization attempt. The TOE shall secure both reference information, and, together with the connected terminal, verification information that are transferred in the channel between the TOE and the terminal.

6.2 Users / Subjects

6.2.1 Subjects drawn from the protection profiles

S.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.

S.Admin

User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator.

S.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 Additional Users/Subjects

S.CSCA

Country Signing Certification Authority

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 CSCA represents the country specific root of the public key infrastructure (PKI) for the electronic document, and creates Document Signer Certificates within this PKI. The CSCA also issues a self-signed CSCA certificate that has to be distributed to other countries by secure diplomatic means, see [ICAO-9303].

S.CVCA

Country Verifying Certification Authority

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

EAC2 terminals, and creates Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed as CVCA Link-Certificates **[TR-03110-3]**.

S.DS

Document Signer

An organization enforcing the policy of the CSCA. A DS signs the Document Security Object (SOD) that is stored on the electronic document for Passive Authentication. A Document Signer is authorized by the national CSCA that issues Document Signer Certificates, see **[ICAO-9303]**. Note that this role is usually delegated to a Personalisation Agent.

S.DV

Document Verifier

An organization issuing terminal certificates. The DV is a Certificate Authority, authorized by the corresponding CVCA to issue certificates for EAC2 terminals **[TR-03110-3]**.

S.EDH

Electronic Document Holder

A person who the electronic document issuer has personalised the electronic document for. Personalisation here refers to associating a person uniquely with a specific electronic document. Note that an electronic document holder can also be an attacker. The electronic document holder is equivalent to the signatory and can use and manage the PIN and the PUK.

S.EDP

Electronic Document Presenter

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

S.Manufacturer

Generic term comprising both the IC manufacturer that produces the integrated circuit, and the electronic document manufacturer that creates the electronic document and attaches the IC to it. The manufacturer is the default user of the TOE during the manufacturing life cycle phase. When referring to the role manufacturer, the TOE itself does not distinguish between the IC manufacturer and the electronic document manufacturer.

S.PACE Terminal

A PACE terminal 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, PIN or PUK). A PACE terminal is not allowed to access sensitive user data.

S.Personalisation Agent

An organization acting on behalf of the electronic document issuer that personalises the electronic document for the electronic document holder. Personalisation includes some or all of the following activities: (i) establishing the identity of the electronic document holder for the biographic data in the electronic document, (ii) enrolling the biometric reference data of the electronic document holder, (iii) writing a subset of these data on the physical

electronic document (optical personalisation) and storing them within the electronic document's chip (electronic personalisation), (iv) writing document meta data (i. e. document type, issuing country, expiry date, etc.) (v) writing the initial TSF data, and (vi) signing the Document Security Object, and the elementary files EF.CardSecurity and the EF.ChipSecurity (if applicable **[ICAO-9303]**, **[TR-03110-3]**) in the role DS. Note that the role personalisation agent may be distributed among several institutions according to the operational policy of the electronic document issuer.

S.EAC2 Terminal

A terminal that has successfully passed Terminal Authentication 2 is an EAC2 terminal. It is authorized by the electronic document issuer through the Document Verifier of the receiving branch (by issuing terminal certificates) to access a subset or all of the data stored on the electronic document.

S.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 PACE terminal nor an EAC2 terminal.

6.2.3 Threat agents

S.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.

6.3 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 SDO for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

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 which 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 Threats related to EAC2**T.Counterfeit/EAC2**

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 a 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 of the electronic document's chip. The attack T.Sensitive_Data is similar to the threat T.Skimming from [PACE-PP] 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) and therefore the possible attack methods.

Threat agent: having high attack potential, knowing the PACE Password, 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 initialisation and personalisation in the operational phase after delivery to the electronic document holder.

T.Eavesdropping

An attacker is listening to the communication between the electronic document and the PACE authenticated BIS-PACE 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 PACE authenticated BIS-PACE by means of changed electronic document holder's related reference data (like biographic or biometric 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's 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 electronic document.

T.Skimming

An attacker imitates an inspection system in order to get access to the user data stored on or transferred between the TOE and the inspecting authority connected via the contactless/contact 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/contact interface of the TOE.

6.3.3 Added Threats

T.Key_Derive

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.Authentication_Replay

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.

6.4 Organisational Security Policies

6.4.1 OSPs 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. the directive, article 2, clause 9, and Annex I **[DIR]**) 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 1, clause 2 **[DIR]**), which is a qualified electronic signature if it is based on a valid qualified certificate (according to the directive Annex I **[DIR]**). 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.

Application Note:

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

P.Sigy_SSCD

TOE as secure signature creation device

The TOE meets the requirements for an SSCD laid down in Annex III of the directive **[DIR]**. 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 OSP related to EAC2

P.EAC2_Terminal

Terminals that intent to be EAC2 terminals must implement the respective terminal part of the protocols required to execute EAC version 2 according to **[TR-03110-2]**, 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 personalisation agent or the manufacturer.

P.Card_PKI

PKI for Passive Authentication (issuing branch)

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 for the passive authentication, i.e. for digital signature creation and verification for the electronic document. For this aim, he runs a Country Signing Certification Authority (CSCA). The electronic document Issuer shall publish the CSCA Certificate (CCSCA). 2.)The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (CCSCA) having to be made available to the electronic document Issuer by strictly secure means. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the electronic document Issuer, see. 3.)A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep the Document Signer Private Key secret and (iv) securely use the Document Signer Private Key for signing the Document Security Objects of electronic documents.

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.

P.Pre-Operational

- 1.)The electronic document Issuer issues the electronic document and approves it using the terminals complying with all applicable laws and regulations.
- 2.)The electronic document Issuer guarantees correctness of the user data (amongst other of those, concerning the electronic document holder) and of the TSF-data permanently stored in the TOE28.
- 3.)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, cf. sec. 1.2.3 above.
- 4.)If the electronic document Issuer authorises a Personalisation Agent to personalise the electronic document for electronic document holders, the electronic document Issuer has to ensure that the Personalisation Agent acts in accordance with the electronic document Issuer's policy.

P.Terminal

The Basic Inspection Systems with PACE (BIS-PACE) shall operate their terminals as follows:

- 1.)The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by electronic document holders.
- 2.)They shall implement the terminal parts of the PACE protocol, of the Passive Authentication and use them in this order. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
- 3.)The related terminals need not to use any own credentials.
- 4.)They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the electronic document).
- 5.)The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

P.Trustworthy_PKI

The CSCA shall ensure that it issues its certificates exclusively to the rightful organisations (DS) and DSs shall ensure that they sign exclusively correct Document Security Objects to be stored on the electronic document.

6.4.3 Added OSP

P.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.

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.Tamper_Resistance

Tamper resistance

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

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.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.DTBS_Integrity_TOE

DTBS/R integrity inside the TOE

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

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.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.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.

Application Note:

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

OT.Lifecycle_Security

Lifecycle security

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

Application Note:

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

7.1.2 SSCD parts 2, 4 and 5 only

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.

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_Auth_Gen

Authorized 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.

7.1.3 SSCD parts 3 and 6 only

OT.SCD_Auth_Imp

Authorized SCD import

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

7.1.4 SSCD part 4 only

OT.TOE_SSCD_Auth

Authentication proof as SSCD

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

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 must not generate electronic signatures with the SCD for altered DTBS.

7.1.6 Additional Security Objectives for the TOE**OT.AC_Pers_EAC2*****Personalisation 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 personalisation agents only, with the following exception: An EAC2 terminal may also write or modify user data according to its effective access rights. The access rights are determined by the electronic document during Terminal Authentication 2. Justification: This security objective for the TOE modifies OT.AC_Pers from **[PACE-PP]** as the additional features of EAC2 allow a strongly controlled, secure and fine-grained access to individual data groups of the electronic document.

OT.CA2***Proof of the Electronic Document's Chip Authenticity***

The TOE must allow EAC2 terminals to verify the identity and authenticity of the electronic document's chip as being issued by the identified issuing state or organization by Chip Authentication 2 **[TR-03110-2]**. The authenticity of the chip and its proof mechanism provided by the electronic document's chip shall be protected against attacks with high attack potential.

OT.Sens_Data_EAC2***Confidentiality of sensitive User Data***

The TOE must ensure confidentiality of sensitive user data by granting access to sensitive data only to EAC2 terminals with corresponding access rights. The authorization of an EAC2 terminal is the minimum set of the access rights drawn from the terminal certificate used for successful authentication and the corresponding DV and CVCA certificates, and the access rights sent to the electronic document as part of PACE. The TOE must ensure confidentiality of all user data during transmission to an EAC2 terminal after Chip Authentication 2. Confidentiality of sensitive user data shall be protected against attacks with high attack potential.

OT.Data_Authenticity***Authenticity of Data***

The TOE must ensure authenticity of the User Data and the TSF-data stored on it by enabling verification of their authenticity at the terminal-side. The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE).

OT.Data_Confidentiality***Confidentiality of Data***

The TOE must ensure confidentiality of the User Data and the TSF-data by granting read access only to the PACE authenticated BIS-PACE connected. The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

OT.Data_Integrity***Integrity of Data***

The TOE must ensure integrity of the User Data and the TSF-data stored on it by protecting these data against unauthorised modification (physical manipulation and unauthorised modifying). The TOE must ensure integrity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

OT.Identification***Identification of the TOE***

The TOE must provide means to store Initialisation 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.Prot_Abuse-Func***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.

OT.Prot_Inf_Leak

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 electronic 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.

Application Note:

This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

OT.Prot_Malfunction

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.

OT.Prot_Phys-Tamper

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.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/contact interface of the TOE without knowledge of the correct values of shared passwords (PACE passwords) in advance.

Application Note:

Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the electronic document's chip (no Chip Authentication), a security objective like OT.Chip_Auth_Proof (proof of electronic document authenticity) cannot be achieved by the current TOE.

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

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 the TOE is under the sole control of the Personalisation Agent. The following operation may be realized:

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

OT.eServices

Provision of eServices The TOE provides eServices Mechanisms enabling to:

- o decrypt encryption keys
- o authenticate the TOE
- o verify CVC certificates Moreover, the TOE ensures the key its uses are genuine by enforcing an access control over the keys update, in order to ensure that only entitled entities can change key values.

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

7.2 Security Objectives for the Operational Environment

7.2.1 All SSCD parts

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.

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.

Application Note:

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

OE.SVD_Auth

Authenticity of the SVD The operational environment shall ensure the authenticity and 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)

- o the name of the signatory controlling the TOE,
- o the SVD matching the SCD stored in the TOE and being under sole control of the signatory,
- o 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.

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 will ensure confidentiality and integrity of the VAD as needed by the authentication method employed from import through its human interface until import through the TOE interface.

OE.DTBS_Protect***SCA protects the data intended to be signed***

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

7.2.3 SSCD part 2, 3, 5 and 6 only**OE.SSCD_Prov_Service*****Authentic SSCD provided by SSCD Provisioning Service***

The SSCD Provisioning Service handles authentic devices that implement the TOE to be prepared for the legitimate user as signatory personalises and delivers the TOE as SSCD to the signatory.

7.2.4 SSCD parts 3 and 6 only**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.

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_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/SVD_Auth_Gen***Authorized 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.

7.2.5 SSCD part 4 only**OE.Dev_Prov_Service*****Authentic SSCD provided by SSCD Provisioning Service***

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

Application Note:

This objective replaces OE.SSCD_Prov_Service from the core PP, which is possible as it does not imply any additional requirements for the operational environment when compared to OE.SSCD_Prov_Service (OE.Dev_Prov_Service is a subset of OE.SSCD_Prov_Service).

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 SSCD.

OE.CGA_SSCD_Auth***Pre-initialisation of the TOE for SSCD authentication***

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

7.2.6 SSCD 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_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.

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_Imp. 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_Imp and leaves only the necessary functionality by the SCA.

7.2.7 Additional Security Objectives for the Operational Environment

OE.Chip_Auth_Key

Key Pairs needed for Chip Authentication

The electronic document issuer has to ensure that the electronic document's chip authentication key pair is generated securely, that the private key of this key pair is stored correctly in the electronic document's chip, and that the corresponding public keys are distributed to the EAC2 terminals that are used according to **[TR-03110-2]** to check the authenticity of the electronic document's chip. Justification: The TSF of **[PACE-PP]** does not include any mechanism to verify the authenticity of an electronic document (i.e. protection against cloning). Therefore, this additional security objective for the operational environment does not mitigate any threat of, and does not fulfill any OSP of **[PACE-PP]**.

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 personalisation agent or the manufacturer. Justification: The TSF of **[PACE-PP]** does not include any mechanism to verify the authenticity of the terminal that reads out the data stored on the electronic document (by successfully executing PACE, a terminal only proves knowledge of the PACE password). Therefore, this additional security objective for the operational environment does not mitigate any threat of, and does not fulfill any OSP of **[PACE-PP]**.

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 CSCA acting on behalf and according to the policy of the electronic document Issuer must (i) generate a cryptographically secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) publish the Certificate of the CSCA Public Key (CCSCA). Hereby authenticity and integrity of these certificates are being maintained. A Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographically secure Document Signing Key Pair, (ii) ensure the secrecy of the Document Signer Private Key, (iii) hand over the Document Signer Public Key to the CSCA for certification, (iv) sign Document Security Objects of genuine electronic documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [6]. The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on electronic document.

OE.Personalisation

Personalisation of ID document

The electronic document Issuer must ensure that the Personalisation Agents acting on his behalf (i) establish the correct identity of the electronic document holder and create the biographical data for the electronic document, (ii) enrol the biometric reference data of the electronic document holder, (iii) write a subset of these data on the physical Passport (optical personalisation) and store them in the electronic document (electronic personalisation) for the electronic document holder as defined in [6], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [6] (in the role of a DS).

OE.Terminal

Terminal operating

The terminal operators must operate their terminals as follows: 1)The related terminals (basic inspection systems, cf. above) are used by terminal operators and by electronic document holders.

2)The related terminals implement the terminal parts of the PACE protocol, of the Passive Authentication(by verification of the signature of the Document Security Object) and use them in this order. The PACE terminal uses randomly and (almost)uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

3)The related terminals need not to use any own credentials.

4)The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication of the electronic document (determination of the authenticity of data groups stored in the electronic document).

5)The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

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 to an authorized person or device who definitely act according to respective regulations and are trustworthy.

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.

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 **[DIR]**, recital (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 authorized 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. OT.SCD/SVD_Gen counters this threat by implementing cryptographically secure generation of the SCD/SVD pair. OT.Sig_Secure ensures cryptographically secure electronic signatures. 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 by resisting tampering attacks.

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 OT.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and OE.SVD_Auth that ensures the authenticity and integrity of the SVD exported by the TOE to the CGA.

OE.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD.

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 paragraph 1(c) of Annex III **[DIR]**. OT.Lifecycle_Security (Lifecycle security) requires the TOE to detect flaws during the initialisation, personalisation 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. OE.DTBS_Protect counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE for SSCD parts 2, 3 and 4 only. For the others SSCD parts, OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. 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.

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 and OE.HID_VAD (Protection of the VAD) provides confidentiality and integrity of the VAD as needed by the authentication method employed for SSCD parts 2, 3 and 4 only. For the others SSCD parts, 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).

OT.Lifecycle_Management ensures that when the TOE is under the Personalisation Agent control, it can not be misused to sign on behalf of the legitimate Signatory.

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 can not be altered in transit between the SCA and the TOE for SSCD parts 2, 3 and 4 only. For the others SSCD parts, 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 Threats related to EAC2

T.Counterfeit/EAC2 The threat T.Counterfeit/EAC2 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.CA2 using a Chip Authentication key pair that is generated within the issuing PKI branch, as aimed by OE.Chip_Auth_Key. According to OE.Chip_Auth_Key, the terminal has to perform the Chip Authentication 2 protocol to verify the authenticity of the electronic document's chip.

T.Sensitive_Data The threat T.Sensitive_Data is countered by the TOE-Objective OT.Sens_Data_EAC2, that requires that read access to sensitive user data is only granted to EAC2 terminals with corresponding access rights. Furthermore, it is required that the confidentiality of the data is ensured during 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 EAC2 terminal.

T.Abuse-Func The threat 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.Prot_Abuse-Func ensures that the usage of functions having not to be used in the operational phase is effectively prevented.

T.Eavesdropping The threat T.Eavesdropping addresses listening to the communication between the TOE and a PACE terminal or an EAC2 terminal in order to gain access to transferred user data. This threat is countered by the security objective OT.Data_Confidentiality through a trusted channel based on PACE Authentication, and by OT.Sens_Data_EAC2 demanding a trusted channel that is based on Chip Authentication 2.

T.Forgery The threat 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 requires the TOE to limit the write access for the electronic document to the trustworthy Personalisation Agent (cf. OE.Personalisation). The TOE will protect the integrity and authenticity of the stored and exchanged User Data or/and TSF-data as aimed by the security objectives OT.Data_Integrity and OT.Data_Authenticity, respectively. The objectives OT.Prot_Phys-Tamper and OT.Prot_Abuse-Func contribute 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 Passive Authentication using the Document Security Object as aimed by OE.Passive_Auth_Sign will be able to effectively verify integrity and authenticity of the data received from the TOE. The threat is also addressed by the refinement of OT.AC_Pers, here renamed OT.AC_Pers_EAC2.

T.Information_Leakage The threats 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 objectives OT.Prot_Inf_Leak.

T.Malfunction The threats 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 objectives OT.Prot_Malfunction.

T.Phys-Tamper The threats 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 objectives OT.Prot_Phys-Tamper.

T.Skimming The threat T.Skimming addresses accessing the user data (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contactless/contact-based interface. This threat is countered by the security objectives OT.Data_Integrity, OT.Data_Authenticity and OT.Data_Confidentiality through the PACE authentication. The objective OE.Electronic_Document_Holder ensures that a PACE session can only be established either by the ID 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.Sens_Data_EAC2 that demands a trusted channel based on Chip Authentication 2, and requires that read access to sensitive user data is only granted to EAC2 terminals with corresponding access rights. Moreover, OE.Terminal_Authentication requires the electronic document issuer to provide the corresponding PKI.

T.Tracing The threat T.Tracing addresses gathering TOE tracing data identifying it remotely by establishing or listening to a communication via the contactless/contact 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.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.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 cannot be replayed as they rely on random data internally generated by the TOE.

7.3.2 Organisational Security Policies

7.3.2.1 OSPs 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 initialisation, personalisation 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 authorized 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 **[DIR]**. This is ensured as follows:

- o OE.SCD_Unique meets the paragraph 1(a) of the directive **[DIR]**, Annex III, by the requirements that the SCD used for signature creation can practically occur only once;
- o OT.SCD_Unique meets the paragraph 1(a) of Annex III **[DIR]**, 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 paragraph 1(a) of Annex III **[DIR]** 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 paragraph 1(b) of Annex III **[DIR]** by the requirements to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE;
- o OT.Sigy_SigF meets the requirement in paragraph 1(c) of Annex III **[DIR]** 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 **[DIR]** as the TOE must not alter the DTBS/R.

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

The usage of SCD under sole control of the signatory is ensured by

- o OT.Lifecycle_Security requiring the TOE to detect flaws during the initialisation, personalisation 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.SCD/SVD_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only, and
- 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.

OE.Dev_Prov_Service ensures that the legitimate user obtains a TOE sample as an authentic, initialised and personalised 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.

OE.SSCD_Prov_Service ensures that the signatory obtains a TOE sample as an authentic, initialised and personalised SSCD from an SSCD provisioning service for SSCD parts 2, 3, 5 and 6 only.

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.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.SSCD_Prov_Service ensures that the signatory uses an authentic TOE, initialised and personalised for the signatory for SSCD parts 2,3, 5 and 6 only.

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 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.

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), OE.DTBS_Protect for SSCD parts 2, 3, 5 and 6 only, it ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE, for the others SSCD parts, 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. OT.Lifecycle_Management ensures that when the TOE is under the Personalisation Agent control, it cannot be misused to sign on behalf of the legitimate Signatory.

7.3.2.2 OSP related to EAC2

P.EAC2_Terminal The OSP P.EAC2_Terminal addresses the requirement for EAC2 terminals to implement the terminal parts of the protocols needed to executed EAC2 according to its specification in [TR-03110-2], and to store (static keys) or generate (temporary keys and nonces) the needed related credentials. This is enforced by OE.Chip_Auth_Key which requires Chip Authentication key 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 Passive Authentication protocol.

