IDEMIA

TnD v5.1 on ID-One Cosmo X (BAC Configuration)

Public Security Target

Reference: FQR 550 0431 Ed 1

DOCUMENT EVOLUTION

Date	Version	Author	Revision
04/04/2023	Ed 1	IDEMIA	Sanitized version created for Public Issue.

Table of contents

1.1 ST IDENTIFICATION 7
1.2 TOE REFERENCE 7
2.1 TECHNICAL TERMS 9
2.2 ABBREVIATIONS 22
2.3 REFERENCES 24
3.1 TOE OVERVIEW 26
3.2 TOE DESCRIPTION 27
3.2.1 Physical scope 27
3.2.2 Logical Scope 28
3.3 REQUIRED NON-TOE HARDWARE/SOFTWARE/FIRMWARE 31
3.4 TOE USAGE AND SECURITY FEATURES FOR OPERATIONAL USE 31
3.4.1 TOE Usage 31
3.4.2 Security Features 33
4.1 DEVELOPMENT ENVIRONMENT 35
4.2 PRODUCTION ENVIRONMENT 36
4.3 PREPARATION ENVIRONMENT 46
4.4 OPERATIONAL ENVIRONMENT 46
5.1 CC CONFORMANCE CLAIM 47
5.2 PP CLAIM 47
5.3 PACKAGE CLAIM 47
5.4 PP CONFORMANCE RATIONALE 47
5.4.1 Main aspects 48
5.4.2 Overview of differences between the PP and the ST 48
6.1 ASSETS 50
6.1.1 Logical MRTD data 50
6.1.2 Miscellaneous 51
6.2 USERS / SUBJECTS 51
6.2.1 IC manufacturer 52
6.2.2 MRTD packaging responsible 52
6.2.3 Embedded software loading responsible 52
6.2.4 Pre-personalization Agent 52
6.2.5 Personalization Agent 52
6.2.6 Terminal 52
6.2.7 Inspection system (IS) 52
6.2.8 MRTD Holder 53
6.2.9 Traveler 53
6.2.10 Attacker 53
6.3 THREATS 53
6.3.1 Threats from PP BAC 53
6.3.2 Additional Threat 55
6.4 ORGANISATIONAL SECURITY POLICIES 56
6.4.1 P.Manufact 56
6.4.2 P.Personalization 56
6.4.3 P.Personal_Data 56
6.5 ASSUMPTIONS 56
6.5.1 Assumptions from PP BAC 56
6.5.2 Additional Assumptions 57
7.1 SECURITY OBJECTIVES FOR THE TOE 59
7.1.1 Security Objectives listed in PP BAC 59
7.1.2 Additional Security Objectives for the TOE 60

7.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 61
7.2.1 Issuing State or Organization 61
7.2.2 Receiving State or Organization 62
7.2.3 Additional Security Objectives for the Operational Environment 63
7.3 SECURITY OBJECTIVES RATIONALE 63
7.3.1 Threats 63
7.3.2 Organisational Security Policies 65
7.3.3 Assumptions 65
7.3.4 SPD and Security Objectives 66
8.1 EXTENDED FAMILIES 70
8.1.1 Extended Family FPT_EMS - TOE Emanation 70
8.1.2 Extended Family FIA_API - Authentication Proof of Identity 70
8.1.3 Extended Family FMT_LIM - Limited capabilities 71
8.1.4 Extended Family FAU_SAS - Audit data storage 72
8.1.5 Extended Family FCS_RND - Generation of random numbers 72
9.1 SECURITY FUNCTIONAL REQUIREMENTS 74
9.1.1 Class FAU Security Audit 74
9.1.2 Class FCS Cryptographic Support 74
9.1.3 Class FIA Identification and Authentication 77
9.1.4 Class FDP User Data Protection 79
9.1.5 Class FMT Security Management 82
9.1.6 Class FPT Protection of the Security Functions 84
9.2 SECURITY ASSURANCE REQUIREMENTS 86
9.2.1 ADV Development 86
9.2.2 AGD Guidance documents 90
9.2.3 ALC Life-cycle support 92
9.2.4 ASE Security Target evaluation 96
9.2.5 ATE Tests 101
9.2.6 AVA Vulnerability assessment 102
9.3 SECURITY REQUIREMENTS RATIONALE 104
9.3.1 Objectives 104
9.3.2 Rationale tables of Security Objectives and SFRs 107
9.3.3 Dependencies 110
9.3.4 Rationale for the Security Assurance Requirements 114
9.3.5 ADV_FSP.5 Complete semi-formal functional specification with additional error information 114
9.3.6 ADV_INT.2 Well-structured internals 114
9.3.7 ADV_TDS.4 Semiformal modular design 114
9.3.8 ALC_CMS.5 Development tools CM coverage 115
9.3.9 ALC_DVS.2 Sufficiency of security measures 115
9.3.10 ALC_TAT.2 Compliance with implementation standards 115
9.3.11 ATE_DPT.3 Testing: modular design 115
10.1 TOE SUMMARY SPECIFICATION 116
10.2 SFRS AND TSS 119
10.2.1 SFRs and TSS - Rationale 119
10.2.2 Association tables of SFRs and TSS 122

Table of figures

Figure 1 Physical Form 28
Figure 2 Logical Scope of the TOE.....29
Figure 3 Life cycle Overview 35

Table of tables

Table 1 TOE Configurations 8
Table 2 Applet Internal Versions 8
Table 3 Different evaluated configurations of the TnD application 27
Table 4 TOE physical ports and interfaces 28
Table 5 TOE Guidance 30
Table 6 TOE Configurations during Personalization 31
Table 7 eMRTD and IDL Terminology 31
Table 8 BAC Configuration 33
Table 9 Option 1: Both Platform and Applet packages are loaded at IC Manufacturer Site 37
Table 10 Option 2: Both Platform and Applet packages are loaded at CC Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites 38
Table 11 Option 3(a): Platform package is loaded at IC Manufacturer Site and Applet package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites through GP Mechanism 39
Table 12 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 Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites 40
Table 13 Option 3(c): Platform package is loaded at IC Manufacturer Site and Applet package in plain format is loaded at Audited IDEMIA Sites only 41
Table 14 Option 4(a): Platform package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites and Applet package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites through GP Mechanism 42
Table 15 Platform package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites and Options 4b(i) Applet package is loaded through Resident application using LSK format and and 4b(ii) DUMP Package is loaded through resident application using DSK Secret Live Key - at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites 44
Table 16 Option 4(c): Platform package is loaded at IC Manufacturer Site and Applet package in plain format is loaded at CC Audited IDEMIA Sites only 45
Table 17 Threats and Security Objectives - Coverage 66
Table 18 Security Objectives and Threats - Coverage 67
Table 19 OSPs and Security Objectives - Coverage 67
Table 20 Security Objectives and OSPs - Coverage 68
Table 21 Assumptions and Security Objectives for the Operational Environment - Coverage 68
Table 22 Security Objectives for the Operational Environment and Assumptions - Coverage 69
Table 23 Security Objectives and SFRs - Coverage 108
Table 24 SFRs and Security Objectives 109
Table 25 SFRs Dependencies 112
Table 26 SARs Dependencies 114
Table 27 SFRs and TSS - Coverage 123
Table 28 TSS and SFRs - Coverage 124

1 ST Introduction

1.1 ST Identification

Title	TnD v5.1 on ID-One Cosmo X (BAC Configuration) Public Security Target
ST Identification	FQR 550 0431 Ed 1
CC Version	3.1 Revision 5
Assurance Level	EAL4 augmented with ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_DVS.2, ALC_CMS.5, ALC_TAT.2 and ATE_DPT.3
ITSEF	Brightsight
Certification Body	NSCIB
Compliant to Protection Profiles	Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control, BSI-CC-PP-0055-2009, Version 1.10, 25th March 2009 [BAC-PP]

1.2 TOE Reference

TOE Commercial Name	TnD v5.1 on ID-One Cosmo X (BAC Configuration)
Applet Code Versions (SAAAAR Code)	See **TOE Configurations** table below
Applet Internal Versions	See **Applet Internal Versions** table below
Platform Name	ID-One Cosmo X
Platform Certificate	[PTF-CERT]
IC Certificate Reference	BSI_DSZ-CC-1107-V3-2022

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

Configurations	Description of the configurations	Content of the config (package/cap files)	
Config 1	TnD Applet without support for MOC	SAAAAR + version + Config of TnD Java Applet on Cosmo X {config 1}	203621FF 05010000 **0101**
		SAAAAR + version + config of Common Package {Cosmo X build} {Config 1}	417641FF 01000000 **0201**
Config 2	TnD Applet with support for MOC	SAAAAR + version + config of TnD Java Applet on Cosmo X {config 2}	203621FF 05010000 **0201**
		SAAAAR + version + config of Common Package {Cosmo X build} {Config 2}	417641FF 01000000 **0301**

Table 1 TOE Configurations

Note:

In the table above a "SAAAAR code" is denoted by first 4 bytes, a "version" by the next 2 bytes and a "config" ID by the last 2 bytes.