P.Terminal_PKI The OSP P.Terminal_PKI is enforced by establishing the receiving PKI branch as aimed by the objective OE.Terminal_Authentication.

P.Card_PKI The OSP P.Card_PKI is enforced by establishing the issuing PKI branch as aimed by the objectives OE.Passive_Auth_Sign (for the Document Security Object).

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.

P.Pre-Operational The OSP 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 and OE.Personalisation 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'. In addition, the threat is also addressed by the refinement of OT.AC_Pers named OT.AC_Pers_EAC2.

P.Terminal The OSP 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 The OSP P.Trustworthy_PKI is enforced by OE.Passive_Auth_Sign (for CSCA, issuing PKI branch).

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

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 authorized users is addressed by OE.SCD/SVD_Auth_Gen (Authorized 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
T.SCD_Divulg	OT.SCD_Secrecy , OT.SCD_Auth_Imp , OE.SCD/SVD_Auth_Gen , OE.SCD_Secrecy	Section 7.3.1
T.SCD_Derive	OT.SCD/SVD_Gen , OT.Sig_Secure , OE.SCD_Unique	Section 7.3.1
T.Hack_Phys	OT.SCD_Secrecy , OT.EMSEC_Design , OT.Tamper_ID , OT.Tamper_Resistance	Section 7.3.1
T.SVD_Forgery	OT.SCD_SVD_Corresp , OE.SVD_Auth , OE.SCD_SVD_Corresp ,	Section 7.3.1

Threats	Security Objectives	Rationale
	<u>OT.TOE TC SVD Exp</u> , <u>OE.CGA TC SVD Imp</u>	
<u>T.SigF Misuse</u>	<u>OT.Lifecycle Security</u> , <u>OT.Sigy SigF</u> , <u>OT.DTBS Integrity TOE</u> , <u>OE.Signatory</u> , <u>OE.DTBS Intend</u> , <u>OT.TOE TC VAD Imp</u> , <u>OT.TOE TC DTBS Imp</u> , <u>OE.HID TC VAD Exp</u> , <u>OE.SCA TC DTBS Exp</u> , <u>OT.Lifecycle Management</u> , <u>OE.HID VAD</u> , <u>OE.DTBS Protect</u>	<u>Section 7.3.1</u>
<u>T.DTBS Forgery</u>	<u>OT.DTBS Integrity TOE</u> , <u>OE.DTBS Intend</u> , <u>OT.TOE TC DTBS Imp</u> , <u>OE.SCA TC DTBS Exp</u> , <u>OE.DTBS Protect</u>	<u>Section 7.3.1</u>
<u>T.Sig Forgery</u>	<u>OT.SCD Unique</u> , <u>OT.Sig Secure</u> , <u>OE.CGA QCert</u> , <u>OE.SCD Unique</u>	<u>Section 7.3.1</u>
<u>T.Counterfeit/EAC2</u>	<u>OT.CA2</u> , <u>OE.Chip Auth Key</u>	<u>Section 7.3.1</u>
<u>T.Sensitive Data</u>	<u>OT.Sens Data EAC2</u> , <u>OE.Terminal Authentication</u>	<u>Section 7.3.1</u>
<u>T.Abuse-Func</u>	<u>OT.Prot Abuse-Func</u>	<u>Section 7.3.1</u>
<u>T.Eavesdropping</u>	<u>OT.Data Confidentiality</u> , <u>OT.Sens Data EAC2</u>	<u>Section 7.3.1</u>
<u>T.Forgery</u>	<u>OT.AC Pers EAC2</u> , <u>OT.Data Authenticity</u> , <u>OT.Data Integrity</u> , <u>OT.Prot Abuse-Func</u> , <u>OT.Prot Phys-Tamper</u> , <u>OE.Personalisation</u> , <u>OE.Passive Auth Sign</u> , <u>OE.Terminal</u>	<u>Section 7.3.1</u>
<u>T.Information Leakage</u>	<u>OT.Prot Inf Leak</u>	<u>Section 7.3.1</u>
<u>T.Malfunction</u>	<u>OT.Prot Malfunction</u>	<u>Section 7.3.1</u>
<u>T.Phys-Tamper</u>	<u>OT.Prot Phys-Tamper</u>	<u>Section 7.3.1</u>
<u>T.Skimming</u>	<u>OT.Data Integrity</u> , <u>OT.Data Authenticity</u> , <u>OT.Data Confidentiality</u> , <u>OT.Sens Data EAC2</u> , <u>OE.Terminal Authentication</u> , <u>OE.Electronic Document Holder</u>	<u>Section 7.3.1</u>
<u>T.Tracing</u>	<u>OT.Tracing</u> , <u>OE.Electronic Document Holder</u>	<u>Section 7.3.1</u>
<u>T.Key Derive</u>	<u>OE.AuthKey Unique</u> , <u>OT.TOE AuthKey Unique</u> , <u>OT.Authentication Secure</u>	<u>Section 7.3.1</u>

Threats	Security Objectives	Rationale
T.Authentication Repl ay	OT.Authentication Secure	Section 7.3.1

Table 16 Threats and Security Objectives - Coverage

Security Objectives	Threats	Rationale
OT.Tamper Resistance	T.Hack Phys	
OT.Tamper ID	T.Hack Phys	
OT.EMSEC Design	T.Hack Phys	
OT.DTBS Integrity TOE	T.SigF Misuse, T.DTBS Forgery	
OT.SigF SigF	T.SigF Misuse	
OT.Sig Secure	T.SCD Derive, T.Sig Forgery	
OT.SCD Secrecy	T.SCD Divulg, T.Hack Phys	
OT.Lifecycle Security	T.SigF Misuse	
OT.SCD SVD Corresp	T.SVD Forgery	
OT.SCD Unique	T.Sig Forgery	
OT.SCD/SVD Gen	T.SCD Derive	
OT.SCD Auth Imp	T.SCD Divulg	
OT.TOE SSCD Auth		
OT.TOE TC SVD Exp	T.SVD Forgery	
OT.TOE TC VAD Imp	T.SigF Misuse	
OT.TOE TC DTBS Imp	T.SigF Misuse, T.DTBS Forgery	
OT.AC Pers EAC2	T.Forgery	
OT.CA2	T.Counterfeit/EAC2	
OT.Sens Data EAC2	T.Sensitive Data, T.Eavesdropping, T.Skimming	
OT.Data Authenticity	T.Forgery, T.Skimming	
OT.Data Confidentiality	T.Eavesdropping, T.Skimming	
OT.Data Integrity	T.Forgery, T.Skimming	
OT.Identification		
OT.Prot Abuse-Func	T.Abuse-Func, T.Forgery	
OT.Prot Inf Leak	T.Information Leakage	
OT.Prot Malfunction	T.Malfunction	
OT.Prot Phys-Tamper	T.Forgery, T.Phys-Tamper	
OT.Tracing	T.Tracing	

Security Objectives	Threats	Rationale
OT.Authentication Secure	T.Key Derive , T.Authentication Replay	
OT.Lifecycle Management	T.SigF Misuse	
OT.eServices		
OT.TOE AuthKey Unique	T.Key Derive	
OE.Signatory	T.SigF Misuse	
OE.DTBS Intend	T.SigF Misuse , T.DTBS Forgery	
OE.SVD Auth	T.SVD Forgery	
OE.CGA QCert	T.Sig Forgery	
OE.SCD SVD Corresp	T.SVD Forgery	
OE.SCD Unique	T.SCD Derive , T.Sig Forgery	
OE.SCD Secrecy	T.SCD Divulg	
OE.SCD/SVD Auth Gen	T.SCD Divulg	
OE.Dev Prov Service		
OE.CGA TC SVD Imp	T.SVD Forgery	
OE.CGA SSCD Auth		
OE.HID TC VAD Exp	T.SigF Misuse	
OE.HID VAD	T.SigF Misuse	
OE.SCA TC DTBS Exp	T.SigF Misuse , T.DTBS Forgery	
OE.Chip Auth Key	T.Counterfeit/EAC2	
OE.Terminal Authentication	T.Sensitive Data , T.Skimming	
OE.Legislative Compliance		
OE.Passive Auth Sign	T.Forgery	
OE.Personalisation	T.Forgery	
OE.Terminal	T.Forgery	
OE.Electronic Document Holder	T.Skimming , T.Tracing	
OE.AuthKey Unique	T.Key Derive	

Table 17 Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives	Rationale
P.CSP_QCert	OT.Lifecycle Security , OT.SCD SVD Corresp , OE.CGA QCert , OT.SCD Auth Imp , OE.SCD/SVD Auth Gen ,	Section 7.3.2

Organisational Security Policies	Security Objectives	Rationale
	OE.SCD_SVD_Corresp , OT.TOE_SSCD_Auth , OE.CGA_SSCD_Auth	
P.QSign	OT.Sig_Secure , OT.Sigy_SigF , OE.CGA_QCert , OE.DTBS_Intend	Section 7.3.2
P.Sigy_SSCD	OT.Lifecycle_Security , OT.SCD/SVD_Gen , OT.SCD_Unique , OT.SCD_Secrecy , OT.Sig_Secure , OT.Sigy_SigF , OT.DTBS_Integrity_TOE , OT.EMSEC_Design , OT.Tamper_Resistance , OT.SCD_Auth_Imp , OE.SCD/SVD_Auth_Gen , OE.SCD_Secrecy , OE.SCD_Unique , OT.TOE_SSCD_Auth , OT.TOE_TC_SVD_Exp , OE.Dev_Prov_Service , OE.CGA_TC_SVD_Imp , OE.CGA_SSCD_Auth , OE.SSCD_Prov_Service	Section 7.3.2
P.Sig_Non-Repud	OT.Lifecycle_Security , OT.SCD_Unique , OT.SCD_SVD_Corresp , OT.SCD_Secrecy , OT.Sig_Secure , OT.Sigy_SigF , OT.DTBS_Integrity_TOE , OT.EMSEC_Design , OT.Tamper_ID , OT.Tamper_Resistance , OE.CGA_QCert , OE.SVD_Auth , OE.DTBS_Intend , OE.Signatory , OE.SCD/SVD_Auth_Gen , OE.SCD_Secrecy , OE.SCD_Unique , OE.SCD_SVD_Corresp , OT.TOE_SSCD_Auth , OT.TOE_TC_SVD_Exp , OE.Dev_Prov_Service , OE.CGA_TC_SVD_Imp , OE.CGA_SSCD_Auth , OT.TOE_TC_VAD_Imp , OT.TOE_TC_DTBS_Imp , OE.HID_TC_VAD_Exp , OE.SCA_TC_DTBS_Exp , OT.Lifecycle_Management , OE.DTBS_Protect , OE.SSCD_Prov_Service	Section 7.3.2
P.EAC2_Terminal	OE.Terminal , OE.Chip_Auth_Key , OE.Terminal_Authentication	Section 7.3.2
P.Terminal_PKI	OE.Terminal_Authentication	Section 7.3.2
P.Card_PKI	OE.Passive_Auth_Sign	Section 7.3.2
P.Manufact	OT.Identification	Section 7.3.2
P.Pre-Operational	OT.Identification , OT.AC_Pers_EAC2 , OE.Personalisation , OE.Legislative_Compliance	Section 7.3.2
P.Terminal	OE.Terminal	Section 7.3.2
P.Trustworthy_PKI	OE.Passive_Auth_Sign	Section 7.3.2
P.eServices	OT.eServices	Section 7.3.2

Table 18 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies	Rationale
OT.Tamper Resistance	P.Sigy SSCD , P.Sig Non-Repud	
OT.Tamper ID	P.Sig Non-Repud	
OT.EMSEC Design	P.Sigy SSCD , P.Sig Non-Repud	
OT.DTBS Integrity TOE	P.Sigy SSCD , P.Sig Non-Repud	
OT.Sigy SigF	P.QSign , P.Sigy SSCD , P.Sig Non-Repud	
OT.Sig Secure	P.QSign , P.Sigy SSCD , P.Sig Non-Repud	
OT.SCD Secrecy	P.Sigy SSCD , P.Sig Non-Repud	
OT.Lifecycle Security	P.CSP QCert , P.Sigy SSCD , P.Sig Non-Repud	
OT.SCD SVD Corresp	P.CSP QCert , P.Sig Non-Repud	
OT.SCD Unique	P.Sigy SSCD , P.Sig Non-Repud	
OT.SCD/SVD Gen	P.Sigy SSCD	
OT.SCD Auth Imp	P.CSP QCert , P.Sigy SSCD	
OT.TOE SSCD Auth	P.CSP QCert , P.Sigy SSCD , P.Sig Non-Repud	
OT.TOE TC SVD Exp	P.Sigy SSCD , P.Sig Non-Repud	
OT.TOE TC VAD Imp	P.Sig Non-Repud	
OT.TOE TC DTBS Imp	P.Sig Non-Repud	
OT.AC Pers EAC2	P.Pre-Operational	
OT.CA2		
OT.Sens Data EAC2		
OT.Data Authenticity		
OT.Data Confidentiality		
OT.Data Integrity		
OT.Identification	P.Manufact , P.Pre-Operational	
OT.Prot Abuse-Func		
OT.Prot Inf Leak		
OT.Prot Malfunction		
OT.Prot Phys-Tamper		
OT.Tracing		
OT.Authentication Secure		
OT.Lifecycle Management	P.Sig Non-Repud	
OT.eServices	P.eServices	

Security Objectives	Organisational Security Policies	Rationale
OT.TOE AuthKey Unique		
OE.Signatory	P.Sig Non-Repud	
OE.DTBS Intend	P.QSign, P.Sig Non-Repud	
OE.SVD Auth	P.Sig Non-Repud	
OE.CGA QCert	P.CSP QCert, P.QSign, P.Sig Non-Repud	
OE.SCD SVD Corresp	P.CSP QCert, P.Sig Non-Repud	
OE.SCD Unique	P.Sigy SSCD, P.Sig Non-Repud	
OE.SCD Secrecy	P.Sigy SSCD, P.Sig Non-Repud	
OE.SCD/SVD Auth Gen	P.CSP QCert, P.Sigy SSCD, P.Sig Non-Repud	
OE.Dev Prov Service	P.Sigy SSCD, P.Sig Non-Repud	
OE.CGA TC SVD Imp	P.Sigy SSCD, P.Sig Non-Repud	
OE.CGA SSCD Auth	P.CSP QCert, P.Sigy SSCD, P.Sig Non-Repud	
OE.HID TC VAD Exp	P.Sig Non-Repud	
OE.SCA TC DTBS Exp	P.Sig Non-Repud	
OE.Chip Auth Key	P.EAC2 Terminal	
OE.Terminal Authentication	P.EAC2 Terminal, P.Terminal PKI	
OE.Legislative Compliance	P.Pre-Operational	
OE.Passive Auth Sign	P.Card PKI, P.Trustworthy PKI	
OE.Personalisation	P.Pre-Operational	
OE.Terminal	P.EAC2 Terminal, P.Terminal	
OE.Electronic Document Holder		
OE.AuthKey Unique		

Table 19 Security Objectives and OSPs - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.CGA	OE.CGA QCert, OE.SVD Auth	Section 7.3.3
A.SCA	OE.DTBS Intend	Section 7.3.3
A.CSP	OE.SCD/SVD Auth Gen, OE.SCD Secrecy, OE.SCD Unique, OE.SCD SVD Corresp	Section 7.3.3

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

Security Objectives for the Operational Environment	Assumptions	Rationale
<u>OE.Signatory</u>		
<u>OE.DTBS Intend</u>	<u>A.SCA</u>	
<u>OE.SVD Auth</u>	<u>A.CGA</u>	
<u>OE.CGA QCert</u>	<u>A.CGA</u>	
<u>OE.SCD SVD Corresp</u>	<u>A.CSP</u>	
<u>OE.SCD Unique</u>	<u>A.CSP</u>	
<u>OE.SCD Secrecy</u>	<u>A.CSP</u>	
<u>OE.SCD/SVD Auth Gen</u>	<u>A.CSP</u>	
<u>OE.Dev Prov Service</u>		
<u>OE.CGA TC SVD Imp</u>		
<u>OE.CGA SSCD Auth</u>		
<u>OE.HID TC VAD Exp</u>		
<u>OE.SCA TC DTBS Exp</u>		
<u>OE.Chip Auth Key</u>		
<u>OE.Terminal Authentication</u>		
<u>OE.Legislative Compliance</u>		
<u>OE.Passive Auth Sign</u>		
<u>OE.Personalisation</u>		
<u>OE.Terminal</u>		
<u>OE.Electronic Document Holder</u>		
<u>OE.AuthKey Unique</u>		

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

8 Security Requirements

8.1 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.

8.1.1 All SSCD parts

8.1.1.1 Protection of the TSF (FPT)

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1: The TSF shall ensure that the TOE does not emit emissions over its attack surface in such amount that these emissions enable access to TSF data and user data as specified in Table below.

ID	Emissions	Attack surface	TSF data	User data
1	side channel	Contact and contactless interfaces	- Session keys - Ephemeral private key ephem - Chip Authentication private keys (SKPICC) - SCD - RAD	Not useful information

Application Note:

This SFR covers the definition in SSCD PPs and extends them by session keys, keys and PIN/PUK as part of the EAC V2 protocol aspects. This extension does not conflict with the strict conformance to SSCD PPs.

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

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

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:

- **(1) self-test according to FPT_TST fails**
- **(2) power shortage**
- **(3) over and under voltage**
- **(4) over and under clock frequency**
- **(5) over and under temperature**
- **(6) integrity problems**
- **(7) unexpected abortion of the execution of the TSF due to external events**
- **No other failure.**

FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that can 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 the following self-tests **during initial start-up and periodically during normal operation** to demonstrate the correct operation of the TSF:

- **integrity of TSF data,**
- **integrity of TSF code.**

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**.

8.1.1.2 Security management (FMT)**FMT_SMR.1 Security roles**

FMT_SMR.1.1 The TSF shall maintain the roles

- **R.Admin**
- **R.Sigy**
- **R.TOE Administrator.**

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:

- o **Creation and modification of RAD,**
- o **Enabling the signature creation function,**
- o **Modification of the security attribute SCD/SVD management, SCD operational,**
- o **Change the default value of the security attribute SCD Identifier,**
- o **Initialization,**
- o **Pre-Personalisation,**
- o **Personalisation,**
- o **Configuration,**
- o **Resume and unblock the PIN and PUK (if any),.**

Application Note:

There is no default value for SCD Identifier.

This SFR covers the definition in SSCD PPs and extends them by EAC V2 protocol aspects.

This extension does not conflict with the strict conformance to SSCD PPs.

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 **SCD/SVD Management** and **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 **R.Admin** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.4 Security attribute value inheritance

FMT_MSA.4.1 The TSF shall use the following rules to set the value of security attributes:

- (1) If **S.Admin** successfully generates an **SCD/SVD** pair without **S.Sigy** being authenticated the security attribute "SCD operational of the SCD" shall be set to "no" as a single operation
- (2) If **S.Sigy** successfully generates an **SCD/SVD** pair the security attribute "SCD operational of the SCD" shall be set to "yes" as a single operation
- (3) 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.
- (4) 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

FMT_MTD.1/Admin Management of TSF data

FMT_MTD.1.1/Admin The TSF shall restrict the ability to **create** the **RAD** to **R.Admin**.

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**.

8.1.1.3 Identification and authentication (FIA)

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

- **Self-test according to FPT_TST.1,**
- **Establishing a trusted channel between a trusted IT product generating the SCD/SVD pair for import of the SCD as described by FDP_UCT.1/SCD and FDP_ITC.1/SCD and the TOE by means of TSF required by FTP_ITC.1/SCD (not applicable for SSCD KG).**
- **Establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD to export the SVD to the CGA ([PP-SSCD4]).**

- Establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD to send the VAD ([PP-SSCD5], [PP-SSCD6]).
- Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS to send the DTBS ([PP-SSCD5], [PP-SSCD6])

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 Authentication failure handling

FIA_AFL.1.1 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 When the defined number of unsuccessful authentication attempts has been met, the TSF shall

- **Block RAD.**

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

- **Self-test according to FPT_TST.1,**
- **Identification of the user by means of TSF required by FIA_UID.1**
- **Establishing a trusted channel between a trusted IT product generating the SCD/SVD pair for import the SCD as described by FDP_UCT.1/SCD and FDP_ITC.1/SCD and the TOE by means of TSF required by FTP_ITC.1/SCD (not applicable for SSCD KG).**
- **Establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD to export the SVD to the CGA ([PP-SSCD4]).**
- **Establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD to send the VAD ([PP-SSCD5], [PP-SSCD6]).**
- **Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS to send the DTBS ([PP-SSCD5], [PP-SSCD6])**

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

8.1.1.4 User data protection (FDP)

The security attributes and 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	authorised, not authorised
SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value

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.**

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.**

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:

- o **Session keys (immediately after closing related communication session),**
- o **the ephemeral private key ephem - SKPICC- PACE (by having generated a DH shared secret K),**
 - o **secret electronic document holder authentication data, e.g. PIN and/or PUK (when their temporarily stored values are not used any more),**
 - o **SCD¹**

¹ [assignment : list of objects]

- SVD (if persistently stored by the TOE)
- DTBS/R.

Application note :

- The following data persistently stored by the TOE shall have the user data attribute "integrity checked persistent stored data": SCD, SVD (if persistently stored by the TOE)
- The following data temporarily stored by the TOE shall have the user data attribute "integrity checked stored data": DTBS/R.

Notes : Should we only consider SCD because SVD and DTBS is out of the scope of the PP

FDP_ACC.1/Signature_Creation Subset access control

FDP_ACC.1.1/Signature_Creation The TSF shall enforce the **Signature Creation SFP** on **Sending of DTBS/R by SCA and Signing of DTBS/R by Signatory**:

- subjects: S.User,
- objects: DTBS/R, SCD,
- 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:

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

8.1.1.5 Cryptographic support (FCS)

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[Cryptographic Operation]** in accordance with a specified cryptographic algorithm **[Cryptographic Algorithm]** and cryptographic key sizes **[Cryptographic Key Sizes]** that meet the following: **[Standards]**

Cryptographic Operation	Cryptographic Algorithms	Cryptographic Key Sizes	In TOE certified scope²?	Standards
Digital signature Satisfied dependencies: FCS_CKM.1 (SCD/SVD pair using RSA)	RSA PKCS#1v1.5with SHA-1	1024 bits	No	[RSA-PKCS#1]
		1536 bits		
		2048 bits		
		3072 bits		
		4096 bits		
	RSA PKCS#1v1.5 with SHA2-224	1024 bits		
		1536 bits		
		2048 bits		
		3072 bits		
		4096 bits		
	RSA PKCS#1v1.5 with SHA2-256	1024 bits		
		1536 bits		
		2048 bits		
		3072 bits		
		4096 bits		
	RSA PKCS#1v1.5 with SHA2-384	1024 bits		
		1536 bits		
		2048 bits		
		3072 bits		
		4096 bits		
	RSA PKCS#1v1.5 with SHA2-512	1024 bits		
		1536 bits		
		2048 bits		
		3072 bits		
		4096 bits		
RSA-PSS PKCS#1 v2.1 with SHA-1	1024 bits	No		
	1536 bits			
	2048 bits			
	3072 bits			
	4096 bits			

² 'No' means this part is considered as legacy in [ECCG-CM] but shall be mentioned as still used in the field

Cryptographic Operation	Cryptographic Algorithms	Cryptographic Key Sizes	In TOE certified scope²?	Standards
	RSA-PSS PKCS#1 v2.1 with SHA2-224	1024 bits		
		1536 bits		
		2048 bits		
		3072 bits		
		4096 bits		
	RSA-PSS PKCS#1 v2.1 with SHA2-256	1024 bits	No	
		1536 bits	Yes	
		2048 bits		
		3072 bits		
		4096 bits		
	RSA-PSS PKCS#1 v2.1 with SHA2-384	1024 bits	No	
		1536 bits	Yes	
		2048 bits		
		3072 bits		
		4096 bits		
	RSA-PSS PKCS#1 v2.1 with SHA2-512	1024 bits	No	
		1536 bits	Yes	
		2048 bits		
		3072 bits		
		4096 bits		
	RSA-PSS PKCS#1 v2.1 with SHA3-224	1024 bits	No	
		1536 bits		
		2048 bits		
		3072 bits		
		4096 bits		
RSA-PSS PKCS#1 v2.1 with SHA3-256	1024 bits	No		
	1536 bits	Yes		
	2048 bits			
	3072 bits			
	4096 bits			
	1024 bits	No		
	1536 bits			

Cryptographic Operation	Cryptographic Algorithms	Cryptographic Key Sizes	In TOE certified scope²?	Standards
	RSA-PSS PKCS#1 v2.1 with SHA3-384	2048 bits	Yes	
		3072 bits		
		4096 bits		
	RSA-PSS PKCS#1 v2.1 with SHA3-512	1024 bits	No	
		1536 bits		
		2048 bits	Yes	
		3072 bits		
		4096 bits		
Digital signature Satisfied dependencies: FCS_CKM.1 (SCD/SVD pair using ECDSA)	ECDSA with SHA-1	192 bits	No	[ECDSA]
		224 bits		
		256 bits		
		320 bits		
		384 bits		
		512 bits		
		521 bits		
	ECDSA with SHA2-224	192 bits	No	
		224 bits		
		256 bits		
		320 bits		
		384 bits		
		512 bits		
		521 bits		
	ECDSA with SHA2-256	192 bits	See Table 22	
		224 bits		
		256 bits		
		320 bits		
		384 bits		
		512 bits		
		521 bits		
	ECDSA with SHA2-384	192 bits		
		224 bits		
		256 bits		

Cryptographic Operation	Cryptographic Algorithms	Cryptographic Key Sizes	In TOE certified scope²?	Standards
		320 bits		
		384 bits		
		512 bits		
		521 bits		
	ECDSA with SHA2-512	192 bits		
		224 bits		
		256 bits		
		320 bits		
		384 bits		
		512 bits		
		521 bits		
	ECDSA with SHA3-224	192 bits	No	
		224 bits		
		256 bits		
		320 bits		
		384 bits		
		512 bits		
		521 bits		
	ECDSA with SHA3-256	192 bits	See Table 22	
		224 bits		
		256 bits		
		320 bits		
		384 bits		
		512 bits		
		521 bits		
	ECDSA with SHA3-384	192 bits		
		224 bits		
		256 bits		
		320 bits		
		384 bits		
		512 bits		
		521 bits		

Cryptographic Operation	Cryptographic Algorithms	Cryptographic Key Sizes	In TOE certified scope²?	Standards	
	ECDSA with SHA3-512	192 bits			
		224 bits			
		256 bits			
		320 bits			
		384 bits			
		512 bits			
		521 bits			
Key agreement Satisfied dependencies: FCS_CKM.1 (Ephemeral key pair based on DH)	Anonymous DH	1024 bits	No	[TR-03111]	
		1536 bits			
		2048 bits			
PACE Authentication Satisfied dependencies: FCS_CKM.1/DH_PACE	PACE IM and GM with ECDH	192 bits	See Table 22	[ICAO-9303]	
		224 bits			
		256 bits			
		320 bits			
		384 bits			
		512 bits			
		521 bits			
	PACE IM and GM with DH	1024 bits	No		
		1536 bits			
		2048 bits			
		PACE IM and GM with 3DES	128 bits		No
	PACE IM and GM with AES	128 bits	Yes		
192 bits					
256 bits					
Secure messaging Encryption/decryption Satisfied dependencies: FCS_CKM.1 (Symmetric keys using 3DES in CBC mode)	3DES in CBC mode³	128 bits	No	[IAS-ECC]	

³ Not in scope of this certification as mentioned as legacy in **[ECCG-CM]**

Cryptographic Operation	Cryptographic Algorithms	Cryptographic Key Sizes	In TOE certified scope ² ?	Standards
Secure messaging Encryption/decryption Satisfied dependencies: FCS_CKM.1 (Symmetric keys using AES in CBC mode)	AES in CBC mode	128 bits	Yes	
		192 bits		
		256 bits		
Secure messaging - MAC generation and verification Satisfied dependencies: FCS_CKM.1 (Symmetric keys using 3DES in CBC mode)	ISO/IEC 9797-1 algorithm 3 padding 2 (3DES)³	128 bits	No	[ISO9797-1]
Secure messaging - MAC generation and verification Satisfied dependencies: FCS_CKM.1 (Symmetric keys using AES in CBC mode)	CMAC (AES)	128 bits	Yes	[ISO9797-1] [NIST-800-38B]
		192 bits		
		256 bits		
Ciphering key decryption Satisfied dependencies: FCS_CKM.1 (Asymmetric key pair using RSA)	RSA-OAEP SHA-1	1024 bits	No	[RSA-PKCS#1]
		1536 bits		
		2048 bits		
		3072 bits		
		4096 bits		
	RSA-OAEP SHA2-256	1024 bits	No	
		1536 bits		
		2048 bits	Yes	
		3072 bits		
		4096 bits		
	RSA PKCS#1v1.5³	1024 bits	No	
		1536 bits		
		2048 bits		
		3072 bits		
		4096 bits		
Ciphering key decryption	ECDH	192 bits	See Table 22	[IAS-ECC]
		224 bits		

Cryptographic Operation	Cryptographic Algorithms	Cryptographic Key Sizes	In TOE certified scope ² ?	Standards
Satisfied dependencies: FCS_CKM.1 (Cryptographic key pair based on ECDH)		256 bits		
		320 bits		
		384 bits		
		512 bits		
		521 bits		
Symmetric encryption/decryption Satisfied dependencies: FCS_CKM.1 (Symmetric keys using AES in CBC mode)	AES-CBC mode	128 bits	Yes	[IAS-ECC], [ISO18033-1]
		192 bits		
		256 bits		
GP secret data encryption Satisfied dependencies: FCS_CKM.1 (GP cryptographic keys using 3DES in CBC mode)	SCP02	128 bits	No	[GP1]
GP secret data encryption Satisfied dependencies: FCS_CKM.1 (GP cryptographic keys using AES in CBC mode)	SCP03 using AES	128 bits	Yes	[GP2]
		192 bits		
		256 bits		
Client/Server Authentication Satisfied dependencies: FCS_CKM.1 (Asymmetric key pair using RSA)	RSA PKCS#1v1.5³	1024 bits	No	[RSA-PKCS#1]
		1536 bits		
		2048 bits		
		3072 bits		
		4096 bits		
	RSA-PSS PKCS#1 v2.1 with SHA-1	1024 bits	No	
		1536 bits		
		2048 bits		
		3072 bits		
		4096 bits		
	1024 bits			
	1536 bits			

Cryptographic Operation	Cryptographic Algorithms	Cryptographic Key Sizes	In TOE certified scope²?	Standards
	RSA-PSS PKCS#1 v2.1 with SHA2-224	2048 bits		
		3072 bits		
		4096 bits		
	RSA-PSS PKCS#1 v2.1 with SHA2-256	1024 bits	No	
		1536 bits		
		2048 bits	Yes	
		3072 bits		
		4096 bits		
	RSA-PSS PKCS#1 v2.1 with SHA2-384	1024 bits	No	
		1536 bits		
		2048 bits	Yes	
		3072 bits		
		4096 bits		
	RSA-PSS PKCS#1 v2.1 with SHA2-512	1024 bits	No	
		1536 bits		
		2048 bits	Yes	
		3072 bits		
		4096 bits		
	RSA-PSS PKCS#1 v2.1 with SHA3-224	1024 bits	No	
		1536 bits		
		2048 bits		
		3072 bits		
		4096 bits		
	RSA-PSS PKCS#1 v2.1 with SHA3-256	1024 bits	No	
		1536 bits		
		2048 bits	Yes	
		3072 bits		
		4096 bits		
	RSA-PSS PKCS#1 v2.1 with SHA3-384	1024 bits	No	
		1536 bits		
		2048 bits	Yes	
		3072 bits		
		4096 bits		

Cryptographic Operation	Cryptographic Algorithms	Cryptographic Key Sizes	In TOE certified scope²?	Standards
	RSA-PSS PKCS#1 v2.1 with SHA3-512	1024 bits	No	
		1536 bits		
		2048 bits	Yes	
		3072 bits		
		4096 bits		
	ECC	192 bits	See Table 22	[IAS-ECC]
		224 bits		
		256 bits		
		320 bits		
		384 bits		
		512 bits		
		521 bits		
Symmetric role Authentication	TDES encryption in CBC mode, Signature using Retail MAC	128 bits³	No	[IAS-ECC]
	AES encryption in CBC mode, Signature using CMAC	128 bits	Yes	
		192 bits		
		256 bits		
	Minidriver: 3DES CBC	128 bits	No	[Minidriver]
192 bits				
Asymmetric Role Authentication	RSA with ISO/IEC 9796-2 with SHA-1	1024 bits	No	[IAS-ECC]
		1536 bits		
		2048 bits		
	RSA with ISO/IEC 9796-2 with SHA2-224	1024 bits		
		1536 bits		
		2048 bits		
	RSA with ISO/IEC 9796-2 with SHA2-256	1024 bits	No	
		1536 bits	Yes	
		2048 bits		
	RSA with ISO/IEC 9796-2 with SHA2-384	1024 bits	No	
		1536 bits	Yes	
		2048 bits		
	1024 bits	No		

Cryptographic Operation	Cryptographic Algorithms	Cryptographic Key Sizes	In TOE certified scope ² ?	Standards
	RSA with ISO/IEC 9796-2 with SHA2-512	1536 bits	Yes	
		2048 bits		
Symmetric Device Authentication Satisfied dependencies: FCS_CKM.1 (Symmetric keys using 3DES in CBC mode)	TDES encryption in CBC mode, Signature using Retail MAC with SHA-1	128 bits ⁵	No	[IAS-ECC] [CEN-14890]
	TDES encryption in CBC mode, Signature using Retail MAC with SHA2-256	128 bits ⁵		
	TDES encryption in CBC mode, Signature using Retail MAC with SHA3-256	128 bits ⁵		
Certificate verification for IAS PKI Satisfied dependencies: FCS_CKM.1 (Asymmetric key pair using RSA)	RSA with ISO/IEC 9796-2 padding with partial recovery and with SHA-1	1024 bits	No	[IAS-ECC]
		1536 bits		
		2048 bits		
	RSA with ISO/IEC 9796-2 padding with partial recovery and with SHA2-256	1024 bits	No	
		1536 bits		
		2048 bits	Yes	
Certificate verification for EAC PKI Satisfied dependencies: FCS_CKM.1 (Asymmetric key pair using ECDSA)	ECDSA with SHA-1	192 bits	No	[ICAO-9303]
		224 bits		
		256 bits		
		320 bits		
		384 bits		
		512 bits		
	ECDSA with SHA2-224	521 bits		
		192 bits		
		224 bits		
		256 bits		
		320 bits		
		384 bits		

Cryptographic Operation	Cryptographic Algorithms	Cryptographic Key Sizes	In TOE certified scope²?	Standards	
		512 bits			
		521 bits			
	ECDSA with SHA2-256	192 bits	See Table 22		
		224 bits			
		256 bits			
		320 bits			
		384 bits			
		512 bits			
		521 bits			
		ECDSA with SHA2-384			192 bits
	224 bits				
	256 bits				
	320 bits				
	384 bits				
	512 bits				
	521 bits				
	ECDSA with SHA2-512				192 bits
		224 bits			
		256 bits			
		320 bits			
		384 bits			
		512 bits			
		521 bits			
Asymmetric Internal Device Authentication Satisfied dependencies: FCS_CKM.1 (Asymmetric key pair using RSA)		RSA with ISO/IEC 9796-2 padding with partial recovery and with SHA-1		1024 bits	No
	1536 bits				
	2048 bits				
	RSA with ISO/IEC 9796-2 padding with partial recovery and with SHA2-256	1024 bits	No		
		1536 bits			
		2048 bits	Yes		
	RSA with ISO/IEC 9796-2 padding	1024 bits	No	[IAS-ECC]	
		1536 bits			

Cryptographic Operation	Cryptographic Algorithms	Cryptographic Key Sizes	In TOE certified scope??	Standards
Asymmetric External Device Authentication Satisfied dependencies: FCS_CKM.1 (Asymmetric key pair using RSA)	with partial recovery and with SHA-1	2048 bits		
	RSA with ISO/IEC 9796-2 padding with partial recovery and with SHA2-256	1024 bits	No	
		1536 bits		
		2048 bits	Yes	
EACv2 Terminal Authentication Satisfied dependencies: FCS_CKM.1 (Asymmetric key pair using ECDSA)	ECDSA with SHA-1	192 bits	No	[TR-03110]
		224 bits		
		256 bits		
		320 bits		
		384 bits		
		512 bits		
		521 bits		
	ECDSA with SHA2-224	192 bits		
		224 bits		
		256 bits		
		320 bits		
		384 bits		
		512 bits		
		521 bits		
	ECDSA with SHA2-256	192 bits	See Table 22	
		224 bits		
		256 bits		
		320 bits		
		384 bits		
		512 bits		
		521 bits		
	ECDSA with SHA2-384	192 bits		
		224 bits		
		256 bits		
		320 bits		
		384 bits		

Cryptographic Operation	Cryptographic Algorithms	Cryptographic Key Sizes	In TOE certified scope²?	Standards
		512 bits		
		521 bits		
	ECDSA with SHA2-512	192 bits		
		224 bits		
		256 bits		
		320 bits		
		384 bits		
		512 bits		
		521 bits		
EACv2 Chip Authentication Satisfied dependencies: FCS_CKM.1 (Cryptographic key pair based on ECDH)	ECDH	192 bits	See Table 22	[TR-03110]
		224 bits		
		256 bits		
		320 bits		
		384 bits		
		512 bits		
		521 bits		
Hashing⁴	SHA-1	none	No	[NIST-180-4]
	SHA2-224		Yes	
	SHA2-256			
	SHA2-384			
	SHA2-512		No	[FIPS-202]
	SHA3-224			
	SHA3-256		Yes	
	SHA3-384			
	SHA3-512			

Following Elliptic Curves are available. Table below indicates those that are in TOE certified scope depending on the curve name:

Key Size	Named curve	In TOE certified scope?
192	BrainpoolP192r1	No
	BrainpoolP192t1	No

⁴ Hashing: there is no dependency with FCS_CKM.1 as no key generation algorithm exists for such operation.

	NIST P192	No
224	BrainpoolP224r1	No
	BrainpoolP224t1	No
	NIST P224	No
256	BrainpoolP256r1	Yes
	BrainpoolP256t1	No
	NIST P256	Yes
	FRP 256v1	Yes
320	BrainpoolP320r1	No
	BrainpoolP320t1	No
384	BrainpoolP384r1	Yes
	BrainpoolP384t1	No
	NIST P384	Yes
512	BrainpoolP512r1	Yes
	BrainpoolP512t1	No
521	NIST P521	Yes

Table 22 Supported Elliptic Curves and certified scope validity

FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.6.1 The TSF shall destroy **all cryptographic keys used by the ID-A v1.1 application** when **key is no longer needed**.

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method **physically overwriting the keys in a randomized manner** 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.

The cryptographic key SCD will be destroyed on demand of the signatory. The signatory may want to destruct the SCD stored in the SSCD e.g. after the qualified certificate for the corresponding SVD is not valid anymore. The destruction of the SCD is allowed for 'S.User' with the security attribute 'Role' set to 'R.Sigy', i.e. the signatory may mandate the administrator to destroy the SCD on his behalf.