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

S	IDEMIA Site code	1 byte
AAAA	Article number	4 bytes
R	Software Release number	1 byte

Applet Internal Versions of above Configurations are as follows:

Configurations	Returned value of DF67
Config 1	00 00 02 08 01 01 00 08
Config 2	00 00 02 08 01 04 00 07

Table 2 Applet Internal Versions

2 Technical Terms, Abbreviations and Associated References

2.1 Technical Terms

Term	Definition
Accurate Terminal Certificate	A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the travel document's chip to produce Terminal Certificates with the correct certificate effective date, see [TR-03110-1].
Advanced Inspection Procedure (with PACE)	A specific order of authentication steps between a travel document and a terminal as required by [TR-03110-1], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SO_D and (iv) Terminal Authentication v.1. AIP can generally be used by EIS-AIP-PACE.
Agreement	This term is used in the current ST in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
Active Authentication	Security mechanism defined in [ICAO-9303]. Option by which means the MTRD's chip proves and the inspection system verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known State of organization.
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7).
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialisation Data and Pre-personalization Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization
Basic Access Control	Security mechanism defined in [ICAO-9303] by which means the MTRD's chip proves and the inspection system protect their communication by means of secure messaging with Basic Access Keys (see there).
Basic Inspection System (BIS)	A technical system being used by an inspecting authority and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). The Basic Inspection System with PACE is a PACE Terminal additionally supporting/applying the Passive Authentication protocol and is authorised by the travel document Issuer through the Document Verifier of receiving state to read a subset of data stored on the travel document.

Term	Definition
Biographical data (bio data).	The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa.
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Card Access Number (CAN)	Password derived from a short number printed on the front side of the data-page.
Certificate chain	A sequence defining a hierarchy certificates. The Inspection System Certificate is the lowest level, Document Verifier Certificate in between, and Country Verifying Certification Authority Certificates are on the highest level. A certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means.
Country Signing CA Certificate (C_{CSCA})	Self-signed certificate of the Country Signing CA Public Key ($K_{Pu\ CSCA}$) issued by CSCA stored in the inspection system.
Country Signing Certification Authority (CSCA)	An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel documents and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [ICAO-9303], 5.5.1. The Country Signing Certification Authority issuing certificates for Document Signers (cf. [6]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [TR-03110-1].
Country Verifying Certification Authority (CVCA)	An organisation enforcing the privacy policy of the travel document Issuer with respect to protection of user data stored in the travel document (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the terminals using it and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [TR-03110-1]. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a CVCS as a subject; hence, it merely represents an organizational entity within this ST.

Term	Definition
	The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [ICAO-9303]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [TR-03110-1].
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CV Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Basic Access Key Derivation Algorithm	The [ICAO-9303] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
Document Details Data	Data printed on and electronically stored in the travel document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
Document Basic Access Keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD's chip and the inspection system [ICAO-9303]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Security Object (SO_D)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS). [ICAO-9303]
Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS), see [TR-03110-1] and [ICAO-9303].

Term	Definition
	This role is usually delegated to a Personalization Agent.
Document Verifier (DV)	An organisation enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organisation / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a Certification Authority, authorised by at least the national CVCA to issue certificates for national terminals, see [TR-03110-1]. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a DV as a subject; hence, it merely represents an organisational entity within this ST. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the travel document Issuer und a foreign CVCA ensuring enforcing the travel document Issuer's privacy policy) [1] [2]
Eavesdropper	A threat agent with low attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO-9303]
ePassport application	[PACE-PP] definition A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [TR-03110-1]. [PP-EAC] definition Non-executable data defining the functionality of the operating system on the IC as the travel document's chip. It includes the file structure implementing the LDS [ICAO-9303],

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

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

Term	Definition
	the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and the TSF Data including the definition the authentication data but except the authentication data itself.
Extended Access Control	Security mechanism identified in [ICAO-9303] by which means the MTRD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait.
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [ICAO-9303]
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases.
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.

Term	Definition
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document.
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [ICAO-9303]
Initialisation	Process of writing Initialisation Data (see below) to the TOE (TOE life-cycle, Phase 2 Manufacturing, Step 3).
Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
Inspection	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [ICAO-9303]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.
Integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO-9303]]
Issuing State	The Country issuing the MRTD. [ICAO-9303]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO-9303]. The capacity expansion technology used is the MRTD's chip.

Term	Definition
Logical Data Structure 2 (LDS2)	The file structures required to support the ICAO LDS2 [9303-10_LDS2] consisting of LDS file structure with three additional and optional applications: • Travel records (stamps); • Visa records; and • Additional biometrics.
Logical travel document	Data of the travel document holder stored according to the Logical Data Structure [ICAO-9303] as specified by ICAO on the contact based/contactless integrated circuit. It presents contact based/contactless readable data including (but not limited to) personal data of the travel document holder the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), the digitized portraits (EF.DG2), the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and the other data according to LDS (EF.DG5 to EF.DG16). EF.COM and EF.SOD
Machine readable travel document (MRTD)	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [ICAO-9303]
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [ICAO-9303] The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for PACE.
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO-9303]
Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.

Term	Definition
Metadata of a CV Certificate	Data within the certificate body (excepting Public Key) as described in [TR-03110-1]. The metadata of a CV certificate comprise the following elements: - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorisation Template, - Certificate Effective Date, - Certificate Expiration Date.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (DG3) or (ii) encoded iris image(s) (DG4) or (iii) both. Note that the European commission decided to use only finger print and not to use iris images as optional biometric reference data.
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [ICAO-9303] part 11. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
PACE passwords	Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [ICAO-9303] part 11 or a user PIN or PUK as specified in [TR-03110-3]
Polymorphic Authentication Terminal / Service	The terminal or authentication web service that is authorized to retrieve the Polymorphic ID attributes form a Polymorphic eMRTD using standard ICAO and EAC1 ePassport protocols (PACE, CAv1, TAv1) and the Polymorphic Authentication (PMA)protocol to retrieve the PP, PI and CPI data. A Polymorphic Authentication Terminal/Service: • implements the terminal part of the PACEv2 with PIN, PA, CAv1 and TAv1 protocols configured in accordance with ICAO DOC9303 and TR-03110 v2.10 and the Polymorphic Authentication protocol (PMA). • performs the Advanced Inspection Procedure as a precondition to gain access to the randomized polymorphic user data (PI, PP and optional CPI) by executing the PMA protocol. The Polymorphic Authentication Terminal/Service must pass PACE with the correct user PIN and successful CAv1/TAv1 in order to be able to execute the PMA protocol successfully.

Term	Definition
	performs the Polymorphic Authentication protocol (PMA) to retrieve the randomized polymorphic user data (PI, PP and optional CPI) and the non-card unique identifiable meta data.
Polymorphic Authentication System	The complete set of sub systems in the polymorphic authentication infrastructure, required to perform user authentication with privacy protection based on (randomized) Polymorphic ID attributes: • Polymorphic Authentication Service • (Central) Key Management Authority • (optional) Polymorphic eMRTD Status Service Polymorphic Service Provider
Polymorphic document holder	The owner of a Polymorphic eMRTD, that contains his Polymorphic ID attributes.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Personalization	The process by which the Personalization Data are stored in and unambiguously, inseparably associated with the travel document. This may also include the optional biometric data collected during the "Enrolment" (cf. paragraph 1.7.4.3, TOE life-cycle, Phase 3, Step 6).
Personalization Agent	An organisation acting on behalf of the travel document Issuer to personalize the travel document for the travel document holder by some or all of the following activities: ICAO eMRTD (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalization) and storing them in the travel document (electronic personalization) for the travel document holder as defined in [TR-03110-1], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [ICAO-9303] (in the role of DS). Polymorphic eMRTD (i) establishing the identity of the polymorphic document holder for requesting the Polymorphic ID attributes, (ii) Requesting the required Polymorphic eMRTD ID attributes from the central Key Management authority, (iii) writing Polymorphic ID attributes, Polymorphic LDS data as defined in [PCA-eMRTD], (iv) writing the TSF data as defined in [PCA-eMRTD],

Term	Definition
	(v) signing the Document Security Object defined in [ICAO-9303] (in the role of DS). Please note that the role 'Personalization Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role.
Personalization Data	A set of data incl. individual-related data (biographic and biometric data) of the travel document holder, dedicated document details data and dedicated initial TSF data (incl. the Document Security Object). Personalization data are gathered and then written into the non-volatile memory of the TOE by the Personalization Agent in the life-cycle phase card issuing.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Key	Symmetric cryptographic key or key set (MAC, ENC) used by the Personalization Agent to prove his identity and get access to the logical travel document and by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE (FIA_UAU.1/PACE_CAM, FIA_UAU.4/PACE_CAM, FIA_UAU.5/PACE_CAM for PACE CAM).
Physical part of the travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) biographical data, data of the machine-readable zone, photographic image and other data.
Pre-personalization	Process of writing Pre-Personalization Data (see below) to the TOE including the creation of the travel document Application (TOE life-cycle, Phase 2, Step 5)
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalization Agent Key Pair and Chip Life-Cycle Production data (CPLC data).