8.1.2 SSCD parts 2, 4 and 5 only

8.1.2.1 Cryptographic support (FCS)

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 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: **[Standards]**

Cryptographic Key	Cryptographic Key Generation Algorithm	Cryptographic Key Sizes	Standards
SCD/SVD pair or Asymmetric key pair	ECDSA	192 bits	[ECDSA]
		224 bits	
		256 bits	
		320 bits	
		384 bits	
		512 bits	
		521 bits	
	RSA	1024 bits	[RSA-PKCS#1]
		1536 bits	
		2048 bits	
		3072 bits	
		4096 bits	
Ephemeral key pair	DH	1024 bits	[RSA-PKCS#3]
		1536 bits	
		2048 bits	
Cryptographic key pair	ECDH	192 bits	[ISO15946-3]
		224 bits	
		256 bits	
		320 bits	
		384 bits	
		512 bits	
		521 bits	
Symmetric keys	3DES in CBC mode	112 bits	[TR-03110-3] [IAS-ECC] [GP1]
	AES in CBC mode	128 bits	[TR-03110-3] [IAS-ECC] [GP2]
		192 bits	
		256 bits	
GP cryptographic keys	3DES in CBC mode	112 bits	[GP1]
	AES in CBC mode	128 bits	[GP2]
		192 bits	
		256 bits	

8.1.2.2 User data protection (FDP)

The security attributes and 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	authorised, not authorised
SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value

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.**

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 and R.Sigy 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.**

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.**

8.1.3 SSCD parts 3 and 6 only

8.1.3.1 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**

8.1.3.2 User data protection (FDP)

The security attributes and 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	authorised, not authorised
SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value

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 user data~~ **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 ~~user data~~ **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: **The SCD shall be sent by an authorized trusted IT environment.**

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 user 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.**

8.1.4 SSCD part 4 only

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

FTP_ITC.1.2/SVD [Editorially Refined] The TSF shall permit **the CGA** 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.**

8.1.4.2 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.

8.1.4.3 Identification and authentication (FIA)

FIA_API.1 Authentication Proof of Identity

FIA_API.1.1 The TSF shall provide a

- o **Mutual Authentication according to [IAS-ECC]**
- o **PACE Authentication according to [TR-03110] and [ICAO-9303]**

to prove the identity of the **SSCD** by including the following properties

- o **trusted channel via session keys usage**
- o **shared password**

to an external entity.

8.1.5 SSSCD parts 5 and 6 only

8.1.5.1 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 and insertion** has occurred.

8.1.5.2 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 HID** 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:

- o **User authentication according to FIA_UAU.1**

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 SCA** 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 **signature creation**.

8.1.6 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_RND.1 Quality metric for random numbers of [PTF-ST]**.

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: [**Standards**]

Cryptographic Key Generation Algorithm	Cryptographic Key Sizes	Standards
ECDH compliant to [ISO15946]	192 bits to 521 bits	Based on ECDH protocol compliant to [TR-03111], [ISO15946]
DH ⁵	1024, 1536, 2048 bits	Based on Diffie Hellman key derivation protocol compliant to [RSA-PKCS#3], [TR-03110-2]

FIA_UID.1/PACE Timing of identification

FIA_UID.1.1/PACE The TSF shall allow

- To establish a communication channel,
- Carrying out the PACE (PIN, PUK, MRZ or CAN) protocol according to [TR-03110-2],
- To read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
- Carrying out the Terminal Authentication protocol 2 according to [TR-03110-2],
- Carrying out the Chip Authentication protocol 2 according to [TR-03110-2],

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

- To establish a communication channel,
- Carrying out the PACE (PIN, PUK, MRZ, CAN) protocol according to [TR-03110-2],
- To read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
- Carrying out the Terminal Authentication protocol 2 according to [TR-03110-2],

⁵ Only length 2048 is in the scope of this certification

- o **Carrying out the Chip Authentication protocol 2 according to [TR-03110-2],**

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 (PIN, PUK, MRZ or CAN) protocol according to [TR-03110-2],**
- o **Authentication Mechanism based on Triple-DES, AES, DH and ECDH,**
- o **Terminal Authentication 2 protocol according to [TR-03110-2].**

FIA_UAU.5/PACE Multiple authentication mechanisms

FIA_UAU.5.1/PACE The TSF shall provide

- o **PACE (PIN, PUK, MRZ or CAN) protocol according to [TR-03110-2],**
- o **Passive Authentication according to [ICAO-9303],**
- o **Secure Messaging according to [TR-03110-3],**
- o **Symmetric Authentication Mechanism based Triple-DES and AES,**
- o **Terminal Authentication 2 protocol according to [TR-03110-2],**
- o **Chip Authentication 2 according to [TR-03110-2]**

to support user authentication.

FIA_UAU.5.2/PACE The TSF shall authenticate any user's claimed identity according to the following rules:

- o **Having successfully run the PACE (PIN, PUK, MRZ or CAN) protocol. TOE accepts only received commands with correct message authentication codes sent by secure messaging with the key agreed with the terminal by the PACE protocol.**
- o **The TOE accepts the authentication attempt as personalization agent by means of GP authentication.**
- o **The TOE accepts the authentication attempt by means of the Terminal Authentication 2 protocol, only if (i) the terminal presents its static public key PKPCD and the key is successfully verifiable up to the CVCA and (ii) the terminal uses the PICC identifier IDPICC = Comp (ephem-PKPICC-PACE) calculated during, and the secure messaging established by the current PACE (PIN, PUK, MRZ or CAN) authentication.**
- o **Having successfully run Chip Authentication 2, the TOE accepts only received commands with correct message authentication codes sent by secure messaging with the key agreed with the terminal by Chip Authentication 2.**

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 PACE terminal.**

FIA_UAU.6/CA Re-authenticating

FIA_UAU.6.1/CA The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after a successful run of Chip Authentication 2 shall be verified as being sent by the EAC2 terminal.**

FIA_AFL.1/PACE Authentication failure handling

FIA_AFL.1.1/PACE The TSF shall detect when **[selection]** unsuccessful authentication attempts occur related to **[list of authentication events]**.

FIA_AFL.1.2/PACE When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **[list of actions]**.

Selection	List of Authentication Attempts	List of Actions
An administrator configurable positive integer within range of acceptable values 0 to 255 consecutive	authentication attempts using the MRZ or CAN password as the shared password for PACE	wait a linear increasing time, starting at a minimum of configurable amount of time, before the next authentication attempt can be performed
An administrator configurable positive integer within range of acceptable values 0 to 14 consecutive	Consecutive failed authentication attempts using the PIN or PUK as the shared password for PACE leaving a single authentication attempt in contactless mode	suspend the reference value of the PIN or PUK according to [TR-03110-2]
'1'	Consecutive failed authentication attempts using the suspended PIN or PUK as the shared password for PACE in contact mode	block the reference value of PIN or PUK according to [TR-03110-2]
An administrator configurable positive integer within range of acceptable values 0 to 15 consecutive	Consecutive failed authentication attempts using the PIN or PUK with VERIFY PIN command	Block the PIN or the PUK
'1'	Personalisation agent or TOE_Administrator authentication attempt	slow down exponentially the next authentication

FIA_API.1/CA Authentication Proof of Identity

FIA_API.1.1/CA The TSF shall provide a **protocol Chip Authentication 2** according to [TR-03110-2] to prove the identity of the **TOE** by including the following properties

- o **Private Key (SKPICC)**

to an external entity.

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) and selected by the personalisation agent, and all TOE intrinsic secret (i.e. cryptographic) data.**

FDP_ACF.1/TRM Security attribute based access control

FDP_ACF.1.1/TRM The TSF shall enforce the **Access Control SFP** to objects based on the following: **1. Subjects:**

- a.Terminal,**
- b.PACE terminal,**
- c.EAC2 terminal.**

2. Objects:

- a. User data stored in the TOE (including sensitive user data) and selected by the personalisation agent,**
- b. all TOE intrinsic secret (i.e. cryptographic) data.**

3. Security attributes: Terminal Authorization Level (access rights).

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 PACE terminal is allowed to read data objects data (object 2.a) specified in FDP_ACF.1.1/TRM after successful PACE authentication according to [TR-03110-2], as required by FIA_UAU.1/PACE.**
- o **Reading, modifying, writing, or using sensitive user data protected by TAv2 and CAv2 (object 2.a specified in FDP_ACF.1.1/TRM) is only allowed to EAC2 terminals using the following mechanism: The TOE applies the EAC2 protocol (cf. FIA_UAU.5) to determine access rights of the terminal according to [TR-03110-2].**

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 PACE terminal or an EAC2 terminal is not allowed to read, to write, to modify, or to use any user data (object 2.a) specified in FDP_ACF.1.1/TRM.**

- Terminals not using secure messaging are not allowed to read, write, modify, or use any user data (object 2.a) specified in FDP_ACF.1.1/TRM.
- No subject is allowed to read, write, modify, or use the data objects TOE intrinsic secrets (object 2.b) specified in FDP_ACF.1.1/TRM.

FDP_UCT.1/TRM Basic data exchange confidentiality

FDP_UCT.1.1/TRM The TSF shall enforce the **Access Control SFP** to **transmit and receive** 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.

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 **PACE terminal** 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-03110-2].**

FTP_ITC.1.2/PACE [Editorially Refined] The TSF shall permit a **PACE terminal** to initiate communication via the trusted channel.

FTP_ITC.1.3/PACE [Editorially Refined] The TSF shall initiate communication via the trusted channel for **any data exchange between the TOE and a PACE terminal after PACE.**

FMT_SMR.1/PACE Security roles

FMT_SMR.1.1/PACE The TSF shall maintain the roles

- **Manufacturer,**
- **Personalisation Agent,**
- **Terminal,**
- **PACE terminal,**
- **Country Verifying Certification Authority,**
- **Document Verifier,**
- **EAC2 terminal,**
- **Electronic 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

- o Initial CVCA Public Key,
- o meta-data of the initial CVCA Certificate as required in [TR-03110-2], resp [TR-03110-3]
- o initial Current Date

to the personalisation 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

- o CVCA Public Key (PKCVCA),
- o meta-data of the CVCA Certificate as required by [TR-03110-2], resp [TR-03110-3]

to the 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 **the current date** to

- o CVCA,
- o Document Verifier,
- o EAC2 terminal possessing an Accurate Terminal Certificate according to [TR-03110-3].

FMT_MTD.1/PA Management of TSF data

FMT_MTD.1.1/PA The TSF shall restrict the ability to **write** the **card/chip security object(s) (SOC) selected in Access Control SFP and the document Security Object (SOD) selected in Access Control SFP** to the **Personalisation Agent**.

FMT_MTD.1/SK_PICC Management of TSF data

FMT_MTD.1.1/SK_PICC The TSF shall restrict the ability to **load** the **Chip Authentication private key(s) (SKPICC) selected in Access Control SFP** to the **personalisation 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

- o PACE passwords,
- o Personalization Agent Keys,

- The Chip Authentication private key(s) (SKPICC),
 - the Restricted Identification private key(s)
- to none.

FMT_MTD.1/Initialize_PIN Management of TSF data

FMT_MTD.1.1/Initialize_PIN The TSF shall restrict the ability to **write** the **initial PIN** and **PUK** selected in **Access Control SFP** to the **personalisation 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** to **PACE terminal (PACE CAN followed by PACE PIN and/or VERIFY PIN command)**.

FMT_MTD.1/Change_PIN Management of TSF data

FMT_MTD.1.1/Change_PIN The TSF shall restrict the ability to **change** the **blocked PIN** to

- The electronic document holder (using the Current PUK for changing),
- An EAC2 terminal or PACE terminal that has access to change the current PIN.

FMT_MTD.1/Unblock_PIN Management of TSF data

FMT_MTD.1.1/Unblock_PIN The TSF shall restrict the ability to **unblock** the **blocked PIN** (including a blocked RAD) to

- the electronic document holder (using the PUK for unblocking),
- An EAC2 terminal or PACE terminal that has access to unblock the current PIN.

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 **Personalisation 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 2 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**.

FTP_ITC.1/CA2 Inter-TSF trusted channel

FTP_ITC.1.1/CA2 [Editorially Refined] The TSF shall provide a communication channel between itself and **an EAC2 terminal** 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 CA2 protocol according to [TR-03110-2].**

FTP_ITC.1.2/CA2 [Editorially Refined] The TSF shall permit **an EAC2 terminal** to initiate communication via the trusted channel.

FTP_ITC.1.3/CA2 The TSF shall initiate communication via the trusted channel for **any data exchange between the TOE and an EAC2 terminal after Chip Authentication 2.**

FMT_LIM.1 Limited capabilities

FMT_LIM.1.1 The TSF shall limit its capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced

Deploying test features after TOE delivery do not allow

- **User Data to be manipulated and disclosed,**
- **TSF data to be manipulated or disclosed,**
- **software to be reconstructed,**
- **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 do not allow

- **User Data to be manipulated and disclosed,**
- **TSF data to be manipulated or disclosed,**
- **software to be reconstructed,**
- **substantial information about construction of TSF to be gathered which may enable other attacks**

8.2 Security Assurance Requirements

The Evaluation Assurance Level is EAL5 augmented with AVA_VAN.5, ALC_DVS.2 and ALC_FLR.3.

8.3 Security Requirements Rationale

8.3.1 Objectives

8.3.1.1 Security Objectives for the TOE

All SSCD parts

OT.Tamper_Resistance is provided by FPT_PHP.3 to resist physical attacks.

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

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

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

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.

FMT_MTD.1/Unblock_PIN ensures the unblocking of the RAD is made under the sole control of the administrator. In phase 6, the RAD may be loaded on the TOE by the Personalisation Agent as defined in FMT_SMF.1. The Personalisation Agent is authenticated with a mutual authentication performed with FCS_RND.1 and FCS_COP.1, and is authenticated with FMT_SMR.1. Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA_AFL.1/PACE. During the mutual authentication, a session encryption key is agreed between the TOE and the Personalisation Agent and used by the TOE to decrypt the RAD

using FCS_COP.1, ensuring the confidentiality of the RAD during its transfer in phase 6. In phase 6, FMT_MSA.1/Signatory guarantees that the Personalisation Agent cannot sign on behalf of the signatory, ensuring the signature creation features remains under the sole control of the signatory.

OT.Sig_Secure is provided by the cryptographic algorithms specified by FCS_COP.1, 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.SCD_Secrecy is provided by the security functions specified by the following SFR. FCS_CKM.1 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.6 ensure that residual information on SCD is destroyed after the SCD has been used for signature creation and that destruction of SCD leaves no residual information.

The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_TST.1 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA). FDP_UCT.1/SCD and FTP_ITC.1/SCD ensures the confidentiality for SCD import. SFR FPT_EMS.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

OT.Lifecycle_Security is provided by the SFR for SCD/SVD generation FCS_CKM.1, SCD usage FCS_COP.1 and SCD destruction FCS_CKM.6 which ensure cryptographically secure lifecycle of the SCD. 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 SCD usage is ensured 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/Unblock_PIN, FMT_SMF.1 and FMT_SMR.1. The test functions FPT_TST.1 provides failure detection throughout the lifecycle. 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.

SSCD parts 2, 4 and 5 only

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 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.

OT.SCD_Unique implements the requirement of practically unique SCD as laid down in Annex III [DIR], paragraph 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1.

OT.SCD/SVD_Gen addresses that generation of a SCD/SVD pair requires proper user authentication. The TSF specified by FIA_UID.1 and FIA_UAU.1 provide user identification and user authentication prior to enabling access to authorised 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 initialisation. The SFR FMT_MSA.4 defines rules for inheritance of the security attribute 'SCD operational' of the SCD.

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 (additionally to the core PP Part2 SSCD KG) 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.AC_Pers_EAC2 The security objective OT.AC_Pers_EAC2 ensures that only the personalisation agent can write user- and TSF-Data into the TOE, and that some of this data cannot be altered after personalisation. This property is covered by FDP_ACC.1/TRM

and FDP_ACF.1/TRM requiring, amongst other, an appropriate authorization level of an EAC2 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 EAC2 terminal can reach the necessary authorization level, using and managing the PIN (the related SFRs are FIA_AFL.1/PACE, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, and FMT_MTD.1/Initialize_PIN) also support the achievement of this objective. FDP_RIP.1 requires erasing the temporal values PIN and PUK. 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. FMT_MTD.1/PA covers the related property of OT.AC_Pers_EAC2 (writing/updating SOC and SOD and, in generally, personalisation data). Updating such data can only be done by the personalisation agent prior to the operational phase. Thus such data cannot be changed after the personalisation of the document, as required by OT.AC_Pers_EAC2. Finally, FMT_MTD.1/KEY_READ ensures that cryptographic keys for EAC2 can not be read by users.

OT.CA2 The security objective OT.CA2 aims at enabling verification of the authenticity of the TOE as a whole device. This objective is mainly achieved by FIA_API.1/CA using FCS_CKM.1/DH_PACE. CA2 provides an evidence of possessing the Chip Authentication Private Key (SKPICC). FMT_MTD.1/SK_PICC governs creating/loading SKPICC, 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 SKPICC and the session keys, here for CMAC. The authentication token TPICC is calculated using FCS_COP.1. The SFRs FCS_COP.1 and FCS_RND.1 represent the general required support for cryptographic operations. FMT_MTD.1/PA requires that the SOC (containing amongst other, the signature of PKPICC) used for Passive Authentication is allowed to be modified only by the personalisation agent only. Hence is to consider as trustworthy.

OT.Sens_Data_EAC2 The security objective of OT.Sens_Data_EAC2 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. The TA2 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 (FMT_MTD.1/Resume_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Change_PIN) 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.6 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 by FTP_ITC.1/CA2 and FTP_ITC.1/PACE using FCS_COP.1. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. FIA_API.1/CA using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, and FIA_UAU.6/CA. 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. CA2 provides an

evidence of possessing the Chip Authentication Private Key (SKPICC). FMT_MTD.1/SK_PICC governs creating/loading SKPICC, 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 SKPICC and session keys, here for KENC. FMT_MTD.1/PA requires that only the personalisation agent is allowed to modify the SOC (containing amongst other, the signature of PKPICC) used for Passive Authentication. The SFRs FCS_COP.1 and FCS_RND.1 represent the general required support for cryptographic operations. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the related functions and roles.

OT.Data_Authenticity The security objective OT.Data_Authenticity ensures the authenticity of user- and TSF-Data (after Terminal- and the Chip Authentication 2) 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/CA2 and FTP_ITC.1/PACE using FCS_COP.1. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. FIA_API.1/CA using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, and FIA_UAU.6/CA. 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. CA2 provides an evidence of possessing the Chip Authentication Private Key (SKPICC). FMT_MTD.1/SK_PICC governs creating/loading SKPICC, 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 SKPICC and session keys, here for KMAC. FMT_MTD.1/PA requires that the SOC (containing amongst other, the signature of PKPICC) used for Passive Authentication is allowed to be modified only by the personalisation agent only. Hence is to consider as trustworthy. A prerequisite for successful CA2 is an accomplished TA2 as required by FIA_UID.1/PACE, FIA_UAU.1/PACE, supported by FCS_COP.1. The TA2 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/PACE, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN) 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/CA and FCS_CKM.6 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 FCS_COP.1 and FCS_RND.1 represent the general required support for cryptographic operations. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the related functions and roles.

OT.Data_Confidentiality The security objective OT.Data_Confidentiality ensures that the TOE always ensures confidentiality of the user- and TSF-Data stored and, after Terminal- and Chip Authentication 2, 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. The TA2 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/PACE, FMT_MTD.1/Resume_PIN,

FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Initialize_PIN) 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.6 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 by FTP_ITC.1/CA2 and FTP_ITC.1/PACE using FCS_COP.1. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. FIA_API.1/CA using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, and FIA_UAU.6/CA. 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. CA2 provides an evidence of possessing the Chip Authentication Private Key (SKPICC). FMT_MTD.1/SK_PICC governs creating/loading SKPICC, 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 SKPICC and session keys, here for KENC. FMT_MTD.1/PA requires that only the personalisation agent is allowed to modify the SOC (containing amongst other, the signature of PKPICC) used for Passive Authentication. The SFRs FCS_COP.1 and FCS_RND.1 represent the general required support for cryptographic operations. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the related functions and roles.

OT.Data_Integrity The security objective OT.Data_Integrity ensures that the TOE always ensures integrity of stored user- and TSF-Data and, after Terminal- and Chip Authentication 2, 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. The TA2 protocol uses the result of 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, using and management of PIN (FIA_AFL.1/PACE, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Initialize_PIN) 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.6 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/CA2 and FTP_ITC.1/PACE using FCS_COP.1. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. FIA_API.1/CA using FCS_CKM.1/DH_PACE possessing the special properties FIA_UAU.5/PACE and FIA_UAU.6/CA. 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. CA2 provides an evidence of possessing the Chip Authentication Private Key (SKPICC). FMT_MTD.1/SK_PICC governs creating/loading SKPICC, and FMT_MTD.1/KEY_READ requires SKPICC to be unreadable by users; thus its value remains confidential. FDP_RIP.1 requires erasing the values of SKPICC and session keys (here: for KMAC). FMT_MTD.1/PA requires that the SOC (containing amongst other, the signature of PKPICC) used for Passive Authentication is

allowed to be modified only by the personalisation agent. Hence, is to considered as trustworthy. The SFRs FCS_COP.1 and FCS_RND.1 represent general support required for cryptographic operations. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support related functions and roles.

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 roles related.

OT.Prot_Abuse-Func The security objective OT.Prot_Abuse_Func aims preventing 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.

OT.Prot_Inf_Leak The security objective OT.Prot_Inf_Leak aims protection against disclosure of confidential User- or/and TSF-data stored on / processed by the TOE. This objective is achieved

- o by FPT_EMS.1 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.

OT.Prot_Malfunction The security objective OT.Prot_Malfunction aims ensuring 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.

OT.Prot_Phys-Tamper The security objective OT.Prot_Phys-Tamper aims protection 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.Tracing The security objective 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/contact-based interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ, PIN, PUK). This objective is achieved as follows: 1. While establishing PACE communication with CAN, MRZ or PUK (non-blocking authentication / authorization data) by FIA_AFL.1/PACE, 2. while establishing PACE communication using the PIN (blocking authentication data) by FIA_AFL.1/PACE, 3. for listening to PACE communication and for establishing CA2 communication (which is of importance for the current PP, if Chip Security Object and PKPICC are card-individual) by FTP_ITC.1/PACE, 4. and for listening to CA2

communication (readable and writable user data: document details data, biographic data, biometric reference data) by FTP_ITC.1/CA2.

OT.Authentication_Secure is provided by the cryptographic algorithms specified by FCS_COP.1 and FCS_RND.1 for (1) the mutual authentication based on an asymmetric scheme (Device Authentication), (2) the mutual authentication based on symmetric scheme, (3) the authentication of the personalisation agent and of the "TOE_Administrator", (4) the authentication of an entity based on a symmetric scheme, (5) the authentication of an entity based on an asymmetric scheme. All these requirements ensure the cryptographic robustness of the authentication mechanisms. 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. FIA_AFL.1/PACE ensures a correct detection and protection of authentication failure or exhaustive attacks. 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 ((1) and (2)). This trusted channel ensures authenticity, integrity and confidentiality of communication. FCS_CKM.1 and FCS_COP.1 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. The data exchanged through this trusted channel are also protected in confidentiality thanks to FCS_COP.1, 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.6 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. The type of authentication scheme used by the TOE to authenticate the administrator or perform a mutual authentication may be controlled by the "TOE_Administrator". It may enforce the TOE to allow the use of symmetric scheme ((2) and (4)) and/or asymmetric ((1) and (5)) schemes. The TSF specified by FIA_UID.1 and FIA_UAU.1 provide "TOE_Administrator" identification and authentication prior to enabling access to authorised functions. The attributes of the authenticated "TOE_Administrator" are provided by FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4 for static attribute initialisation. Access control is provided by FMT_SMR.1 and FMT_SMF.1. Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA_AFL.1.

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 Personalisation Agent. The Personalisation Agent is authenticated with a mutual authentication performed with

FCS_RND.1 and FCS_COP.1 and is authenticated with FMT_SMR.1. Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA_AFL.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, FMT_MOF.1, FMT_MTD.1/Admin, FMT_MTD.1/Signatory ensures the Personalisation Agent does not control the TOE anymore. In phase 6, the Personalisation 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 Personalisation 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 Personalisation Agent can realize these functions. Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA_AFL.1.

OT.eServices implements the requirement of practically unique TOE's authentication private key, which is provided by the cryptographic algorithms specified by FCS_CKM.1/DH_PACE.

OT.TOE_AuthKey_Unique is provided by the cryptographic mechanisms specified by FCS_COP.1 for (1) the DH Computation, (2) the Certificate verification, (3) the C/S Authentication, (4) the 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. The Agent(s) entitled to perform such operations shall be authenticated with FMT_SMR.1 using cryptographic protocols specified by FCS_COP.1 and FCS_RND.1 for (1) the mutual authentication based on an asymmetric scheme (Device Authentication), (2) the mutual authentication based on symmetric scheme, (3) the authentication of an entity based on a symmetric scheme, (4) the authentication of an entity based on an asymmetric scheme. 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 and FIA_UAU.1. Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA_AFL.1/PACE.

8.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
<u>OT.Tamper Resistance</u>	<u>FPT_PHP.3</u>	<u>Section 9.3.1</u>
<u>OT.Tamper ID</u>	<u>FPT_PHP.1</u>	<u>Section 9.3.1</u>
<u>OT.EMSEC Design</u>	<u>FPT_EMS.1</u>	<u>Section 9.3.1</u>
<u>OT.DTBS Integrity TOE</u>	<u>FDP_SDI.2/DTBS</u>	<u>Section 9.3.1</u>
<u>OT.Sigy SigF</u>	<u>FDP_ACF.1/Signature Creation,</u> <u>FDP_ACC.1/Signature Creation,</u>	<u>Section 9.3.1</u>

Security Objectives	Security Functional Requirements	Rationale
	FDP RIP.1 , FDP SDI.2/DTBS , FIA AFL.1 , FIA UAU.1 , FIA UID.1 , FMT MOF.1 , FMT MSA.1/Signatory , FMT MSA.2 , FMT MSA.3 , FMT MSA.4 , FMT MTD.1/Admin , FMT MTD.1/Signatory , FMT SMR.1 , FMT SMF.1 , FMT MTD.1/Unblock PIN , FCS COP.1 , FIA AFL.1/PACE , FCS RND.1	
OT.Sig Secure	FDP SDI.2/Persistent , FPT TST.1 , FCS COP.1	Section 9.3.1
OT.SCD Secrecy	FCS CKM.1 , FCS CKM.6 , FDP RIP.1 , FDP SDI.2/Persistent , FPT FLS.1 , FPT PHP.3 , FPT TST.1 , FPT EMS.1 , FDP UCT.1/SCD , FTP ITC.1/SCD	Section 9.3.1
OT.Lifecycle Security	FCS CKM.1 , FCS CKM.6 , FDP ACC.1/SCD/SVD Generation , FDP ACF.1/SCD/SVD Generation , FDP ACC.1/SVD Transfer , FDP ACF.1/Signature Creation , FDP ACC.1/Signature Creation , FDP ACF.1/SVD Transfer , 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 SMR.1 , FMT SMF.1 , FPT TST.1 , FCS COP.1 , FDP ACC.1/SCD Import , FDP ACF.1/SCD Import , FDP ITC.1/SCD , FDP UCT.1/SCD , FTP ITC.1/SCD , FMT MTD.1/Unblock PIN	Section 9.3.1
OT.SCD SVD Corresp	FCS CKM.1 , FDP SDI.2/Persistent , FMT MSA.4 , FMT SMF.1	Section 9.3.1
OT.SCD Unique	FCS CKM.1	Section 9.3.1
OT.SCD/SVD Gen	FDP ACC.1/SCD/SVD Generation , FDP ACF.1/SCD/SVD Generation , FIA UAU.1 , FIA UID.1 , FMT MSA.1/Admin , FMT MSA.2 , FMT MSA.3 , FMT MSA.4	Section 9.3.1
OT.SCD Auth Imp	FIA UID.1 , FIA UAU.1 , FDP ACC.1/SCD Import , FDP ACF.1/SCD Import	Section 9.3.1
OT.TOE SSCD Auth	FIA UAU.1 , FIA API.1	Section 9.3.1

Security Objectives	Security Functional Requirements	Rationale
OT.TOE TC SVD Exp	FDP ACF.1/SVD Transfer , FDP ACC.1/SVD Transfer , FDP DAU.2/SVD , FTP ITC.1/SVD	Section 9.3.1
OT.TOE TC VAD Imp	FTP ITC.1/VAD	Section 9.3.1
OT.TOE TC DTBS Imp	FDP UIT.1/DTBS , FTP ITC.1/DTBS	Section 9.3.1
OT.AC Pers EAC2	FDP ACF.1/TRM , FDP RIP.1 , FDP ACC.1/TRM , FMT SMF.1 , FMT SMR.1/PACE , FMT MTD.1/PA , FMT MTD.1/KEY READ , FMT MTD.1/Initialize PIN , FMT MTD.1/Resume PIN , FMT MTD.1/Change PIN , FMT MTD.1/Unblock PIN , FMT MTD.1/INI ENA , FMT MTD.1/INI DIS , FIA UID.1/PACE , FIA UAU.1/PACE , FIA AFL.1/PACE	Section 9.3.1
OT.CA2	FCS CKM.1/DH PACE , FIA API.1/CA , FDP RIP.1 , FMT MTD.1/PA , FMT MTD.1/SK PICC , FMT MTD.1/KEY READ , FCS RND.1 , FCS COP.1	Section 9.3.1
OT.Sens Data EAC2	FTP ITC.1/CA2 , FCS CKM.1/DH PACE , FIA UAU.1/PACE , FIA UAU.5/PACE , FIA API.1/CA , FIA UAU.6/CA , FIA UID.1/PACE , FIA UAU.4/PACE , FIA UAU.6/PACE , FDP ACF.1/TRM , FDP ACC.1/TRM , FDP UCT.1/TRM , FDP UIT.1/TRM , FTP ITC.1/PACE , FMT SMR.1/PACE , FMT MTD.1/CVCA INI , FMT MTD.1/CVCA UPD , FMT MTD.1/DATE , FMT MTD.1/PA , FMT MTD.1/SK PICC , FMT MTD.1/KEY READ , FMT MTD.1/Initialize PIN , FMT MTD.1/Resume PIN , FMT MTD.1/Change PIN , FMT MTD.1/Unblock PIN , FMT MTD.3 , FMT SMF.1 , FCS CKM.6 , FDP RIP.1 , FCS RND.1 , FCS COP.1	Section 9.3.1
OT.Data Authenticity	FTP ITC.1/CA2 , FCS CKM.1/DH PACE , FIA UAU.1/PACE , FIA UAU.5/PACE , FIA API.1/CA , FIA UAU.6/CA , FIA UID.1/PACE , FIA UAU.4/PACE , FIA UAU.6/PACE , FTP ITC.1/PACE ,	Section 9.3.1

Security Objectives	Security Functional Requirements	Rationale
	FMT SMR.1/PACE , FMT MTD.1/CVCA INI , FMT MTD.1/CVCA UPD , FMT MTD.1/DATE , FMT MTD.1/PA , FMT MTD.1/SK PICC , FMT MTD.1/KEY READ , FMT MTD.1/Initialize PIN , FMT MTD.1/Resume PIN , FMT MTD.1/Change PIN , FMT MTD.1/Unblock PIN , FMT MTD.3 , FMT SMF.1 , FCS CKM.6 , FDP RIP.1 , FCS RND.1 , FIA AFL.1/PACE , FCS COP.1	
OT.Data Confidentiality	FTP ITC.1/CA2 , FCS CKM.1/DH PACE , FIA UAU.1/PACE , FIA UAU.5/PACE , FIA API.1/CA , FIA UAU.6/CA , FIA UID.1/PACE , FIA UAU.4/PACE , FIA UAU.6/PACE , FDP ACF.1/TRM , FDP ACC.1/TRM , FDP UCT.1/TRM , FDP UIT.1/TRM , FTP ITC.1/PACE , FMT SMR.1/PACE , FMT MTD.1/CVCA INI , FMT MTD.1/CVCA UPD , FMT MTD.1/DATE , FMT MTD.1/PA , FMT MTD.1/SK PICC , FMT MTD.1/KEY READ , FMT MTD.1/Initialize PIN , FMT MTD.1/Resume PIN , FMT MTD.1/Change PIN , FMT MTD.1/Unblock PIN , FMT MTD.3 , FMT SMF.1 , FCS CKM.6 , FDP RIP.1 , FCS RND.1 , FIA AFL.1/PACE , FCS COP.1	Section 9.3.1
OT.Data Integrity	FTP ITC.1/CA2 , FCS CKM.1/DH PACE , FIA UAU.1/PACE , FIA UAU.5/PACE , FIA API.1/CA , FIA UAU.6/CA , FIA UID.1/PACE , FIA UAU.4/PACE , FIA UAU.6/PACE , FDP ACF.1/TRM , FDP ACC.1/TRM , FDP UCT.1/TRM , FDP UIT.1/TRM , FTP ITC.1/PACE , FMT SMR.1/PACE , FMT MTD.1/CVCA INI , FMT MTD.1/CVCA UPD , FMT MTD.1/DATE , FMT MTD.1/PA , FMT MTD.1/SK PICC , FMT MTD.1/KEY READ , FMT MTD.1/Initialize PIN , FMT MTD.1/Resume PIN , FMT MTD.1/Change PIN , FMT MTD.1/Unblock PIN , FMT MTD.3 , FPT PHP.3 , FMT SMF.1 , FCS CKM.6 ,	Section 9.3.1

Security Objectives	Security Functional Requirements	Rationale
	FDP RIP.1 , FCS RND.1 , FCS COP.1 , FIA AFL.1/PACE	
OT.Identification	FMT SMF.1 , FMT SMR.1/PACE , FMT MTD.1/INI ENA , FMT MTD.1/INI DIS	Section 9.3.1
OT.Prot Abuse-Func	FMT LIM.1 , FMT LIM.2	Section 9.3.1
OT.Prot Inf Leak	FPT FLS.1 , FPT TST.1 , FPT PHP.3 , FPT EMS.1	Section 9.3.1
OT.Prot Malfunction	FPT FLS.1 , FPT TST.1	Section 9.3.1
OT.Prot Phys-Tamper	FPT PHP.3	Section 9.3.1
OT.Tracing	FIA AFL.1/PACE , FTP ITC.1/CA2 , FTP ITC.1/PACE	Section 9.3.1
OT.Authentication Secure	FPT TST.1 , FMT SMR.1 , FMT SMF.1 , FMT MSA.2 , FMT MSA.3 , FMT MSA.4 , FIA UID.1 , FIA AFL.1 , FIA UAU.1 , FDP SDI.2/Persistent , FDP RIP.1 , FCS COP.1 , FCS CKM.6 , FCS CKM.1 , FIA AFL.1/PACE , FCS RND.1	Section 9.3.1
OT.Lifecycle Management	FMT SMR.1 , FMT SMF.1 , FMT MOF.1 , FMT MSA.1/Admin , FMT MSA.2 , FMT MSA.3 , FMT MTD.1/Admin , FMT MTD.1/Signatory , FIA UID.1 , FIA AFL.1 , FIA UAU.1 , FCS COP.1 , FDP ACC.1/SCD/SVD Generation , FDP ACF.1/SCD/SVD Generation , FMT MTD.1/TOE State , FCS RND.1	Section 9.3.1
OT.eServices	FCS CKM.1/DH PACE	Section 9.3.1
OT.TOE AuthKey Unique	FMT SMR.1 , FMT SMF.1 , FIA UID.1 , FIA UAU.1 , FCS COP.1 , FIA AFL.1/PACE , FCS RND.1	Section 9.3.1

Table 23 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives	Rationale
FPT EMS.1	OT.EMSEC Design , OT.SCD Secrecy , OT.Prot Inf Leak	
FPT FLS.1	OT.SCD Secrecy , OT.Prot Inf Leak , OT.Prot Malfunction	

Security Functional Requirements	Security Objectives	Rationale
<u>FPT_PHP.1</u>	<u>OT.Tamper ID</u>	
<u>FPT_PHP.3</u>	<u>OT.Tamper Resistance,</u> <u>OT.SCD Secrecy,</u> <u>OT.Data Integrity,</u> <u>OT.Prot Inf Leak, OT.Prot Phys-Tamper</u>	
<u>FPT_TST.1</u>	<u>OT.Sig Secure, OT.SCD Secrecy,</u> <u>OT.Lifecycle Security,</u> <u>OT.Prot Inf Leak,</u> <u>OT.Prot Malfunction,</u> <u>OT.Authentication Secure</u>	
<u>FMT_SMR.1</u>	<u>OT.Sigy SigF,</u> <u>OT.Lifecycle Security,</u> <u>OT.Authentication Secure,</u> <u>OT.Lifecycle Management,</u> <u>OT.TOE AuthKey Unique</u>	
<u>FMT_SMF.1</u>	<u>OT.Sigy SigF,</u> <u>OT.Lifecycle Security,</u> <u>OT.SCD SVD Corresp,</u> <u>OT.AC Pers EAC2,</u> <u>OT.Sens Data EAC2,</u> <u>OT.Data Authenticity,</u> <u>OT.Data Confidentiality,</u> <u>OT.Data Integrity,</u> <u>OT.Identification,</u> <u>OT.Authentication Secure,</u> <u>OT.Lifecycle Management,</u> <u>OT.TOE AuthKey Unique</u>	
<u>FMT_MOF.1</u>	<u>OT.Sigy SigF,</u> <u>OT.Lifecycle Security,</u> <u>OT.Lifecycle Management</u>	
<u>FMT_MSA.1/Admin</u>	<u>OT.Lifecycle Security,</u> <u>OT.SCD/SVD Gen,</u> <u>OT.Lifecycle Management</u>	
<u>FMT_MSA.1/Signatory</u>	<u>OT.Sigy SigF,</u> <u>OT.Lifecycle Security</u>	
<u>FMT_MSA.2</u>	<u>OT.Sigy SigF,</u> <u>OT.Lifecycle Security,</u> <u>OT.SCD/SVD Gen,</u> <u>OT.Authentication Secure,</u> <u>OT.Lifecycle Management</u>	
<u>FMT_MSA.3</u>	<u>OT.Sigy SigF,</u> <u>OT.Lifecycle Security,</u> <u>OT.SCD/SVD Gen,</u>	

Security Functional Requirements	Security Objectives	Rationale
	<u>OT.Authentication Secure</u> , <u>OT.Lifecycle Management</u>	
<u>FMT MSA.4</u>	<u>OT.Sigy SigF</u> , <u>OT.Lifecycle Security</u> , <u>OT.SCD SVD Corresp</u> , <u>OT.SCD/SVD Gen</u> , <u>OT.Authentication Secure</u>	
<u>FMT MTD.1/Admin</u>	<u>OT.Sigy SigF</u> , <u>OT.Lifecycle Security</u> , <u>OT.Lifecycle Management</u>	
<u>FMT MTD.1/Signatory</u>	<u>OT.Sigy SigF</u> , <u>OT.Lifecycle Security</u> , <u>OT.Lifecycle Management</u>	
<u>FIA UID.1</u>	<u>OT.Sigy SigF</u> , <u>OT.SCD/SVD Gen</u> , <u>OT.SCD Auth Imp</u> , <u>OT.Authentication Secure</u> , <u>OT.Lifecycle Management</u> , <u>OT.TOE AuthKey Unique</u>	
<u>FIA AFL.1</u>	<u>OT.Sigy SigF</u> , <u>OT.Authentication Secure</u> , <u>OT.Lifecycle Management</u>	
<u>FIA UAU.1</u>	<u>OT.Sigy SigF</u> , <u>OT.SCD/SVD Gen</u> , <u>OT.SCD Auth Imp</u> , <u>OT.TOE SSCD Auth</u> , <u>OT.Authentication Secure</u> , <u>OT.Lifecycle Management</u> , <u>OT.TOE AuthKey Unique</u>	
<u>FDP SDI.2/DTBS</u>	<u>OT.DTBS Integrity TOE</u> , <u>OT.Sigy SigF</u>	
<u>FDP SDI.2/Persistent</u>	<u>OT.Sig Secure</u> , <u>OT.SCD Secrecy</u> , <u>OT.SCD SVD Corresp</u> , <u>OT.Authentication Secure</u>	
<u>FDP RIP.1</u>	<u>OT.Sigy SigF</u> , <u>OT.SCD Secrecy</u> , <u>OT.AC Pers EAC2</u> , <u>OT.CA2</u> , <u>OT.Sens Data EAC2</u> , <u>OT.Data Authenticity</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u> , <u>OT.Authentication Secure</u>	
<u>FDP ACC.1/Signature Creation</u>	<u>OT.Sigy SigF</u> , <u>OT.Lifecycle Security</u>	
<u>FDP ACF.1/Signature Creation</u>	<u>OT.Sigy SigF</u> , <u>OT.Lifecycle Security</u>	