Term	Definition
Pre-personalized travel document's chip	Travel document's chip equipped with a unique identifier.
Receiving State	The Country to which the MRTD holder is applying for entry. [ICAO-9303]
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
RF-terminal	A device being able to establish communication with an RF-chip according to ISO/IEC 14443 [ISO14443].
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means [ICAO-9303].
Secure messaging in encrypted /combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [ISO7816]
Service Provider	An official organisation (inspection authority) providing inspection service which can be used by the travel document holder. Service Provider uses terminals (BIS-PACE) managed by a DV.
Skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Standard Inspection Procedure	A specific order of authentication steps between an travel document and a terminal as required by [ICAO-9303] and [TR-03110-1], namely PACE or BAC and Passive Authentication with SO_D. SIP can generally be used by BIS-PACE and BIS-BAC.
Inspection Procedure for multi-application eMRTDs	This section describes an inspection procedure designed for eMRTDs containing one or more applications besides the eMRTD application ("LDS2-documents"): [LDS2_TR] Annex A2.
Terminal	A terminal is any technical system communicating with the TOE either through the contact based or contactless interface. A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter. In this ST the role 'Terminal' corresponds to any terminal being authenticated by the TOE. Terminal may implement the terminal's part of the PACE protocol and thus authenticate itself to the travel document using a shared password (CAN or MRZ).

Term	Definition
Terminal Authorization	Intersection of the Certificate Holder Authorizations of the Inspection System Certificate, the Document Verifier Certificate and Country Verifier Certification Authority which shall be valid for the Current Date.
Terminal Authorisation Level	Intersection of the Certificate Holder Authorisations defined by the Terminal Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
TOE tracing data	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document.
Travel document	Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [ICAO-9303] (there "Machine readable travel document").
Travel document (electronic)	The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: *ePassport*.
Travel Document Holder	The rightful holder of the travel document for whom the issuing State or Organisation personalized the travel document.
Travel document's Chip	A contact based / contactless integrated circuit chip complying with ISO/IEC 14443 [15] and programmed according to the Logical Data Structure as specified by ICAO, [ICAO-9303], sec III.
Traveler	Person presenting the travel document to the inspection system and claiming the identity of the travel document holder.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [CC-1]).
Unpersonalized travel document	The travel document that contains the travel document chip holding only Initialisation Data and Pre-personalization Data as delivered to the Personalization Agent from the Manufacturer.
User data	All data (being not authentication data) stored in the context of the ePassport application of the travel document as defined in [5] and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE. CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC-1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC-2]).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is

Term	Definition
	being claimed, to determine whether it matches the enrollee's template. [ICAO-9303]
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

2.2 Abbreviations

Acronym	Definition
CC	Common Criteria
BIS	Basic Inspection System
BIS-PACE	Basic Inspection System with PACE
CA	Chip Authentication
CAN	Card Access Number
CLFDB	Ciphered Load File Data Block
PS	Personalization System
DBI	Digital Blurring of Images
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DF	Dedicated File
DH	Diffie Hellman
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EF	Elementary File
FID	File identifier
GP	Global Platform
IC	Integrated Chip
ICC	Integrated Chip card
ICCSN	Integrated Circuit Card Serial Number.
IFD	Interface Device
MAC	Message Authentication code
MF	Master File

MRZ	Machine readable zone
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile
PT	Personalization Terminal
RF	Radio Frequency
ROM	Read Only Memory
RSA	Rivest Shamir Adleman
RSA CRT	Rivest Shamir Adleman – Chinese Remainder Theorem
SAI	SAI (Scanning Area Identifier)
SAR	Security assurance requirement
SCP	Secure Channel Procotol
SFR	Security functional requirement
SHA	Secure Hashing Algorithm
SIP	Standard Inspection Procedure
ST	Security Target
TA	Terminal Authentication
TOE	Target Of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy (defined by the current document)

2.3 References

Reference	Description
[AGD_OPE]	FQR 220 1580 Ed 2 - TnD v5.1 on ID-One Cosmo X - Operational User Guidance (AGD_OPE)
[AGD_PRE]	FQR 220 1579 Ed 4 - TnD v5.1 on ID-One Cosmo X - Preparative Procedures (AGD_PRE)
[BAC-PP]	Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control, BSI-CC-PP-0055-2009, Version 1.10, 25th March 2009
[CC-1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 5. April 2017. CCMB-2017-04-001.
[CC-2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-002.
[CC-3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1. Revision 5. April 2017. CCMB-2017-04-004.
[EAC-PP]	EAC- Machine readable travel documents with "ICAO Application", Extended Access control – BSI-PP-0056 v1.10 25th march 2009
[ICAO-9303]	International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – 7th edition, 2015
[ISO14443]	ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2016
[ISO15946-2]	ISO/IEC15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002.
[ISO18013-3]	ISO/IEC 18013-3: Information technology — Personal identification — ISO-compliant driving licence. Part 3: Access control, authentication and integrity validation, 2009-03-01 Including ISO/CEI 18013-3/AC1:2011, TECHNICAL CORRIGENDUM 1, Published 2011-12-01
[ISO7816]	ISO/IEC 7816: Identification cards — Integrated circuit cards.
[ISO9796-2]	ISO/IEC 9796-2: 2002, Information Technology - Security Techniques - Digital Signature Schemes giving message recovery - Part 2: Integer factorization based mechanisms
[JCAPI]	Published by Oracle. Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5. May 2015.

Reference	Description
[NIST-180-4]	NIST. FIPS 180-4, Secure Hash Standard, February 2011.
[NIST-186-3]	NIST. Digital Signature Standard (DSS), FIPS 186-3, 2009
[PACE-PP]	Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011-MA-01, Version 1.01, 22 July 2014, BSI.
[PP-PL]	Java Card System - Open Configuration Protection Profile, Version 3.0.5, BSI-CC-PP-0099-2017
[PTF-ST]	Security Target Lite ID-ONE COSMO X, FQR 110 A19A Ed 2
[PTF-CERT]	ANSSI-CC-2023/06
[RFC-5639]	Lochter, Manfred; Merkle, Johannes. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, 2010
[PP-IC]	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014.
[TR-03110-1]	Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20.03.2012 by BSI
[TR-03110-2]	Technical Guideline TR-03110-2, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 2 – Extended Access Control Version 2 (EACv2),Password Authenticated Connection Establishment (PACE),and Restricted Identification (RI), Version 2.10, 20.03.2012 by BSI
[TR-03110-3]	TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3: Common Specifications, version 2.10, 2012-03-07 by BSI

3 TOE Overview and Description

3.1 TOE Overview

The TOE is a composite product that consist of an IDEMIA applet named TnD v5.1 and its supporting "Common" library package on top of the COSMO X Global Platform Java Card 3.0.5 operating system and Infineon SLC37 contact/contactless smart card security controller in **BAC configuration**.

It supports the ICAO and TR-3110-1 and -3 defined protocols for Basic Access Control (BAC), Chip Authentication v1 (CAv1) and Active Authentication (AA). In addition, the TOE supports Chip Authentication v1 with AES secure messaging.

For compliancy with the protection profiles claimed in this security target, the BAC protocol MUST be configured on the TOE for each configured ID document application mentioned below.

Within the scope of this ST, the TOE can be configured as a stand-alone application or as a combination of the following official ID document applications:

- ICAO/EAC eMRTD and
- EU/ISO Driving Licence compliant to ISO/IEC 18013 or ISO/IEC TR 19446.

The TOE may be used as an ISO Driving Licence (IDL) compliant to ISO/IEC 18013 or ISO/IEC TR 19446, as both eMRTD and IDL applications share the same protocols and data structure organization.