Security Functional Requirements	Security Objectives	Rationale
<u>FCS COP.1</u>	<u>OT.Sigy SigE, OT.Sig Secure, OT.Lifecycle Security, OT.CA2, OT.Sens Data EAC2, OT.Data Authenticity, OT.Data Confidentiality, OT.Data Integrity, OT.Authentication Secure, OT.Lifecycle Management, OT.TOE AuthKey Unique</u>	
<u>FCS CKM.6</u>	<u>OT.SCD Secrecy, OT.Lifecycle Security, OT.Sens Data EAC2, OT.Data Authenticity, OT.Data Confidentiality, OT.Data Integrity, OT.Authentication Secure</u>	
<u>FCS CKM.1</u>	<u>OT.SCD Secrecy, OT.Lifecycle Security, OT.SCD SVD Corresp, OT.SCD Unique, OT.Authentication Secure</u>	
<u>FDP ACC.1/SVD Transfer</u>	<u>OT.Lifecycle Security, OT.TOE TC SVD Exp</u>	
<u>FDP ACF.1/SVD Transfer</u>	<u>OT.Lifecycle Security, OT.TOE TC SVD Exp</u>	
<u>FDP ACC.1/SCD/SVD Generation</u>	<u>OT.Lifecycle Security, OT.SCD/SVD Gen, OT.Lifecycle Management</u>	
<u>FDP ACF.1/SCD/SVD Generation</u>	<u>OT.Lifecycle Security, OT.SCD/SVD Gen, OT.Lifecycle Management</u>	
<u>FTP ITC.1/SCD</u>	<u>OT.SCD Secrecy, OT.Lifecycle Security</u>	
<u>FDP UCT.1/SCD</u>	<u>OT.SCD Secrecy, OT.Lifecycle Security</u>	
<u>FDP ITC.1/SCD</u>	<u>OT.Lifecycle Security</u>	
<u>FDP ACC.1/SCD Import</u>	<u>OT.Lifecycle Security, OT.SCD Auth Imp</u>	
<u>FDP ACF.1/SCD Import</u>	<u>OT.Lifecycle Security, OT.SCD Auth Imp</u>	
<u>FTP ITC.1/SVD</u>	<u>OT.TOE TC SVD Exp</u>	
<u>FDP DAU.2/SVD</u>	<u>OT.TOE TC SVD Exp</u>	

Security Functional Requirements	Security Objectives	Rationale
<u>FIA_API.1</u>	<u>OT.TOE SSCD Auth</u>	
<u>FDP UIT.1/DTBS</u>	<u>OT.TOE TC DTBS Imp</u>	
<u>FTP ITC.1/VAD</u>	<u>OT.TOE TC VAD Imp</u>	
<u>FTP ITC.1/DTBS</u>	<u>OT.TOE TC DTBS Imp</u>	
<u>FCS_RND.1</u>	<u>OT.Sigy SigF, OT.CA2,</u> <u>OT.Sens Data EAC2,</u> <u>OT.Data Authenticity,</u> <u>OT.Data Confidentiality,</u> <u>OT.Data Integrity,</u> <u>OT.Authentication Secure,</u> <u>OT.Lifecycle Management,</u> <u>OT.TOE AuthKey Unique</u>	
<u>FCS_CKM.1/DH PACE</u>	<u>OT.CA2, OT.Sens Data EAC2,</u> <u>OT.Data Authenticity,</u> <u>OT.Data Confidentiality,</u> <u>OT.Data Integrity, OT.eServices</u>	
<u>FIA_UID.1/PACE</u>	<u>OT.AC Pers EAC2,</u> <u>OT.Sens Data EAC2,</u> <u>OT.Data Authenticity,</u> <u>OT.Data Confidentiality,</u> <u>OT.Data Integrity</u>	
<u>FIA_UAU.1/PACE</u>	<u>OT.AC Pers EAC2,</u> <u>OT.Sens Data EAC2,</u> <u>OT.Data Authenticity,</u> <u>OT.Data Confidentiality,</u> <u>OT.Data Integrity</u>	
<u>FIA_UAU.4/PACE</u>	<u>OT.Sens Data EAC2,</u> <u>OT.Data Authenticity,</u> <u>OT.Data Confidentiality,</u> <u>OT.Data Integrity</u>	
<u>FIA_UAU.5/PACE</u>	<u>OT.Sens Data EAC2,</u> <u>OT.Data Authenticity,</u> <u>OT.Data Confidentiality,</u> <u>OT.Data Integrity</u>	
<u>FIA_UAU.6/PACE</u>	<u>OT.Sens Data EAC2,</u> <u>OT.Data Authenticity,</u> <u>OT.Data Confidentiality,</u> <u>OT.Data Integrity</u>	
<u>FIA_UAU.6/CA</u>	<u>OT.Sens Data EAC2,</u> <u>OT.Data Authenticity,</u> <u>OT.Data Confidentiality,</u> <u>OT.Data Integrity</u>	

Security Functional Requirements	Security Objectives	Rationale
<u>FIA AFL.1/PACE</u>	<u>OT.Sigy SigF</u> , <u>OT.AC Pers EAC2</u> , <u>OT.Data Authenticity</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u> , <u>OT.Tracing</u> , <u>OT.Authentication Secure</u> , <u>OT.TOE AuthKey Unique</u>	
<u>FIA API.1/CA</u>	<u>OT.CA2</u> , <u>OT.Sens Data EAC2</u> , <u>OT.Data Authenticity</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u>	
<u>FDP ACC.1/TRM</u>	<u>OT.AC Pers EAC2</u> , <u>OT.Sens Data EAC2</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u>	
<u>FDP ACF.1/TRM</u>	<u>OT.AC Pers EAC2</u> , <u>OT.Sens Data EAC2</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u>	
<u>FDP UCT.1/TRM</u>	<u>OT.Sens Data EAC2</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u>	
<u>FDP UIT.1/TRM</u>	<u>OT.Sens Data EAC2</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u>	
<u>FTP ITC.1/PACE</u>	<u>OT.Sens Data EAC2</u> , <u>OT.Data Authenticity</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u> , <u>OT.Tracing</u>	
<u>FMT SMR.1/PACE</u>	<u>OT.AC Pers EAC2</u> , <u>OT.Sens Data EAC2</u> , <u>OT.Data Authenticity</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u> , <u>OT.Identification</u>	
<u>FMT MTD.1/CVCA INI</u>	<u>OT.Sens Data EAC2</u> , <u>OT.Data Authenticity</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u>	
<u>FMT MTD.1/CVCA UPD</u>	<u>OT.Sens Data EAC2</u> , <u>OT.Data Authenticity</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u>	
<u>FMT MTD.1/DATE</u>	<u>OT.Sens Data EAC2</u> , <u>OT.Data Authenticity</u> ,	

Security Functional Requirements	Security Objectives	Rationale
	<u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u>	
<u>FMT MTD.1/PA</u>	<u>OT.AC Pers EAC2</u> , <u>OT.CA2</u> , <u>OT.Sens Data EAC2</u> , <u>OT.Data Authenticity</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u>	
<u>FMT MTD.1/SK PICC</u>	<u>OT.CA2</u> , <u>OT.Sens Data EAC2</u> , <u>OT.Data Authenticity</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u>	
<u>FMT MTD.1/KEY READ</u>	<u>OT.AC Pers EAC2</u> , <u>OT.CA2</u> , <u>OT.Sens Data EAC2</u> , <u>OT.Data Authenticity</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u>	
<u>FMT MTD.1/Initialize PIN</u>	<u>OT.AC Pers EAC2</u> , <u>OT.Sens Data EAC2</u> , <u>OT.Data Authenticity</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u>	
<u>FMT MTD.1/Resume PIN</u>	<u>OT.AC Pers EAC2</u> , <u>OT.Sens Data EAC2</u> , <u>OT.Data Authenticity</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u>	
<u>FMT MTD.1/Change PIN</u>	<u>OT.AC Pers EAC2</u> , <u>OT.Sens Data EAC2</u> , <u>OT.Data Authenticity</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u>	
<u>FMT MTD.1/Unblock PIN</u>	<u>OT.Sigy SigF</u> , <u>OT.Lifecycle Security</u> , <u>OT.AC Pers EAC2</u> , <u>OT.Sens Data EAC2</u> , <u>OT.Data Authenticity</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u>	
<u>FMT MTD.1/TOE State</u>	<u>OT.Lifecycle Management</u>	
<u>FMT MTD.3</u>	<u>OT.Sens Data EAC2</u> , <u>OT.Data Authenticity</u> , <u>OT.Data Confidentiality</u> , <u>OT.Data Integrity</u>	

Security Functional Requirements	Security Objectives	Rationale
FMT_MTD.1/INI_ENA	OT.AC Pers EAC2 , OT.Identification	
FMT_MTD.1/INI_DIS	OT.AC Pers EAC2 , OT.Identification	
FTP_ITC.1/CA2	OT.Sens Data EAC2 , OT.Data Authenticity , OT.Data Confidentiality , OT.Data Integrity , OT.Tracing	
FMT_LIM.1	OT.Prot Abuse-Func	
FMT_LIM.2	OT.Prot Abuse-Func	

Table 24 SFRs and Security Objectives

8.3.3 Dependencies

8.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FCS_CKM.1	(FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1) and (FCS_RBG.1 or FCS_RNG.1) and (FCS_CKM.6)	FCS_COP.1 , FCS_CKM.6 , FCS_RND.1
FCS_CKM.1/DH_PACE	(FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1) and (FCS_RBG.1 or FCS_RNG.1) and (FCS_CKM.6)	FCS_COP.1 , FCS_CKM.6 , FCS_RND.1
FCS_CKM.6	(FCS_CKM.1 or FCS_CKM.5 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1 , FDP_ITC.1/SCD
FCS_COP.1	(FCS_CKM.1 or or FCS_CKM.5 FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.6)	FCS_CKM.6 , FCS_CKM.1 , FDP_ITC.1/SCD
FCS_RND.1	No Dependencies	
FDP_ACC.1/SCD_Import	(FDP_ACF.1)	FDP_ACF.1/SCD Import
FDP_ACC.1/SCD/SVD_Generation	(FDP_ACF.1)	FDP_ACF.1/SCD/SVD Generation
FDP_ACC.1/Signature_Creation	(FDP_ACF.1)	FDP_ACF.1/Signature Creation

Requirements	CC Dependencies	Satisfied Dependencies
FDP_ACC.1/SVD Transfer	(FDP_ACF.1)	FDP_ACF.1/SVD Transfer
FDP_ACC.1/TRM	(FDP_ACF.1)	FDP_ACF.1/TRM
FDP_ACF.1/SCD/SVD Generation	(FDP_ACC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/SCD/SVD Generation
FDP_ACF.1/SCD Import	(FDP_ACC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/SCD Import
FDP_ACF.1/Signature Creation	(FDP_ACC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/Signature Creation
FDP_ACF.1/SVD Transfer	(FDP_ACC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/SVD Transfer
FDP_ACF.1/TRM	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/TRM
FDP_DAU.2/SVD	(FIA_UID.1)	FIA_UID.1
FDP_ITC.1/SCD	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/SCD Import
FDP_RIP.1	No Dependencies	
FDP_SDI.2/DTBS	No Dependencies	
FDP_SDI.2/Persistent	No Dependencies	
FDP_UCT.1/SCD	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FTP_ITC.1/SCD, FDP_ACC.1/SCD Import
FDP_UCT.1/TRM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/TRM, FTP_ITC.1/PACE
FDP_UIT.1/DTBS	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/Signature Creation, FTP_ITC.1/DTBS
FDP_UIT.1/TRM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/TRM, FTP_ITC.1/PACE
FIA_AFL.1	(FIA_UAU.1)	FIA_UAU.1
FIA_AFL.1/PACE	(FIA_UAU.1)	FIA_UAU.1/PACE
FIA_API.1	No Dependencies	
FIA_API.1/CA	No Dependencies	
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FIA_UAU.1/PACE	(FIA_UID.1)	FIA_UID.1/PACE

Requirements	CC Dependencies	Satisfied Dependencies
FIA_UAU.4/PACE	No Dependencies	
FIA_UAU.5/PACE	No Dependencies	
FIA_UAU.6/PACE	No Dependencies	
FIA_UAU.6/CA	No Dependencies	
FIA_UID.1	No Dependencies	
FIA_UID.1/PACE	No Dependencies	
FMT_LIM.1	No Dependencies	
FMT_LIM.2	No Dependencies	
FMT_MOF.1	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1 , FMT_SMF.1
FMT_MSA.1/Admin	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1 , FMT_SMF.1 , FDP_ACC.1/Signature Creation , FDP_ACC.1/SVD Transfer , FDP_ACC.1/SCD/SVD Generation , FDP_ACC.1/SCD Import
FMT_MSA.1/Signatory	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1 , FMT_SMF.1 , FDP_ACC.1/Signature Creation
FMT_MSA.2	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1 , FMT_MSA.1/Admin , FMT_MSA.1/Signatory , FDP_ACC.1/Signature Creation , FDP_ACC.1/SCD/SVD Generation
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1 , FMT_MSA.1/Admin , FMT_MSA.1/Signatory
FMT_MSA.4	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.1/Signature Creation , FDP_ACC.1/SCD/SVD Generation
FMT_MTD.1/Admin	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1 , FMT_SMF.1
FMT_MTD.1/Change PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE , FMT_SMF.1
FMT_MTD.1/CVCA INI	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE , FMT_SMF.1
FMT_MTD.1/CVCA UPD	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE , FMT_SMF.1

Requirements	CC Dependencies	Satisfied Dependencies
FMT_MTD.1/DATE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE , FMT_SMF.1
FMT_MTD.1/INI_DIS	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE , FMT_SMF.1
FMT_MTD.1/INI_ENA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE , FMT_SMF.1
FMT_MTD.1/Initialize PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE , FMT_SMF.1
FMT_MTD.1/KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE , FMT_SMF.1
FMT_MTD.1/PA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE , FMT_SMF.1
FMT_MTD.1/Resume PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE , FMT_SMF.1
FMT_MTD.1/Signatory	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1 , FMT_SMF.1
FMT_MTD.1/SK_PICC	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE , FMT_SMF.1
FMT_MTD.1/TOE State	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE , FMT_SMR.1 , FMT_SMF.1
FMT_MTD.1/Unblock PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/PACE , FMT_SMF.1
FMT_MTD.3	(FMT_MTD.1)	FMT_MTD.1/CVCA_INI , FMT_MTD.1/CVCA_UPD , FMT_MTD.1/DATE
FMT_SMF.1	No Dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1
FMT_SMR.1/PACE	(FIA_UID.1)	FIA_UID.1/PACE
FPT_EMS.1	No Dependencies	
FPT_FLS.1	No Dependencies	
FPT_PHP.1	No Dependencies	
FPT_PHP.3	No Dependencies	
FPT_TST.1	No Dependencies	
FTP_ITC.1/CA2	No Dependencies	
FTP_ITC.1/DTBS	No Dependencies	
FTP_ITC.1/PACE	No Dependencies	
FTP_ITC.1/SCD	No Dependencies	
FTP_ITC.1/SVD	No Dependencies	

Requirements	CC Dependencies	Satisfied Dependencies
FTP_ITC.1/VAD	No Dependencies	

Table 25 SFRs Dependencies

Rationale for the exclusion of Dependencies

The dependency FMT_MSA.3 of FDP_ACF.1/TRM is discarded. The access control TSF according to FDP_ACF.1/TRM uses security attributes that have been defined during personalisation, and that are fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary.

8.3.3.2 SARs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.5 , ADV_TDS.4
ADV_FSP.5	(ADV_IMP.1) and (ADV_TDS.1)	ADV_IMP.1 , ADV_TDS.4
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.4 , ALC_TAT.2
ADV_TDS.4	(ADV_FSP.5)	ADV_FSP.5
ADV_INT.2	(ADV_IMP.1) and (ADV_TDS.3) and (ALC_TAT.1)	ADV_IMP.1 , ADV_TDS.4 , ALC_TAT.2
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.5
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.5 , ALC_DVS.2 , ALC_LCD.1
ALC_CMS.5	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	
ALC_FLR.3	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.2	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1 , ASE_INT.1 , ASE_REQ.2
ASE_ECD.1	No Dependencies	
ASE_INT.1	No Dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1 , ASE_OBJ.2
ASE_SPD.1	No Dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.5 , ASE_INT.1 , ASE_REQ.2

Requirements	CC Dependencies	Satisfied Dependencies
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.5 , ATE_FUN.1
ATE_DPT.3	(ADV_ARC.1) and (ADV_TDS.4) and (ATE_FUN.1)	ADV_ARC.1 , ADV_TDS.4 , ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.5 , AGD_OPE.1 , AGD_PRE.1 , ATE_COV.2 , ATE_FUN.1
AVA_VAN.5	(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)	ADV_ARC.1 , ADV_FSP.5 , ADV_IMP.1 , ADV_TDS.4 , AGD_OPE.1 , AGD_PRE.1 , ATE_DPT.3

Table 26 SARs Dependencies

8.3.4 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 specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, 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.3: Systematic flaw remediation

8.3.5 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 application, i.e., the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure.

8.3.6 ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE. Due to the nature of the TOE, there is a need to justify the sufficiency of these procedures to protect the confidentiality and the integrity of the TOE. The TOE shall be protected in confidentiality and integrity during its development to meet the security objective OT.Lifecycle_Security.

8.3.7 ALC_FLR.3 Systematic flaw remediation

The flaw remediation assurance improves a rigorous management for updating the TOE in the context of sensible market where the Javacard Plateform need a long life cycle to embed the additionnal applications.

9 TOE Summary Specification

9.1 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 **[IFX-ST]**, **[PTF-ST]** and are not redefined in this security target, although they must be considered for the TOE.

9.1.1 Chip security functionalities

The full list of the IC Platform security functionalities can be checked in the IC Platform Security Target **[IFX-ST]**.

9.1.2 Platform security functionalities

The full list of the JC Platform security functionalities can be checked in the JC Platform Security Target **[PTF-ST]**.

9.1.3 Application security functionalities

SF.AUTHENTICATION

Only authenticated terminals can get access to the user data stored on the TOE. The ID-A applet offers several authentication schemes enabling to authenticate different roles, such as:

- o The signatory entitled to use the services offered by the card. It is called "User Authentication".
- o The device communicating with the card, to establish a trusted channel (secure messaging) and protect the communication. It is called "Device authentication".
- o The administrator of a service, to administrate some features. It is called "Role authentication".

The **User authentication** is based on the submission of a PIN/password.

- o Knowledge based: The Authentication of the user relies on a shared secret (PIN), known by both the holder and the smartcard. The Card holder is authenticated by the means of the VERIFY command. For each SCD separate signatory's RADs (PINs) are assigned. The verification process uses a velocity checking mechanism, thus a remaining tries counter and a maximum error counter are defined for each PIN. If the verification fails, the tries 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 blocked and can no longer be used. Note that a successful verification of the PIN resets its remaining tries counter to the maximum error counter.

The **Device Authentication** aims at authenticating both entities willing to communicate and securing the communication between the card and a service provider (it might be a terminal, a server, etc).

- o Authentication Scheme: The smart card implements a mutual authentication scheme. This one relies either on 3DES or AES Cipher block and used to:

- Authenticate the terminal and the card.
- Generate two temporary keys that will be further used to compute session keys for the secure messaging in the subsequent commands.
- Initialize the counter used at each checksum computation.
- PACE Authentication: PACE establishes Secure Messaging between the ID-A application and a terminal based on weak (short) passwords:
 - Strong session keys are provided independent of the strength of the password.
 - The entropy of the password(s) used to authenticate the terminal can be very low (e.g., 6 digits are sufficient in general).

The detailed specification of the PACE protocol can be found in **[ICAO-9303]**. As opposed to the original context in which PACE is used, i.e., before the application selection, the ID-A application simply considers the PACE protocol as another way to initiate secure messaging with the terminal. In other words, PACE is a precondition that may or may not be required before executing any command.