The TnD v5.1 application embeds other secure functionalities, like PACE (Generic Mapping (GM), Integrated Mapping (IM) and Chip Authentication Mapping (CAM)), Terminal Authentication v1 (TAv1), LDS2 protocol extensions for EAC1, Polymorphic Authentication protocol (PMA) for privacy-protected authentication with polymorphic ID attributes and Digital Bluring of Images (DBI), which are not in the scope of this evaluation, but are covered in the scope of other evaluated configurations of this product shown in Table 3 below.

This ST considers the TnD v5.1 application in **BAC configuration**, marked **bold** in the table below.

Configuration	PP Conformity	Extensions to the PP
1. EAC	PP 0056v1 (EAC)	- Active Authentication (AA) - Restart secure messaging AES128, AES192 and AES256 secure messaging (in addition to 3DES) after CAv1 - Digital Blurring of Images (DBI)
2. PACE/EAC1/Polymorphic eMRTD/LDS2	PP 0068 (PACE) PP 0056v2 (ICAO application, EAC with PACE)	- ICAO LDS2 protocol extensions for TAv1, PACE and CAv1 - Polymorphic eMRTD extensions for PMA and PACE - Active Authentication (AA) - PACE-CAM - BAC de-activation - Digital Blurring of Images (DBI)
3. BAC	**PP 0055 (BAC)**	- **Active Authentication (AA)** - **Chip Authentication v1 (CAv1)** - **Restart secure messaging AES128, AES192 and AES256 secure messaging (in addition to 3DES) after CAv1**

Table 3 Different evaluated configurations of the TnD application

Note
For interoperability reasons, an eMRTD will most likely support BAC, PACE and EAC. The three TOE configurations mentioned above cover the security level of the TOE depending on the inspection procedure executed by the Inspection System/Advanced Inspection System:

- If the Inspection System reads MRTD data after having performed BAC + EAC, the security of the MRTD will be covered by the security evaluation of the TOE described in the ST claiming compliance to [EAC-PP].
- If the Inspection System reads MRTD data after having performed PACE + EAC, the security of the MRTD will be covered by the security evaluation of the TOE described in the ST, claiming compliance to [EAC-PP-V2] and [PACE-PP].
- If the Inspection System reads MRTD data by performing only BAC, the security of the MRTD will be covered by the security evaluation of the TOE described in this ST, which claims compliance to the [BAC-PP].

3.2 TOE Description

The TOE in the **BAC configuration** encompasses the following features:

- In Personalization phase:
  - authentication protocol for personalization agent authentication;
  - 3DES, AES128, AES192 and AES256 Global Platform secure messaging;
  - access control;
  - Creation and configuration of application instances and their logical data structure;
  - Secure data loading;
  - Secure import and/or on-chip generation of Chip Authentication key pair for CAv1;
  - Secure import and/or on-chip generation of the AA key pair;
  - life-cycle phase switching to operational phase;

- In operational phase:
  - Chip Authentication v1 (CAv1);
  - Active Authentication (AA);
  - After CAv1: restart ICAO secure messaging in 3DES, AES128, AES192 or AES256 cipher mode;

3.2.1 Physical scope

From physical/hardware point of view, the TOE is a bare microchip with its external interfaces for communication. The physical medium on 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 in several form factors like wafer, chip modules on a reel, chip modules embedded in ID3 passport booklets or ID3 holder pages, chip modules embedded in ID1 cards, chip modules embedded in antenna inlays, etc.

The physical form of the module is depicted in Figure 1 below. The cryptographic boundary of the module is the surface and edges of the die and associated bond pads, shown as circles.

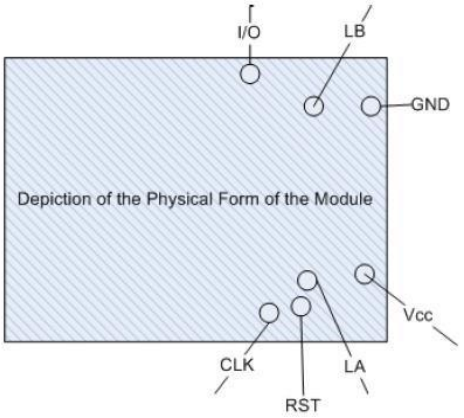

Figure 1 Physical Form

The contactless ports (LA and LB) of the module require a connection to an antenna. The other ports are required for connection to the contact plate of the contact chip module. The chip module's electrical interfaces are according to [ISO7816] and [ISO14443] interface specifications for respectively contact and contactless connections to card reader 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 4 TOE physical ports and interfaces

3.2.2 Logical Scope

The Target of Evaluation (TOE), addressed by the current security target, is an electronic travel document representing a contactless/contact based smart card or passport programmed according to Logical data structure (LDS). Electronic Passport is specified in [ICAO-9303], additionally providing the Chip Authentication v1 and Active Authentication according to [ICAO-9303]. The TOE may also be used as an ISO driving license, compliant to ISO/IEC 18013 or ISO/IEC TR 19446.

The TOE supports:

- Basic Access Control (BAC) protocol,
- Chip Authentication v1 (CAv1) protocol with AES128, ASE192, AES256 extensions,

- Active Authentication (AA) and

In accordance with [BAC-PP] the communication between terminal and chip SHALL be established and protected by the Basic Access Control protocol.

The "TnD v5.1 on Cosmo X" TOE consists of:

- The MRTD's chip circuitry and the IC dedicated software;
- The IC embedded software being the "ID-One Cosmo X platform" 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.
- TnD v5.1 Applet along with its Common (library) Package loaded in non-volatile (FLASH) memory*;
- The associated guidance documentation in [AGD_PRE] and [AGD_OPE];
- The Personalization Agent Key set (see [AGD_PRE]).

* In the remaining part of this Security Target, we refer "TnD v5.1 Applet along with its Common (library) Package" as "TnD v5.1 Application".

A schematic overview of the TOE's logical architecture is shown in Figure 2 below.

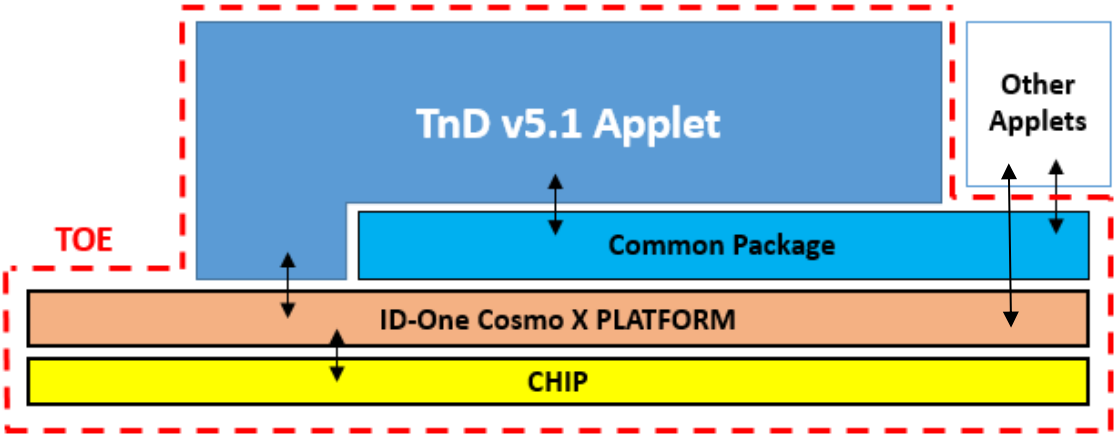

Figure 2 Logical Scope of the TOE

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 5 TOE Guidance

This ST Lite will also be provided along with above mentioned documents.

All the above mentioned guidance documents will be delivered via mail in a .pgp encrypted format.

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

Section 4, "Life Cycle" in this ST provides for more details about the TOE delivery for the different options.

3.3 Required Non-TOE hardware/software/firmware

The TOE does not require any explicit non-TOE hardware, software or firmware to perform its claimed security features. The TOE comprises the chip, the complete operating system and the TnD v5.1 application. Note that for an ICAO compliant ID document, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete travel document. Nevertheless, these parts are not critical for the security of the TOE.

In order to powerup the TOE and to communicate with it, a card reader is required.

3.4 TOE usage and security features for operational use

3.4.1 TOE Usage

Depending on its configuration during pre-personalization and personalization, the TOE can be used as:

- ICAO/EAC eMRTD or
- EU/ISO Driving Licence.

The ICAO/EAC eMRTD and Driver Licence are installed as a separate application instances of the TnD v5.1 applet, each having its own dedicated application identifier and personalization. The following TOE configurations are covered within the scope of this Security Target:

Configuration at Personalization	ICAO/EAC eMRTD	Driver licence
1	present	-
2	-	present

Table 6 TOE Configurations during Personalization

The authentication protocols Chip authentication (CAv1) and Active Authentication specified in [ICAO-9303] and [TR-03110] have also been referred to in ISO18013 for EU driving licences. The BAP-1 protocol defined in ISO18013 is equal to Basic Access Protocol (BAC) defined in [ICAO-9303]. As to the logical data structure, the ISO18013 uses the same concept of Passive Authentication defined in [ICAO-9303], but specifies different ISO7816-4 elementary file identifiers for storing the ICAO defined content of DG3, DG4 and DG15.

When an Issuing state is using the product as an ISO compliant Driving licence, the following name mapping of roles, definitions, data groups and protocol is applicable within the scope of this security target:

MRTD	ISO Driving License
MRTD	IDL
ICAO	ISO/IEC
ICAO 9303	ISO/IEC 18013 or ISO/IEC TR 19446
BAC	BAP-1
DG3	DG7
DG4	DG8
DG15	DG13
MRZ	MRZ or SAI (Scanning area identifier)
Traveler	Holder

Table 7 eMRTD and IDL Terminology

Note
In the remaining parts of this document, the word "MRTD" SHOULD be understood either as an

MRTD in the sense of ICAO or a driving license compliant to ISO/IEC 18013 or ISO/IEC TR 19446 depending on the targeted usage envisioned by the issuer.

A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this Security Target contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip according to LDS for contactless machine reading. The authentication of the traveler is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) optional biometrics using the reference data stored in the MRTD. The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

The MRTD is viewed as unit of

a) the **physical MRTD** as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder
   i) the biographical data on the biographical data page of the passport book,
   ii) the printed data in the Machine-Readable Zone (MRZ) and
   iii) the printed portrait.

b) the **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [ICAO-9303] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder
   i) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
   ii) the digitized portraits (EF.DG2),
   iii) the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both
   iv) the other data according to LDS (EF.DG5 to EF.DG16) and
   v) the Document security object.

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and the MRTD's chip is uniquely identified by the Document Number.

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [ICAO-9303]. These security measures include the binding of the MRTD's chip to the passport book.

The logical MRTD is protected in authenticity and integrity by a digital signature created by the document signer acting for the issuing State or Organization and the security features of the MRTD's chip.

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Extended Access Control to and the Data Encryption of additional sensitive biometrics as optional security measure in the 'ICAO Doc 9303' [ICAO-9303]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

This security target addresses the protection of the logical travel document (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Extended Access Control Mechanism. Also it addresses the Chip Authentication Version 1 described in [TR-03110] as an alternative to the Active Authentication stated in [ICAO-9303].

During the pre-personalization and personalization, the Personalization Agent, once authenticated, gets the rights (access control) for (1) reading and writing data,(2) instantiating the application, and

(4) writing of personalization data. The Personalization Agent can so create the file structure (MF / ADF) required for this configuration.

3.4.2 Security Features

3.4.2.1 Active Authentication (AA)

Active Authentication is an authentication mechanism ensuring the chip is genuine. It uses a challenge-response protocol between the IS and the chip.
Active Authentication is realized with the INTERNAL AUTHENTICATE command. The key and algorithms supported are the following:

- RSA ISO/IEC 9796-2 with a key length of 1536, 1792, 2048, 2560, 3072, 3584 and 4096 bits and hashing algorithm of SHA1 or SHA2 (i.e. SHA224, SHA256, SHA384 and SHA512).
- ECDSA over prime field curves with hashing algorithm of SHA1 or SHA2 and the key sizes 192 to 521.

3.4.2.2 Basic Access Control (BAC)

The protocol for Basic Access Control is specified by [BAC-PP]. Basic Access Control checks that the terminal has physical access to the MRTD's data page. This is enforced by requiring the terminal to derive an authentication key from the optically read MRZ of the MRTD. The protocol for Basic Access Control is based on [ISO11770-2] key establishment mechanism 6. This protocol is also used to generate session keys that are used to protect the confidentiality (and integrity) of the transmitted data.

The Basic Access Control (BAC) is a security feature that is supported by the TOE. The inspection system reads the printed data in the MRZ (for MRTD), authenticates itself as inspection system by means of keys derived from MRZ data. After successful 3DES based authentication, the TOE provides read access to data requiring BAC rights by means of a private communication (secure messaging) with the inspection system.

The purpose of this mechanism is to ensure that the holder gives access to the IS to the logical MRTD (data stored in the chip); It is achieved by a mutual authentication.
Once the mutual authentication is performed, a secure messaging is available to protect the communication between the chip and the IS. This table lists the supported configurations for BAC protocol:

Configuration	Key Algo	Key Length	Hash Algo	MAC Algo
BAC	3DES 2Key	16-bytes	SHA-1	Retail MAC

Table 8 BAC Configuration

3.4.2.3 Chip Authentication v1 (CAv1)

The Chip Authentication v1 protocol is an ephemeral-static Diffie-Hellman key agreement protocol that provides secure communication and unilateral authentication of the MRTD chip.

The protocol establishes Secure Messaging between an MRTD chip and a terminal based on a static key pair stored on the MRTD chip. Chip Authentication v1 is an alternative to the optional ICAO Active Authentication, i.e. it enables the terminal to verify that the MRTD chip is genuine but has two advantages over the original protocol:

- Challenge Semantics are prevented because the transcripts produced by this protocol are non-transferable.
- Besides authentication of the MRTD chip this protocol also provides strong session keys.

CAv1 provides implicit authentication of both the MRTD chip itself and the stored data by performing Secure Messaging using the new session keys.

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].

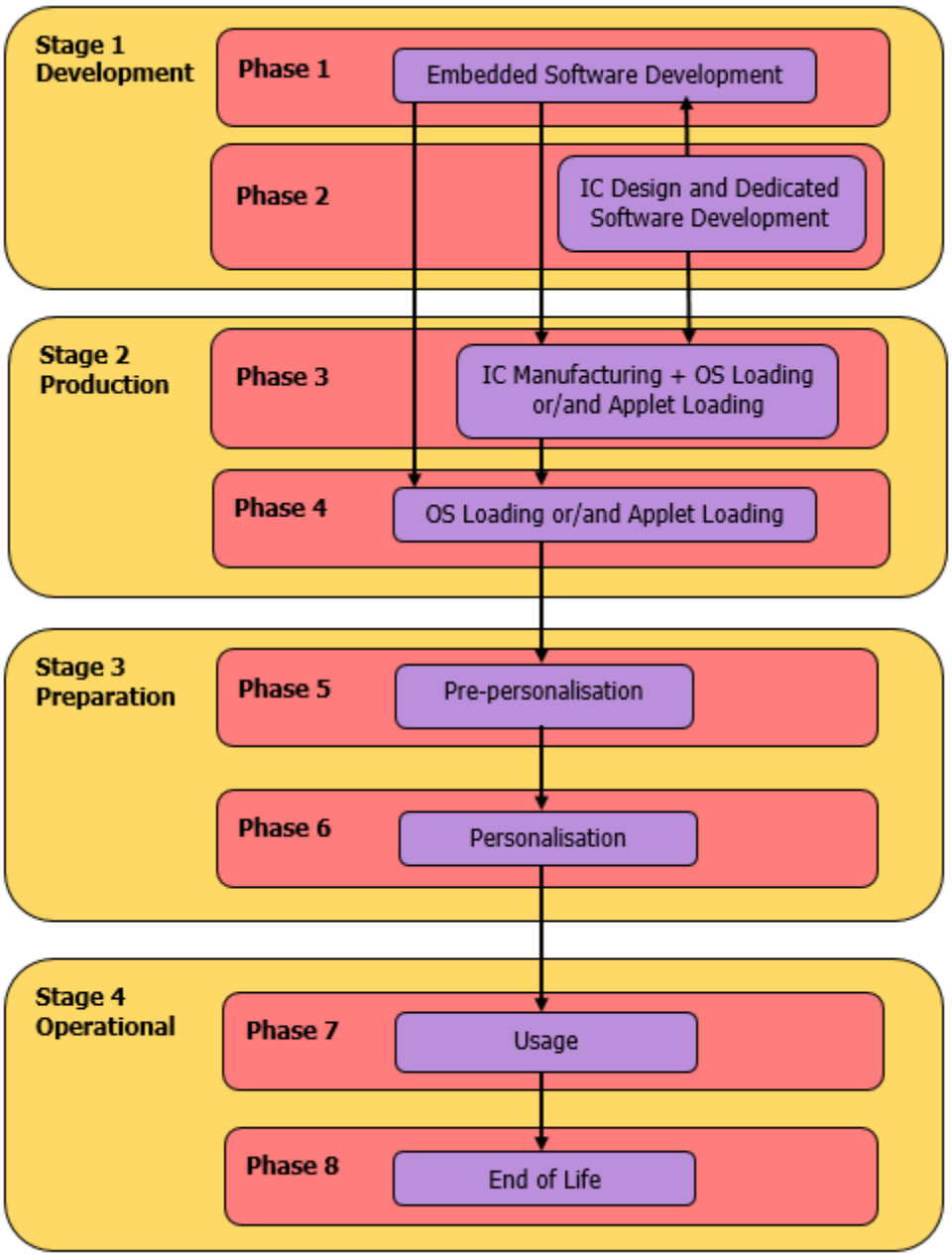

Figure 3 Life cycle Overview

4.1 Development Environment

In this environment, the following two phases take place:

- Phase 1: IC Embedded Software Development (Java Card Open Platform components and TnD v5.1 Application)

- 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 TnD v5.1 Application).