- EAC2 as defined in **[TR-03110-2]** which consists of two parts:
 - Chip Authentication aims at authenticating the chip and initiates a secure communication channel to communicate. The protocol in Version 2 provides explicit authentication of the chip by verifying the authentication token and implicit authentication of the stored data by performing Secure Messaging using the new session keys.
 - Terminal Authentication protocol uses the secure messaging established by the Chip Authentication Mechanism to protect the confidentiality and integrity of the sensitive data during their transmission from the TOE to the terminal. Therefore, Terminal Authentication can only be performed if Chip Authentication has been successfully executed.

The **Role Authentication** presents the procedure to authenticate an external entity to the card in order to associate to it a specific role (e.g. access rights). Two schemes may be used, relying either on 3DES, AES or RSA Cipher block. The following procedure describes:

- The cryptographic operation that allows the authentication
- The specification of the associated role in the card This feature is described in **[IAS_ECC]**. In ID-A, the Access conditions "Secure Messaging" mandates both a successful terminal authentication and an active secure messaging session. This security function manages authentication failure: when the "highest value in the configurable range of positive numbers fixed by the Administrator" unsuccessful authentication attempts have been met, the TSF shall block the RAD. This security functionality allows the following operations to be performed before the user is authenticated:
 - Identification of the user,
 - Establishing a trusted path between the HID and the TOE,
 - Establishing a trusted channel between the SCA and the TOE,
 - Establishing a trusted channel between the CGA and the TOE.

SF.APP_CRYPTO

This SF performs high level cryptographic operations:

- key generation:
 - SF.APP_CRYPTO performs RSA CRT key generation of size 1024, 1536, 2048, 3072 and 4096 bits in conformance with RSA PKCS#1 v2.1.

- SF.APP_CRYPTO performs Elliptic curves key generation of size 192,224,256, 320, 384,512 and 521 bits in conformance with ANS X9.62.
- o Digital signature generation:
 - the signature generation function shall have an access condition based upon previous authentication of user.
 - signature generation by using ECDSA algorithm with cryptographic key sizes of 192,224,256, 320, 384,512 and 521(provided by the cryptographic library of the Platform).
 - signature generation by using RSA algorithm with cryptographic key sizes of 1024, 1536, 2048, 3072 and 4096 bits (provided by Platform).
- o SCD/SVD key pair consistency check: SF.APP_CRYPTO performs SCD/SVD consistency check before signature generation by signature generation followed by signature verification. If the signature verification does not match the signature generation, then the key pair is not consistent.
- o Key agreement using anonymous DH with key sizes 1024, 1536, 2048, 3072 and 4096 bits.
- o PACE Authentication (IM and GM) with ECDH(192,224,256, 320,384, 512, 521 bits), AES(128 192 256 bits) and DES(128).
- o Secure messaging (encryption and decryption) using:
 - Triple DES in CBC mode (key size 112 bits).
 - AES in CBC mode (key sizes 128,192,256 bits).
- o Secure messaging (message authentication code) using:
 - ISO/IEC 9797-1 algorithm 3 padding 2 (3DES) with key size 112 bits.
 - AES CMAC with key sizes 128,192 and 256 bits.
- o Ciphering Key Decryption using:
 - RSA-OAEP SHA-1 and SHA-256, RSA PKCS#1v1.5 with key sizes 1024, 1536, 2048, 3072, and 4096 bits
 - ECDH with key sizes 192, 224, 256, 320, 384, 512, and 521 bits
- o Authentication cryptogram creation/verification: SF.APP_CRYPTO performs the following authentication cryptogram calculation/verification:
 - Mutual authentication based on TDES or AES
 - PACE authentication based on **[ICAO-9303]**
- o Random number generation that meet FCS_RND.1 Quality metric for random numbers of **[PTF-ST]**.
- o Client Server Authentication using RSA-PKCS#1v1.5 and RSA-PKCS#1v2.1
- o Symmetric Role Authentication using TDES and AES
- o Asymmetric Role authentication using RSA with ISO/IEC 9796-2 with SHA-1 SHA-224 SHA-256 SHA-384 or SHA-512 with key sizes 1024, 1536 or 2048 bits
- o Symmetric Device Authentication using TDES and AES
- o Certificate verification for IAS PKI using RSA
- o Certificate verification foe EAS PKI using ECDSA
- o Asymmetric Internal Device Authentication using RSA
- o Asymmetric External Device Authentication using RSA
- o EACv2 Terminal Authentication using ECDSA
- o EACv2 Chip Authentication using ECDH

- o Hashing algorithms SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384 and SHA3-512
- o GP Secret data encryption using SCP02 and SCP03.
- o Symmetric Encryption and Decryption using AEC-CBC mode with key sizes 128, 192, 256 bits
- o Data Hashing: SF.APP_CRYPTO performs SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384 and SHA3-512 in conformance with NIST FIPS PUB 180-2, in order to calculate a hash value.
- o Certificate Calculation and verification.
- o RSA and ECC based key decipherment.

All cryptographic functionalities are provided by the platform **[PTF-ST]**.

SF.MANAGEMENT

This SF manages the access to objects (files, directories, data and secrets) stored in the ID-A file system. It also controls write access of initialization, pre-personalisation and personalisation data.

This SF ensures secure management of secrets such as cryptographic keys. It also covers access to keys as well as secure key deletion.

This SF controls all the operations relative to the RAD/VAD management, including the Cardholder (signatory) authentication:

- o RAD creation: the RAD is stored and is associated to a maximum successful presentation number (usage counter) and to a maximum error number.
- o VAD verification: the RAD can be accessed only if its format and integrity are correct and if the usage counter has not reached 0. If the RAD is blocked, then it cannot be used anymore until unblocked.
- o RAD ratification counter: The number of authentication attempts is limited by a counter associated to the RAD. The counter is decremented each time the VAD verification fails. The RAD cannot be used any longer if the counter reaches zero.
- o RAD usage counter: the usage counter is decremented each time the RAD is verified successfully. When this counter reaches 0, the RAD cannot be verified anymore.
- o RAD modification: the RAD can be changed by the cardholder (loading a new value). The RAD is managed and stored by the application. The operations on RAD and VAD are performed thanks to services offered by the platform.

This SF manages the security environment of the application and:

- o Maintains the roles (e.g. Signatory and Administrator).
- o Controls if the authentication required for a specific operation has been performed with success.
- o Manages restriction to security function access and to security attribute modification.
- o Ensures that only secure values are accepted for security attributes. This security functionality restricts the ability to perform the function Signature creation SFP to Signatory. This security functionality ensures that only Administrator is authorized to
 - Modify Initialization SFP and Signature creation SFP attributes
 - Specify alternative default values

This SF provides the electronic signature application with access control and ensures that the following operations are executed by authorized roles:

- o Export of SVD to CGA
- o Generation of SCD/SVD pair by the Signatory
- o Creation of RAD by the Administrator
- o Signing of DTBS/R by S.Signatory
- o Destruction of SCD/SVD pair on-demand by the Signatory

This SF manages Session key generation: Session keys are protected in integrity and confidentiality during generation.

This SF enforces secure storage of the session keys during generation. This SF manages Secret destruction: This SF calls the security function of the JC Platform to erase keys.

This SF manages Secret loading: Loading of a secret is always done by an authorized user through a secure command. This command is accepted only after authentication of the authorized user.

This SF manages Secret transfer: This SF manages the secure transfer of every secret to the crypto processor when used for cryptographic operation. Access control is enforced by the APDU methods as specified in the interface defined in the functional specification.

SF.TRUSTED_CHANNEL

This SF 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.

The ID-A Package performs the following secure messaging tasks with external applications (SCA, HID or CGA) for protection of the communication data as the DTBS, authentication data as the VAD or for ensuring the integrity of the SVD:

- o PACE or mutual authentication or EAC2 or device authentication with privacy protection used to establish session keys for secure messaging.
- o Encryption and decryption of the transmitted message.
- o MAC generation and verification for secure messaging.
- o ECDH key agreement.
- o Secure hash computation.
- o Random number generation.

This SF manages four modes of secure channel during the personalisation phase:

- o No secure messaging
- o Integrity mode
- o Confidentiality mode
- o Integrity and confidentiality mode

SF.APP_INTEGRITY

This security functionality monitors the integrity of sensitive user data and the integrity of the DTBS/R. The integrity of persistently stored data such as SCD, RAD and SVD is monitored using the platform features **[PTF-ST]**. In case of integrity error this TSF will:

- o Prohibit the use of the altered data, and
- o Inform the S.Signatory about integrity error. This TSF also monitors the integrity of the access conditions of created data objects and also ensures that no residual information is available after a RAD update or clearance.

SF.RATIF

A counter is associated to a secret key, to a password and to the VAD, which is used to count the number of successive unsuccessful authentication attempts. The counter is

reinitialised when the authentication is successful. If the counter reaches its maximum value, then the related secret is suspended or blocked and cannot be used anymore.

SF.ESERVICE

This security function enables to perform electronic services. It is active in phase 7. This security function offers the following electronic services:

- o C/S authentication
- o Decryption key decipherment
- o Certificate verification
- o Symmetric encryption and decryption

SF.ADM_AUTH

This security function manages the authentication of external entities by the TOE. It is active in phase 6 and 7. This security function enables the TOE to authenticate external entities and may be either realized using symmetric or asymmetric cryptography. This security function manages as well the validation process of the role associated to the authentication key used by the external entity. Upon successful authentication, the associated role is authenticated and can proceed to switch from Phase 6 to Phase 7 for example. Each key is associated to an error counter (it may be infinite) which aims at ensuring its protecting against brute force attacks. Upon each wrong authentication, it decrements the error counter (if present), and restores it to its maximum value upon a successful authentication. When the error counter has reached '00', the security function blocks the usage of the key, and bans the authentication of the associated role. This security function allows the authentication of the following roles:

- o TOE_Administrator
- o User_Admin

9.2 SFRs and TSS

9.2.1 SFRs and TSS - Rationale

All SSCD parts

Protection of the TSF (FPT)

FPT_EMS.1 is met by SF.APP_INTEGRITY and SF.MANAGEMENT which ensure secure execution of cryptographic operations on keys.

FPT_FLS.1 is met by JC Platform and the IC that ensure that failures in the TSF are detected and that the proper actions (reset, card termination) are taken in order to preserve a secure state of the TOE. It is also met by SF.APP_INTEGRITY that monitors the integrity of sensitive user data and the integrity of the DTBS/R.

FPT_PHP.1 is met by SF.APP_INTEGRITY, the JC Platform and the IC that ensure that physical tampering of the TOE is detected and that the proper actions (reset, card termination) are taken, so that it can be determined if a physical tampering has occurred.

FPT_PHP.3 is met by the JC Platform and the IC that ensures that physical tampering of the TOE is detected and that the proper actions (reset, card termination) are taken in order to protect the TOE. It is also met by SF.APP_INTEGRITY that monitors the integrity of sensitive data.

FPT_TST.1 is met by JC Platform and the IC that performs a set of self-tests at start-up, thus checking the correct operation of the TSF, and that verifies the integrity of the stored executable code before or during its execution and by SF.APP_INTEGRITY that provides means to verify the integrity of the data stored on the TOE.

Security management (FMT)

FMT_SMR.1 is met by SF.AUTHENTICATION that provides user authentication as administrator or as signatory and by SF.MANAGEMENT that grants to the administrator and to the signatory specific access rights, thus defining roles for the TOE.

FMT_SMF.1 requires that the TSF shall be capable of performing the following management functions: (1) Creation and modification of the reference authentication data (RAD), (2) Enabling the signature-creation function, (3) Modification of the security attribute SCD/SVD management, SCD operational, (4) Change the default value of the security attribute SCD Identifier, (5) none. This is realized by SF.MANAGEMENT.

FMT_MOF.1 is met by SF.MANAGEMENT and SF.AUTHENTICATION that ensures that only authenticated signatory can perform DTBS signature.

FMT_MSA.1/Admin is met by SF.AUTHENTICATION and SF.MANAGEMENT that manage the access right policy of the TOE.

FMT_MSA.1/Signatory is met by SF.AUTHENTICATION and SF.MANAGEMENT that manage the access right policy of the TOE.

FMT_MSA.2 is met by SF.AUTHENTICATION and SF.MANAGEMENT that manage the access right policy of the TOE and in particular manages the security attributes.

FMT_MSA.3 is met by SF.AUTHENTICATION and SF.MANAGEMENT that manage the access right policy of the TOE and in particular manage the security attributes, their initialisation and their access rights.

FMT_MSA.4 requires that the TSF shall use the following rules to set the value of security attributes: (1) if S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute 'SCD operational of the SCD' shall be set to 'no' as a single operation; (2) if S.Sigy successfully generates an SCD/SVD pair the security attribute 'SCD operational of the SCD' shall be set to 'yes' as a single operation. This is realized by SF.MANAGEMENT and SF.AUTHENTICATION.

FMT_MTD.1/Admin

- o is met by SF.MANAGEMENT that manages the authentication function and ensure that only authenticated administrator can create the RAD.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

FMT_MTD.1/Signatory

- o is met by SF.MANAGEMENT that manages the authentication function and ensure that only authenticated signatory can modify the RAD.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

Identification and authentication (FIA)

FIA_UID.1

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.

FIA_AFL.1

- o This SFR is met by SF.AUTHENTICATION and SF.MANAGEMENT.
- o This SFR is also met by SF.RATIF that ensures that the RAD is blocked after a defined number of failed successive signatory authentication attempts.

FIA_UAU.1

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.
- o is met by SF.TRUSTED_CHANNEL that provides a trusted secure messaging with CGA and SCA.

User data protection (FDP)

FDP_SDI.2/DTBS is met by SF.APP_INTEGRITY, that ensures the integrity of data stored in the TOE, by the JC Platform and the IC that ensure that the proper reaction is taken (reset or card termination) if an integrity error is detected, so that the user knows an error had occurred and that no altered data can be used.

FDP_SDI.2/Persistent is met by SF.APP_INTEGRITY, that ensures the integrity of data stored in the TOE, by the JC Platform and the IC that ensure that the proper reaction is taken (reset or card termination) if an integrity error is detected, so that the user knows an error had occurred and that no altered data can be used.

FDP_RIP.1 is met by SF.MANAGEMENT that ensures erasure of data in FLASH and in RAM (e.g. after the signature creation process), and in particular of SCD, VAD and RAD.

FDP_ACC.1/Signature_Creation is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that all the access conditions are met before a dedicated operation can be performed, and in particular that only a user authenticated as signatory can perform signature of DTBS loading from an authorized SCA with a RSA key pair whose consistency has been verified, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACF.1/Signature_Creation is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that all the access conditions are met before a dedicated operation can be performed, and in particular that only a user authenticated as signatory can perform signature of DTBS loading from an authorized SCA with a RSA key pair whose consistency has been verified, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

Cryptographic support (FCS)

FCS_COP.1

- o is met by SF.APP_CRYPTO that provides RSA key pair consistency check.
- o is met by SF.APP_CRYPTO that provides electronic signature generation compliant with RSA PKCS#1 v2.1.
- o is met by SF.APP_CRYPTO that provides TDES in CBC mode or AES in CBC mode for encryption and decryption.
- o is met by SF.APP_CRYPTO that provides ISO/IEC 9797-1 algorithm 3 padding 2 (3DES) or CMAC (AES) for integrity.
- o is met by SF.AUTHENTICATION that provides Symmetric and Asymmetric Mutual Authentications.
- o is met by SF.TRUSTED_CHANNEL that provides secure messaging with CGA and SCA.
- o is met by SF.APP_CRYPTO that provides Data Hashing.
- o is met by SF.APP_CRYPTO that provides signature verification.
- o is met by SF.AUTHENTICATION that provides PACE authentication, and
- o is met by SF.APP_CRYPTO that provides TDES in CBC mode or AES in CBC mode for encryption and decryption.
- o is met by SF.TRUSTED_CHANNEL that provides secure messaging with CGA and SCA.
- o is met by SF.AUTHENTICATION that provides PACE authentication, and
- o is met by SF.APP_CRYPTO that provides TDES in CBC mode or AES in CBC mode for MAC calculation.
- o is met by SF.TRUSTED_CHANNEL that provides secure messaging with CGA and SCA.

FCS_CKM.6 is met by SF.MANAGEMENT, as SF.MANAGEMENT manages the secure destruction of secret, and in particular of the SCD.

SSCD parts 2, 4 and 5 only

Cryptographic support (FCS)

FCS_CKM.1

- o is met by SF.APP_CRYPTO that ensures that the TOE generates SCD/SVD cryptographic key pairs.
- o is also met by SF.APP_CRYPTO, which provides RSA calculation.
- o is also met by SF.MANAGEMENT, which ensures the protection of the keys during generation.

User data protection (FDP)

FDP_ACC.1/SVD_Transfer is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SVD export, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACF.1/SVD_Transfer is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SVD export, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACC.1/SCD/SVD_Generation is met by SF.MANAGEMENT, SF.AUTHENTICATION 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 can perform SCD/SVD generation, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACF.1/SCD/SVD_Generation is met by SF.MANAGEMENT, SF.AUTHENTICATION 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 can perform SCD/SVD generation, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

SSCD parts 3 and 6 only

Trusted path/channels (FTP)

FTP_ITC.1/SCD is met by SF.AUTHENTICATION and SF.MANAGEMENT that enforce the access right policy for SCD Import and by SF.TRUSTED_CHANNEL, SF.APP_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a CSP to protect the exchanged data (SCD) from modification and disclosure.

User data protection (FDP)

FDP_UCT.1/SCD is met by SF.AUTHENTICATION and SF.MANAGEMENT that ensure that all the conditions are met before allowing a SCD import and by SF.TRUSTED_CHANNEL, SF.APP_CRYPTO that provide cryptographic means to protect the SCD from disclosure during its import.

FDP_ITC.1/SCD is met by SF.AUTHENTICATION and SF.MANAGEMENT that ensure that all the required conditions are met before allowing a SCD import operation.

FDP_ACC.1/SCD_Import is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SCD import, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACF.1/SCD_Import is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SCD import, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

SSCD part 4 only*Trusted path/channels (FTP)*

FTP_ITC.1/SVD is met by SF.AUTHENTICATION and SF.MANAGEMENT that enforce the access right policy for SVD Transfer and by SF.TRUSTED_CHANNEL, SF.APP_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a CGA to protect the exchanged data (SVD) from modification and disclosure.

User data protection (FDP)

FDP_DAU.2/SVD is met by SF.AUTHENTICATION and SF.TRUSTED_CHANNEL to ensure that exported SVD to the CGA is authenticated and unmodified.

*Identification and authentication (FIA)***FIA_API.1**

- o The TOE supports RSA calculations in order to generate signatures (SF.APP_CRYPTO).
- o The TOE supports the establishment of a trusted channel/path based on 3DES or AES mutual authentication with negotiation of symmetric cryptographic keys used for the protection of the communication data with respect to confidentiality and integrity (SF.TRUSTED_CHANNEL, SF.APP_CRYPTO).

SSCD parts 5 and 6 only*User data protection (FDP)*

FDP_UIT.1/DTBS requires that integrity of the DTBS/R to be signed is to be verified, as well as the DTBS/R is not altered by the TOE. This is provided by the trusted channel integrity verification mechanisms (SF.TRUSTED_CHANNEL, SF.APP_CRYPTO).

Trusted path/channels (FTP)

FTP_ITC.1/VAD is met by SF.AUTHENTICATION, SF.MANAGEMENT that enforce the access right policy for VAD transfer and by SF.TRUSTED_CHANNEL, SF.APP_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a HID to protect the exchanged data (VAD) from modification and disclosure.

FTP_ITC.1/DTBS is met by SF.AUTHENTICATION and SF.MANAGEMENT that enforce the access right policy for DTBS Import and by SF.TRUSTED_CHANNEL, SF.APP_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a SCA to protect the exchanged data (DTBS) from modification and disclosure.

Additional SFRs**FCS_RND.1**

- o is met by SF.APP_CRYPTO and SF.AUTHENTICATION.