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
TnD v5.1 Applet Developer	IDEMIA	MANILA, JAKARTA,COURBEVOIE and PESSAC R&D sites	ALC
Embedded Software Developer (Java Card Open Platform)	IDEMIA	Platform Developer Refer to [PTF-ST]	ALC
Redaction and Review of Documents	IDEMIA	NOIDA and HAARLEM R&D site	ALC
IC Developer	INFINEON	IC Manufacturer Refer to [PTF-ST]	ALC

4.2 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 TnD v5.1 Application loading (TnD v5.1 applet and its Common package)

The TnD v5.1 Applet run time code and its Common Package are integrated in the FLASH memory of the chip.

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

(Option 1) Image Loading audited IC Manufacturer site

FLASH image containing both the "Cosmo X" Java Card Platform OS along with the TnD v5.1 Application is securely delivered directly from the software developer (IDEMIA R&D Audited Site) to the **IC Manufacturer** (Infineon CC Audited Site) to be loaded into FLASH memory. The FLASH image is always encrypted. Decryption is performed by the FLASH loader application inside the IC. The IC loader application is preconfigured with the FLASH decryption (and Authentication) key the during IC wafer initialisation by the IC Manufacturer.

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

- The TOE delivery point occurs in Phase 4, as soon as the loading of the image with Java Card Platform OS + TnD 5.1 Applet + Common package by the IC Manufacturer has completed.

Package	Actor for FLASH image loading	Site For FLASH image loading	Covered by CC
FLASH image containing Java Card Platform OS + TnD v5.1 Applet and Common package	IC Manufacturer	**IC Manufacturer CC Audited Production Plants specified in [PTF-ST]**	**ALC**

Table 9 Option 1: Both Platform and Applet packages are loaded at IC Manufacturer Site

(Option 2) Image loading at IDEMIA and External sites

FLASH image containing both Cosmo X Platform along with TnD v5.1 Applet and Common package is securely delivered directly from the software developer (IDEMIA R&D Audited Site) for loading to **CC Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen or Ostrava) or **Non-Audited IDEMIA Sites** or **External Sites**.

TOE Delivery point:

- If loading of Java Card Platform package + TnD v5.1 Applet run time code including its Common Package (as described below) is performed in Audited IDEMIA Production Sites, then TOE delivery is considered at the end of Phase 4.
- If loading of Java Card Platform package + + TnD v5.1 Applet run time code including its Common Package (as described below) is performed in Non-Audited IDEMIA Production Sites or External Sites, then TOE delivery is considered after Phase 4.

Package	Actor for FLASH image loading	Site for FLASH image loading	Covered by CC
FLASH image containing the Java Card Platform OS + TnD v5.1 Applet and Common package	IDEMIA Authorized Entity or External Authorized Agent	**CC Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)** or Non-Audited IDEMIA Sites or External Sites	**ALC** or AGD

Table 10 Option 2: Both Platform and Applet packages are loaded at CC Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites

(Option 3) Platform loaded by IC Manufacturer, Applet loaded by IDEMIA or 3rd party
Only the Cosmo X Platform is delivered to the IC Manufacturer (Infineon Audited Sites) to be loaded.

With the Cosmo X Platform already loaded (i.e. present) on the chip, the following options (**3a or 3b (i) or 3b (ii) or 3c**) can be chosen for loading the TnD v5.1 applet and its Common Package.

(Option 3a) Applet loading using GP CLFDB mechanism.
The TnD v5.1 Applet with its Common package along with the TOE's guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen, Ostrava) or **Non-Audited IDEMIA Sites** or **External Sites**.
Loading of the TnD v5.1 Applet and its Common package on top of the already present COSMO X GP Java Card OS in any of these sites is accomplished by using a GP CLFDB decryption Key.

TOE Delivery points:

- If loading of the TnD v5.1 Applet with its Common package on top of already loaded Java Card Platform package (as described below) is done in a CC Audited IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.

- If loading of the TnD v5.1 Applet with its Common package on top of already loaded Java Card Platform package (as described below) is done in Non-Audited IDEMIA Production Sites or External Sites then, TOE delivery is considered after phase 4.

Package	Actor	Site	Covered by
Image containing only Java Card Platform OS	IC Manufacturer	IC Manufacturer Production Plants Refer to [PTF-CERT]	ALC
TnD v5.1 Applet and Common package loaded through GP mechanism using CLFDB Key	IDEMIA Authorized Entity or External Authorized Agent	**Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)** or Non-Audited IDEMIA Sites or External Sites	**ALC** or AGD

Table 11 Option 3(a): Platform package is loaded at IC Manufacturer Site and Applet package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites through GP Mechanism

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

(i) TnD v5.1 Application with Common package along with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen, Ostrava) or **Non-Audited IDEMIA Sites** or **External Sites**.

TnD v5.1 applet and its Common package are securely loaded via LSK on top of the present COSMO X Java Card OS in any of these sites. This loading is accomplished by using the IDEMIA "Resident Application" of the COSMO X OS

(ii) The DUMP package (including TnD v5.1 Application with Common package data) with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen, Ostrava) or **Non-Audited IDEMIA Sites** or **External Sites**.

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

TOE Delivery points:

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

Package	Actor	Site	Covered by
Image containing only Java Card Platform OS	IC Manufacturer	IC Manufacturer Production Plants Refer to [PTF-CERT]	ALC
3b (i) TnD v5.1 Applet and Common package loaded through Resident Application using LSK format	IDEMIA Authorized Entity or External Authorized Agent	**Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)** or Non-Audited IDEMIA Sites or External Sites	**ALC** or AGD
3b (ii) DUMP PACKAGE Ciphered format [DSK Secret Live Key]	IDEMIA Authorized Entity		

Table 12 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 Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites

(Option 3c) Applet loading in plain (unprotected) format using GP
TnD v5.1 Application with Common package along with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **CC Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen, Ostrava).

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

TOE Delivery points:

- The loading of TnD v5.1 applet and Common package on top of already loaded Java Card Platform package is done in plain (unprotected) format in Common Criteria Audited IDEMIA Production Sites. The TOE delivery is considered at the end of Phase 4.

Package	Actor	Site	Covered by
Image containing only Java Card Platform OS	IC Manufacturer	IC Manufacturer Production Plants Refer to [PTF-CERT]	ALC
TnD v5.1 Applet and Common package in Plain Format	IDEMIA Authorized Entity	CC Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)	ALC

Table 13 Option 3(c): Platform package is loaded at IC Manufacturer Site and Applet package in plain format is loaded at Audited IDEMIA Sites only

(Option 4) Platform and Applet loaded by IDEMIA or 3rd party
Only Cosmo X Platform is securely delivered directly from the software developer (IDEMIA R&D Audited Site) for loading to **CC Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen or Ostrava) or **Non-Audited IDEMIA Sites** or **External Sites**.

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

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

(Option 4a) Applet loading using GP CLFDB mechanism
TnD v5.1 Applet and Common package along with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen, Ostrava) or **Non-Audited IDEMIA Sites** or **External Sites**.

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

TOE Delivery points:

- If loading of the TnD v5.1 Applet and Common package on top of already loaded Java Card Platform package (as described below) is done in CC Audited IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.

- If loading of the TnD v5.1 Applet and Common package onto the already loaded Java Card Platform OS package (as described below) is done in Non-Audited IDEMIA Production Sites or External Sites then, TOE delivery is considered after Phase 4.

Package	Actor	Site	Covered by
Image containing only Java Card Platform OS	IDEMIA Authorized Entity or External Authorized Agent	**Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)** or Non-Audited IDEMIA Sites or External Sites	**ALC** or AGD
TnD v5.1 Applet and Common package loaded through GP mechanism using CLFDB Key	IDEMIA Authorized Entity or External Authorized Agent	**Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)** or Non-Audited IDEMIA Sites or External Sites	**ALC** or AGD

Table 14 Option 4(a): Platform package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites and Applet package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites through GP Mechanism

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

(i) TnD v5.1 Application with Common package along with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen, Ostrava) or **Non-Audited IDEMIA Sites** or **External Sites**.

Secure loading of TnD v5.1 applet and its Common package is done via LSK on top of the present COSMO X Java Card OS (already loaded by **Audited IDEMIA Production Sites** or **Non-Audited IDEMIA Sites** or **External Sites)** in any of these sites. This loading is accomplished by using the IDEMIA "Resident Application" of the COSMO X OS

(ii) DUMP package (including the TnD v5.1 Applet and Common package data) with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen, Ostrava) or **Non-Audited IDEMIA Sites** or **External Sites**.

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

TOE Delivery points:

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

Package	Actor	Site	Covered by
Image containing only Java Card Platform OS	IDEMIA Authorized Entity or External Authorized Agent	**Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)** or Non-Audited IDEMIA Sites or External Sites	**ALC** or AGD
4b (i) TnD v5.1 Applet and Common package loaded through Resident Application using LSK format	IDEMIA Authorized Entity or External Authorized Agent	**Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)** or Non-Audited IDEMIA Sites or External Sites	**ALC** or AGD
4b (ii) DUMP PACKAGE Ciphered format [DSK Secret Live Key]	IDEMIA Authorized Entity		

Table 15 Platform package is loaded at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites and Options 4b(i) Applet package is loaded through Resident application using LSK format and and 4b(ii) DUMP Package is loaded through resident application using DSK Secret Live Key - at Audited IDEMIA Sites or Non-Audited IDEMIA Sites or External Sites

(Option 4c) Applet loading in plain (unprotected) format using GP
TnD v5.1 Application with Common package along with the guidance documentation is securely delivered directly from the Software Developer (IDEMIA R&D Audited Site) to **Audited IDEMIA Production Sites** (Haarlem, Noida, Vitré, Shenzhen, Ostrava).

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

TOE Delivery points:

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

Package	Actor	Site	Covered by
Image containing only Java Card Platform OS	IDEMIA Authorized Entity or External Authorized Agent	**CC Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)** or Non-Audited IDEMIA Sites or External Sites	**ALC** or AGD
TnD v5.1 Applet and Common package in Plain Format	IDEMIA Authorized Entity	**CC Audited IDEMIA Production Sites (Shenzhen, Haarlem, Vitré, Noida, Ostrava)**	**ALC**

Table 16 Option 4(c): Platform package is loaded at IC Manufacturer Site and Applet package in plain format is loaded at CC Audited IDEMIA Sites only

4.3 Preparation Environment

In this environment, the following two phases take place:

- Phase 5: Pre-personalization of the applet
- Phase 6: Personalization

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

The TnD v5.1 applet is pre-personalized and personalized according to [AGD_PRE].

These two phases are covered by [AGD_PRE] tasks of the TOE and Guidance tasks of [PTF-ST].

4.4 Operational Environment

- Phase 7: Use Phase

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

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

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

This phase is covered by [AGD_OPE] tasks of the TOE and Guidance tasks of [PTF-ST].

5 Conformance Claims

5.1 CC Conformance Claim

This security target claims conformance to the Common Criteria version 3.1, revision 5 ([CC-1], [CC-2] and [CC-3]).

The conformance to the Common Criteria is claimed as follows:

CC	Conformance rationale
Part 2	Conformance with the extended[3] part: FAU_SAS.1 "Audit Storage" FCS_RND.1 "Quality metric for random numbers" FMT_LIM.1 "Limited capabilities" FMT_LIM.2 "Limited availability" FPT_EMS.1 "TOE Emanation" FIA_API.1 "Authentication Proof of Identity"
Part 3	Conformance to Part 3.

Table 8: Conformance Rationale

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

Application note
Not all key sizes specified in this security target have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". In order to be protected against attackers with a "high attack potential", sufficiently large cryptographic key sizes SHALL be configured for this TOE. References can be found in national and international document standards. Further details have been specified in the TOE's guidance documentation [AGD_PRE].

5.2 PP Claim

This security target claims strict conformance to:
Common Criteria Protection Profile - Machine Readable Travel Document with "ICAO Application", Basic Access Control, BSI-PP-0055, Version 1.10, 25th March. 2009 [BAC-PP]

5.3 Package Claim

This ST is conforming to assurance package EAL4 augmented with ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_DVS.2, ALC_CMS.5, ALC_TAT.2 and ATE_DPT.3 defined in CC part 3 [CC-3].

5.4 PP Conformance Rationale

This ST is claimed to be strictly conformant to the above mentioned PP [BAC-PP]. A detailed justification is given in the following.

[3] The rationale for SFR addition is described in the relative PP

5.4.1 Main aspects

- All definitions of the security problem definition in [BAC-PP] have been taken exactly from the PP in the same wording.
- All security objectives have been taken exactly from [BAC-PP] in the same wording.
- The part of extended components definition has been taken originally from [BAC-PP], except for FIA_API which has been taken from [EAC-PP]. Note that the ST does not claim conformance to [EAC-PP].
- All SFRs for the TOE have been taken originally from the [BAC-PP] added by according iterations, selections and assignments.
- The security assurance requirements (SARs) have been taken originally from the PP.

5.4.2 Overview of differences between the PP and the ST

Threats

The threat **T.Counterfeit** has been added to describe an unauthorized copy or reproduction of a genuine MRTD's chip.

Assumptions

Two assumption was added to cover Active Authentication and Chip Authentication during personalization:

- **A.Insp_Sys_Chip_Auth**
- **A.Insp_Sys_AA**

Security Objectives for the TOE

The **OT.Chip_Auth_Proof** and **OT.AA_Proof** were added to cover Chip Authentication and Active Authentication.

Security Objectives for the Environment

Additional OEs were added to cover Active Authentication and Chip Authentication v1 (CAv1):

- **OE.Auth_MRTD**
- **OE.Exam_Chip_Auth**
- **OE.Exam_MRTD_AA**
- **OE.Activ_Auth_Sign**

Security Functional Requirements

The Security Target enhances additional security functional requirements to support Chip Authentication v1 (CAv1) and Active Authentication.

The additions do not contradict any of the threats, assumptions, organizational policies, objectives or SFRs stated in the [PP_BAC] that covers the advanced security methods BAC in operational use phase.

6 Security Problem Definition

6.1 Assets

6.1.1 Logical MRTD data

The following table presents the assets of the TOE and their corresponding phase(s).

Asset	Phase 5	Phase 6	Phase 7
Personal Data	No	Yes	Yes
Biometric Data	No	Yes	Yes
EF.COM	No	Yes	Yes
EF.SOD	No	Yes	Yes
CA_PK	No	Yes	Yes
CA_SK	No	Yes	Yes
Perso_K	No	Yes	No
BAC_K	No	Yes	Yes
Session_K	Yes	Yes	Yes
LCS	Yes	Yes	Yes

6.1.1.1 Personal Data

The Personal Data are the logical MRTD standard User Data of the MRTD holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16).

6.1.1.2 Biometric Data

The Biometric Data are the sensitive biometric reference data (EF.DG3, EF.DG4).

6.1.1.3 EF.COM

The EF.COM is an elementary file containing the list of the existing elementary files (EF) with the user data.

6.1.1.4 EF.SOD

The elementary file Document Security Object is used by the inspection system for Passive Authentication of the logical MRTD.

6.1.1.5 Chip Authentication Public Key (CA_PK)

The Chip Authentication Public Key (contained in EF.DG14) is used by the inspection system for the Chip Authentication.

6.1.1.6 Chip Authentication Private Key (CA_SK)

The Chip Authentication Private Key is used by the application to process Chip Authentication.

6.1.1.7 Personalization Agent keys (Perso_K)

This key set used for mutual authentication between the Personalization agent and the chip, and secure communication establishment.

6.1.1.8 BAC keys (BAC_K)

This key set used for secure communication establishment between the Terminal and the chip.

6.1.1.9 Secure Messaging session keys (Session_K)

Session keys are used to secure communication in confidentiality and authenticity.

6.1.1.10 TOE Life Cycle State (LCS)

This is the Life Cycle State related to the Prepersonalization, Personalization and use phase of the application.