FCS_CKM.1/DH_PACE

- o is met by SF.APP_CRYPTO that ensures that the TOE generates SCD/SVD cryptographic key pairs for PACE.
- o is also met by SF.APP_CRYPTO, which provides DH calculation.
- o is also met by SF.MANAGEMENT, which ensures the protection of the keys during generation.

FIA_UID.1/PACE

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.

FIA_UAU.1/PACE

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.
- o is met by SF.TRUSTED_CHANNEL that provides a trusted secure messaging with CGA and SCA.

FIA_UAU.4/PACE

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.
- o is met by SF.TRUSTED_CHANNEL that provides a trusted secure messaging with CGA and SCA.

FIA_UAU.5/PACE

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.
- o is met by SF.TRUSTED_CHANNEL that provides a trusted secure messaging with CGA and SCA.

FIA_UAU.6/PACE

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.
- o is met by SF.TRUSTED_CHANNEL that provides a trusted secure messaging with CGA and SCA.

FIA_UAU.6/CA

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.
- o is met by SF.TRUSTED_CHANNEL that provides a trusted secure messaging with CGA and SCA.

FIA_AFL.1/PACE

- o This SFR is met by SF.AUTHENTICATION and SF.MANAGEMENT.
- o This SFR is also met by SF.RATIF that ensures that the PIN or PUK is suspended after a defined number of failed successive signatory PACE authentication attempts.
- o This SFR is also met by SF.RATIF that ensures that the PIN or PUK is blocked after a defined number of failed successive signatory PACE authentication attempts.
- o This SFR is also met by SF.RATIF that ensures that the PIN, PUK or CAN is suspended until the next successful authentication attempt by an configurable amount of time after a defined number of failed signatory PACE authentication attempts.

FIA_API.1/CA

- o The TOE supports the establishment of a trusted channel/path based on 3DES or AES mutual authentication with negotiation of cryptographic keys used for the protection of the communication data with respect to confidentiality and integrity (SF.TRUSTED_CHANNEL, SF.APP_CRYPTO).

FDP_ACC.1/TRM

- o is met by SF.MANAGEMENT, SF.AUTHENTICATION 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, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACF.1/TRM

- o is met by SF.MANAGEMENT, SF.AUTHENTICATION 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, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FDP_UCT.1/TRM

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that ensure that all the conditions are met before allowing user data transmission and by SF.TRUSTED_CHANNEL, SF.APP_CRYPTO that provide cryptographic means to protect user data from disclosure during its import.

FDP_UIT.1/TRM requires that integrity of user data to be authenticated. This is provided by the trusted channel integrity verification mechanisms (SF.TRUSTED_CHANNEL, SF.APP_CRYPTO).

FTP_ITC.1/PACE

- o is met is met by SF.AUTHENTICATION and SF.MANAGEMENT that enforce the access right policy for data exchange between the TOE and a PACE terminal and by SF.TRUSTED_CHANNEL, SF.APP_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a PACE terminal to protect the exchanged data from modification and disclosure.

FMT_SMR.1/PACE

- o is met by SF.AUTHENTICATION that provides user authentication for PACE and by SF.MANAGEMENT that grants to the users specific access rights, thus defining roles for the TOE.

FMT_MTD.1/CVCA_INI

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated personalisation agent can write initial CVCA (public key, meta-data of the certificate, current date).
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

FMT_MTD.1/CVCA_UPD

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated Country Verifying Certification Authority can update CVCA (public key, meta-data of the certificate).
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

FMT_MTD.1/DATE

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated users (Country Verifying Certification Authority, Document Verifier or EAC2 terminal) can modify the current date of CVCA.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

FMT_MTD.1/PA

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated personalisation agent can write SOC and SOD selected in Access Control SFP.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

FMT_MTD.1/SK_PICC

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated personalisation agent can load SKPICC selected in Access Control SFP.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

FMT_MTD.1/KEY_READ

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that none can read PACE passwords and SKPICC.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

FMT_MTD.1/Initialize_PIN

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated authenticated personalisation agent can write PIN, PUK and CAN, selected in Access Control SFP.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

FMT_MTD.1/Resume_PIN

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated electronic document holder can resume suspended PIN selected in Access Control SFP.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

FMT_MTD.1/Change_PIN

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated users (electronic document holder or an authorized terminal) can change blocked PIN selected in Access Control SFP.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

FMT_MTD.1/Unblock_PIN

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated users (electronic document holder or an authorized terminal) can unblock blocked PIN selected in Access Control SFP.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

FMT_MTD.1/TOE State is met by SF.ADM_AUTH that manages the authentication function and ensures that only authenticated by GP authentication in phase 6 (personaliser) can switch the life cycle. This last operation is ensued by the SF.MANAGEMENT.

FMT_MTD.3

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only secure values are accepted for TSF data of the Terminal Authentication protocol 2 and the Access Control SFP.

FMT_MTD.1/INI_ENA

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated Manufacturer can write Initialisation Data and Pre-personalisation Data.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

FMT_MTD.1/INI_DIS

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated Personalisation Agent can read out Initialisation Data and Pre-personalisation Data.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

FTP_ITC.1/CA2

- o is met is met by SF.AUTHENTICATION and SF.MANAGEMENT that enforce the access right policy for data exchange between the TOE and an EAC2 terminal and by SF.TRUSTED_CHANNEL, SF.APP_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and an EAC2 terminal to protect the exchanged data from modification and disclosure.

FMT_LIM.1

- o is met by SF.MANAGEMENT and SF.AUTHENTICATION.

FMT_LIM.2

- o is met by SF.MANAGEMENT and SF.AUTHENTICATION.

9.2.2 Association tables of SFRs and TSS

Security Functional Requirements	TOE Summary Specification
FPT_EMS.1	SF.APP_INTEGRITY , SF.MANAGEMENT
FPT_FLS.1	SF.APP_INTEGRITY
FPT_PHP.1	SF.APP_INTEGRITY
FPT_PHP.3	SF.APP_INTEGRITY
FPT_TST.1	SF.APP_INTEGRITY
FMT_SMR.1	SF.AUTHENTICATION , SF.MANAGEMENT
FMT_SMF.1	SF.MANAGEMENT
FMT_MOF.1	SF.MANAGEMENT , SF.AUTHENTICATION
FMT_MSA.1/Admin	SF.MANAGEMENT , SF.AUTHENTICATION
FMT_MSA.1/Signatory	SF.MANAGEMENT , SF.AUTHENTICATION
FMT_MSA.2	SF.MANAGEMENT , SF.AUTHENTICATION
FMT_MSA.3	SF.MANAGEMENT , SF.AUTHENTICATION
FMT_MSA.4	SF.MANAGEMENT , SF.AUTHENTICATION
FMT_MTD.1/Admin	SF.MANAGEMENT , SF.AUTHENTICATION
FMT_MTD.1/Signatory	SF.MANAGEMENT , SF.AUTHENTICATION
FIA_UID.1	SF.AUTHENTICATION , SF.MANAGEMENT
FIA_AFL.1	SF.MANAGEMENT , SF.AUTHENTICATION , SF.RATIF
FIA_UAU.1	SF.AUTHENTICATION , SF.MANAGEMENT , SF.TRUSTED_CHANNEL
FDP_SDI.2/DTBS	SF.APP_INTEGRITY
FDP_SDI.2/Persistent	SF.APP_INTEGRITY
FDP_RIP.1	SF.MANAGEMENT
FDP_ACC.1/Signature Creation	SF.MANAGEMENT , SF.AUTHENTICATION
FDP_ACF.1/Signature Creation	SF.MANAGEMENT , SF.AUTHENTICATION
FCS_COP.1	SF.APP_CRYPTO , SF.AUTHENTICATION , SF.TRUSTED_CHANNEL
FCS_CKM.6	SF.MANAGEMENT
FCS_CKM.1	SF.APP_CRYPTO , SF.MANAGEMENT

Security Functional Requirements	TOE Summary Specification
<u>FDP_ACC.1/SVD Transfer</u>	<u>SF.MANAGEMENT</u> , <u>SF.AUTHENTICATION</u>
<u>FDP_ACF.1/SVD Transfer</u>	<u>SF.MANAGEMENT</u> , <u>SF.AUTHENTICATION</u>
<u>FDP_ACC.1/SCD/SVD Generation</u>	<u>SF.MANAGEMENT</u> , <u>SF.AUTHENTICATION</u>
<u>FDP_ACF.1/SCD/SVD Generation</u>	<u>SF.MANAGEMENT</u> , <u>SF.AUTHENTICATION</u>
<u>FTP_ITC.1/SCD</u>	<u>SF.MANAGEMENT</u> , <u>SF.APP_CRYPTO</u> , <u>SF.TRUSTED_CHANNEL</u> , <u>SF.AUTHENTICATION</u>
<u>FDP_UCT.1/SCD</u>	<u>SF.TRUSTED_CHANNEL</u> , <u>SF.APP_CRYPTO</u> , <u>SF.AUTHENTICATION</u> , <u>SF.MANAGEMENT</u>
<u>FDP_ITC.1/SCD</u>	<u>SF.MANAGEMENT</u> , <u>SF.AUTHENTICATION</u>
<u>FDP_ACC.1/SCD Import</u>	<u>SF.MANAGEMENT</u> , <u>SF.AUTHENTICATION</u>
<u>FDP_ACF.1/SCD Import</u>	<u>SF.MANAGEMENT</u> , <u>SF.AUTHENTICATION</u>
<u>FTP_ITC.1/SVD</u>	<u>SF.MANAGEMENT</u> , <u>SF.TRUSTED_CHANNEL</u> , <u>SF.APP_CRYPTO</u> , <u>SF.AUTHENTICATION</u>
<u>FDP_DAU.2/SVD</u>	<u>SF.AUTHENTICATION</u> , <u>SF.TRUSTED_CHANNEL</u>
<u>FIA_API.1</u>	<u>SF.APP_INTEGRITY</u> , <u>SF.TRUSTED_CHANNEL</u>
<u>FDP_UIT.1/DTBS</u>	<u>SF.TRUSTED_CHANNEL</u> , <u>SF.APP_CRYPTO</u>
<u>FTP_ITC.1/VAD</u>	<u>SF.TRUSTED_CHANNEL</u> , <u>SF.APP_CRYPTO</u> , <u>SF.AUTHENTICATION</u> , <u>SF.MANAGEMENT</u>
<u>FTP_ITC.1/DTBS</u>	<u>SF.TRUSTED_CHANNEL</u> , <u>SF.APP_CRYPTO</u> , <u>SF.MANAGEMENT</u> , <u>SF.AUTHENTICATION</u>
<u>FCS_RND.1</u>	<u>SF.APP_CRYPTO</u> , <u>SF.AUTHENTICATION</u>
<u>FCS_CKM.1/DH PACE</u>	<u>SF.APP_CRYPTO</u> , <u>SF.MANAGEMENT</u> , <u>SF.ESERVICE</u>
<u>FIA_UID.1/PACE</u>	<u>SF.AUTHENTICATION</u> , <u>SF.MANAGEMENT</u>
<u>FIA_UAU.1/PACE</u>	<u>SF.AUTHENTICATION</u> , <u>SF.MANAGEMENT</u> , <u>SF.TRUSTED_CHANNEL</u>
<u>FIA_UAU.4/PACE</u>	<u>SF.AUTHENTICATION</u> , <u>SF.MANAGEMENT</u> , <u>SF.TRUSTED_CHANNEL</u>
<u>FIA_UAU.5/PACE</u>	<u>SF.AUTHENTICATION</u> , <u>SF.MANAGEMENT</u> , <u>SF.TRUSTED_CHANNEL</u>
<u>FIA_UAU.6/PACE</u>	<u>SF.AUTHENTICATION</u> , <u>SF.MANAGEMENT</u> , <u>SF.TRUSTED_CHANNEL</u>
<u>FIA_UAU.6/CA</u>	<u>SF.AUTHENTICATION</u> , <u>SF.MANAGEMENT</u> , <u>SF.TRUSTED_CHANNEL</u>
<u>FIA_AFL.1/PACE</u>	<u>SF.AUTHENTICATION</u> , <u>SF.MANAGEMENT</u> , <u>SF.RATIF</u>
<u>FIA_API.1/CA</u>	<u>SF.TRUSTED_CHANNEL</u> , <u>SF.APP_CRYPTO</u>

Security Functional Requirements	TOE Summary Specification
FDP_ACC.1/TRM	SF.AUTHENTICATION , SF.MANAGEMENT
FDP_ACF.1/TRM	SF.AUTHENTICATION , SF.MANAGEMENT
FDP_UCT.1/TRM	SF.TRUSTED_CHANNEL , SF.AUTHENTICATION , SF.APP_CRYPTO , SF.MANAGEMENT
FDP_UIT.1/TRM	SF.TRUSTED_CHANNEL , SF.APP_CRYPTO
FTP_ITC.1/PACE	SF.MANAGEMENT , SF.APP_CRYPTO , SF.TRUSTED_CHANNEL , SF.AUTHENTICATION
FMT_SMR.1/PACE	SF.AUTHENTICATION , SF.MANAGEMENT
FMT_MTD.1/CVCA_INI	SF.AUTHENTICATION , SF.MANAGEMENT
FMT_MTD.1/CVCA_UPD	SF.AUTHENTICATION , SF.MANAGEMENT
FMT_MTD.1/DATE	SF.AUTHENTICATION , SF.MANAGEMENT
FMT_MTD.1/PA	SF.AUTHENTICATION , SF.MANAGEMENT
FMT_MTD.1/SK_PICC	SF.AUTHENTICATION , SF.MANAGEMENT
FMT_MTD.1/KEY_READ	SF.AUTHENTICATION , SF.MANAGEMENT
FMT_MTD.1/Initialize_PIN	SF.AUTHENTICATION , SF.MANAGEMENT
FMT_MTD.1/Resume_PIN	SF.AUTHENTICATION , SF.MANAGEMENT
FMT_MTD.1/Change_PIN	SF.AUTHENTICATION , SF.MANAGEMENT
FMT_MTD.1/Unblock_PIN	SF.AUTHENTICATION , SF.MANAGEMENT
FMT_MTD.1/TOE State	SF.MANAGEMENT , SF.ADM_AUTH
FMT_MTD.3	SF.AUTHENTICATION
FMT_MTD.1/INI_ENA	SF.MANAGEMENT , SF.AUTHENTICATION
FMT_MTD.1/INI_DIS	SF.AUTHENTICATION , SF.MANAGEMENT
FTP_ITC.1/CA2	SF.MANAGEMENT , SF.APP_CRYPTO , SF.TRUSTED_CHANNEL , SF.AUTHENTICATION
FMT_LIM.1	SF.MANAGEMENT , SF.AUTHENTICATION
FMT_LIM.2	SF.MANAGEMENT , SF.AUTHENTICATION

Table 27 SFRs and TSS - Coverage

TOE Summary Specification	Security Functional Requirements
SF.AUTHENTICATION	FCS_RND.1 , FIA_UID.1/PACE , FIA_UAU.1/PACE , FIA_UAU.4/PACE , FIA_UAU.5/PACE , FIA_UAU.6/PACE , FIA_UAU.6/CA , FIA_AFL.1/PACE , FDP_ACC.1/TRM , FDP_ACF.1/TRM , FDP_UCT.1/TRM , FTP_ITC.1/PACE , FMT_SMR.1/PACE , FMT_MTD.1/CVCA_INI , FMT_MTD.1/CVCA_UPD , FMT_MTD.1/DATE , FMT_MTD.1/PA ,

TOE Summary Specification	Security Functional Requirements
	FMT MTD.1/SK PICC, FMT MTD.1/KEY READ, FMT MTD.1/Initialize PIN, FMT MTD.1/Resume PIN, FMT MTD.1/Change PIN, FMT MTD.1/Unblock PIN, FMT MTD.3, FMT MTD.1/INI ENA, FMT MTD.1/INI DIS, FTP ITC.1/CA2, FMT LIM.1, FMT LIM.2, FMT SMR.1, 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, FIA UID.1, FIA AFL.1, FIA UAU.1, FDP ACC.1/Signature Creation, FDP ACF.1/Signature Creation, FCS COP.1, FDP ACC.1/SVD Transfer, FDP ACF.1/SVD Transfer, FDP ACC.1/SCD/SVD Generation, FDP ACF.1/SCD/SVD Generation, FTP ITC.1/SCD, FDP UCT.1/SCD, FDP ITC.1/SCD, FDP ACC.1/SCD Import, FDP ACF.1/SCD Import, FTP ITC.1/SVD, FDP DAU.2/SVD, FTP ITC.1/VAD, FTP ITC.1/DTBS
SF.APP CRYPTO	FCS RND.1, FCS CKM.1/DH PACE, FIA API.1/CA, FDP UCT.1/TRM, FDP UIT.1/TRM, FTP ITC.1/PACE, FTP ITC.1/CA2, FCS COP.1, FCS CKM.1, FTP ITC.1/SCD, FDP UCT.1/SCD, FTP ITC.1/SVD, FDP UIT.1/DTBS, FTP ITC.1/VAD, FTP ITC.1/DTBS
SF.MANAGEMENT	FCS CKM.1/DH PACE, FIA UID.1/PACE, FIA UAU.1/PACE, FIA UAU.4/PACE, FIA UAU.5/PACE, FIA UAU.6/PACE, FIA UAU.6/CA, FIA AFL.1/PACE, FDP ACC.1/TRM, FDP ACF.1/TRM, FDP UCT.1/TRM, FTP ITC.1/PACE, FMT SMR.1/PACE, FMT MTD.1/CVCA INI, FMT MTD.1/CVCA UPD, FMT MTD.1/DATE, FMT MTD.1/PA, FMT MTD.1/SK PICC, FMT MTD.1/KEY READ, FMT MTD.1/Initialize PIN, FMT MTD.1/Resume PIN, FMT MTD.1/Change PIN, FMT MTD.1/Unblock PIN, FMT MTD.1/TOE State, FMT MTD.1/INI ENA, FMT MTD.1/INI DIS, FTP ITC.1/CA2, FMT LIM.1, FMT LIM.2, FPT EMS.1, FMT SMR.1, FMT SMF.1, FMT MOF.1, FMT MSA.1/Admin, FMT MSA.1/Signatory, FMT MSA.2, FMT MSA.3, FMT MSA.4,

TOE Summary Specification	Security Functional Requirements
	FMT_MTD.1/Admin , FMT_MTD.1/Signatory , FIA_UID.1 , FIA_AFL.1 , FIA_UAU.1 , FDP_RIP.1 , FDP_ACC.1/Signature Creation , FDP_ACF.1/Signature Creation , FCS_CKM.6 , FCS_CKM.1 , FDP_ACC.1/SVD Transfer , FDP_ACF.1/SVD Transfer , FDP_ACC.1/SCD/SVD Generation , FDP_ACF.1/SCD/SVD Generation , FTP_ITC.1/SCD , FDP_UCT.1/SCD , FDP_ITC.1/SCD , FDP_ACC.1/SCD Import , FDP_ACF.1/SCD Import , FTP_ITC.1/SVD , FTP_ITC.1/VAD , FTP_ITC.1/DTBS
SF.TRUSTED_CHANNEL	FIA_UAU.1/PACE , FIA_UAU.4/PACE , FIA_UAU.5/PACE , FIA_UAU.6/PACE , FIA_UAU.6/CA , FIA_API.1/CA , FDP_UCT.1/TRM , FDP_UIT.1/TRM , FTP_ITC.1/PACE , FTP_ITC.1/CA2 , FIA_UAU.1 , FCS_COP.1 , FTP_ITC.1/SCD , FDP_UCT.1/SCD , FTP_ITC.1/SVD , FDP_DAU.2/SVD , FIA_API.1 , FDP_UIT.1/DTBS , FTP_ITC.1/VAD , FTP_ITC.1/DTBS
SF.APP_INTEGRITY	FPT_EMS.1 , FPT_FLS.1 , FPT_PHP.1 , FPT_PHP.3 , FPT_TST.1 , FDP_SDI.2/DTBS , FDP_SDI.2/Persistent , FIA_API.1
SF.RATIF	FIA_AFL.1/PACE , FIA_AFL.1
SF.ESERVICE	FCS_CKM.1/DH PACE
SF.ADM_AUTH	FMT_MTD.1/TOE State

Table 28 TSS and SFRs - Coverage