6.1.2 Miscellaneous

6.1.2.1 Authenticity of the MRTD's chip

The authenticity of the MRTD's chip personalized by the issuing State or Organization for the MRTD holder is used by the Traveler to prove his possession of a genuine MRTD.

6.2 Users / Subjects

The following table presents the assets of the TOE and their corresponding phase(s) according to §1.3.6 TOE description

Subject	Phase 3	Phase 4	Phase 5	Phase 6	Phase 7
IC manufacturer (Manufacturer role)	Yes	No	No	No	No
MRTD packaging responsible (Manufacturer role)	No	Yes	No	No	No
Embedded software loading responsible (Manufacturer role)	No	Yes	No	No	No
Pre-personalization Agent (Manufacturer role)	No	No	Yes	No	No
Personalization Agent	No	No	No	Yes	No
Terminal	No	No	Yes	Yes	Yes
Inspection System	No	No	No	No	Yes

Subject	Phase 3	Phase 4	Phase 5	Phase 6	Phase 7
MRTD Holder	No	No	No	No	Yes
Traveler	No	No	No	No	Yes
Attacker	Yes	Yes	Yes	Yes	Yes

6.2.1 IC manufacturer

This additional subject is a refinement of the role Manufacturer as described in [PP_BAC]. It is the manufacturer of the IC.

If the IC Manufacturer loads the TOE at phase 3, this subject is responsible for the embedded software downloading in the IC. This subject does not use Flash loader, even if it is embedded in the IC.

6.2.2 MRTD packaging responsible

This additional subject is a refinement of the role Manufacturer as described in [PP_BAC]. This subject is responsible for the combination of the IC with hardware for the contactless and/or contact interface.

6.2.3 Embedded software loading responsible

This additional subject is a refinement of the role Manufacturer as described in [PP_BAC]. This subject is responsible for the embedded software loading when the TOE is loaded by the OS loader in phase 4 before TOE delivery point This subject does not exist if the TOE is loaded by the IC Manufacturer. This subject used the Flash loader embedded in the IC.

6.2.4 Pre-personalization Agent

This additional subject is a refinement of the role Manufacturer as described in [PP_BAC]. This subject is responsible for the preparation of the card, i.e. creation of the MF and MRTD ADF. He also sets Personalization Agent keys.

6.2.5 Personalization Agent

The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (iv) signing the Document Security Object defined in [ICAO-9303].

6.2.6 Terminal

A terminal is any technical system communicating with the TOE through the contactless interface.

Note: as the TOE may also be used in contact mode, the terminal may also communicate using the contact interface

6.2.7 Inspection system (IS)

A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the Traveler and verifying its authenticity and (ii) verifying the Traveler as MRTD holder. The Basic Inspection System (BIS) (i) contains a terminal for the contactless

communication with the MRTD's chip, (ii) implements the terminals part of the Basic Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the MRTD or other parts of the passport book providing this information. The General Inspection System (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism. The Extended Inspection System (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

6.2.8 MRTD Holder

The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.

6.2.9 Traveler

Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.

6.2.10 Attacker

A threat agent trying (i) to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the printed MRZ data), (ii) to read or to manipulate the logical MRTD without authorization, or (iii) to forge a genuine MRTD.

6.3 Threats

6.3.1 Threats from PP BAC

6.3.1.1 T.Chip_ID

"Identification of MRTD's chip"

Adverse action: An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface.

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance

Asset: Anonymity of user

6.3.1.2 T.Skimming

"Skimming the logical MRTD"

Adverse action: An attacker imitates an inspection system trying to establish a communication to read the logical MRTD or parts of it via the contactless communication channel of the TOE.

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance.

Asset: confidentiality of logical MRTD data.

6.3.1.3 T.Eavesdropping

"Eavesdropping to the communication between TOE and inspection system"

Adverse action: An attacker is listening to an existing communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know these data in advance.

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance.

Asset: confidentiality of logical MRTD data.

6.3.1.4 T.Forgery

"Forgery of data on MRTD's chip"

Adverse action: An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data. This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the Traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a Traveler into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another contactless chip.

Threat agent: having enhanced basic attack potential, being in possession of one or more legitimate MRTDs.

Asset: authenticity of logical MRTD data.

6.3.1.5 T.Abuse-Func

"Abuse of Functionality"

Adverse action: An attacker may use functions of the TOE which shall not be used in the phase "Operational Use" in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data. This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder.

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD.

Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

6.3.1.6 T.Information_Leakage

"Information Leakage from MRTD's chip"

Adverse action: An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker. Leakage may occur through emanations, variations in power

consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD.

Asset: confidentiality of logical MRTD and TSF data.

6.3.1.7 T.Phys-Tamper

"Physical Tampering"

Adverse action: An attacker may perform physical probing of the MRTD's chip in order (i) to disclose TSF Data or (ii) to disclose/reconstruct the MRTD's chip Embedded Software. An attacker may physically modify the MRTD's chip in order to (i) modify security features or functions of the MRTD's chip, (ii) modify security functions of the MRTD's chip Embedded Software, (iii) modify User Data or (iv) to modify TSF data. The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRTD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD.

Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

6.3.1.8 T.Malfunction

"Malfunction due to Environmental Stress"

Adverse action: An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software. This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD.

Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

6.3.2 Additional Threat

6.3.2.1 T.Counterfeit

"MRTD's chip"

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

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

Asset: authenticity of logical MRTD data

6.4 Organisational Security Policies

6.4.1 P.Manufact

"Manufacturing of the MRTD's chip"

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

6.4.2 P.Personalization

"Personalization of the MRTD by issuing State or Organization only"

The issuing State or Organization guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical MRTD with respect to the MRTD holder. The personalization of the MRTD for the holder is performed by an agent authorized by the issuing State or Organization only.

6.4.3 P.Personal_Data

"Personal data protection policy"

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [ICAO-9303].

Application Note:

Note that EF.DG3 and EF.DG4 are only readable after successful EAC authentication, not covered by this ST.

6.5 Assumptions

6.5.1 Assumptions from PP BAC

6.5.1.1 A.MRTD_Manufact

"MRTD manufacturing on phase 4 to 6"

It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain

confidentiality and integrity of the MRTD and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

6.5.1.2 A.MRTD_Delivery

"MRTD delivery during phase 4 to 6"

Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:

- Procedures shall ensure protection of TOE material/information under delivery and storage.
- Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
- Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

6.5.1.3 A.Pers_Agent

"Personalization of the MRTD's chip"

The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document Basic Access Keys, (iii) the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip, and (iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

6.5.1.4 A.Insp_Sys

"Inspection Systems for global interoperability"

The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the Traveler and verifying its authenticity and (ii) verifying the Traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO-9303]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

6.5.1.5 A.BAC-Keys

"Cryptographic quality of Basic Access Control Keys"

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the [ICAO-9303], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

6.5.2 Additional Assumptions

6.5.2.1 A.Insp_Sys_Chip_Auth

"Inspection Systems for global interoperability on chip authenticity"

The Inspection System implements the following protocol to authenticate the MRTD's chip: Chip Authentication v1 as defined in [TR-03110].

The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the Traveler and verifying its authenticity and (ii) verifying the Traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO-9303]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD. The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism v1. The General Inspection System reads the logical travel document under BAC and performs the Chip Authentication v1 to verify the logical travel document and establishes a new secure messaging that is different from the BAC one.

6.5.2.2 A.Insp_Sys_AA

The Inspection System implements the Active Authentication Mechanism. The Inspection System verifies the authenticity of the MRTD's chip during inspection using the signature returned by the TOE during Active Authentication.

7 Security Objectives

7.1 Security Objectives for the TOE

This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organizational security policies to be met by the TOE.

7.1.1 Security Objectives listed in PP BAC

7.1.1.1 OT.AC_Pers

"Access Control for Personalization of logical MRTD"

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [ICAO-9303] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG 3 to EF.DG16 are added.

7.1.1.2 OT.Data_Int

"Integrity of personal data"

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The TOE must ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data.

7.1.1.3 OT.Data_Conf

"Confidentiality of personal data"

The TOE must ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. Read access to EF.DG1 to EF.DG16 is granted to terminals successfully authenticated as Personalization Agent. Read access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 is granted to terminals successfully authenticated as Basic Inspection System. The Basic Inspection System shall authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Basic Inspection System.

7.1.1.4 OT.Identification

"Identification and Authentication of the TOE"

The TOE must provide means to store IC Identification and Pre-Personalization Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the MRTD". The storage of the Pre-Personalization data includes writing of the Personalization Agent Key(s). In Phase 4 "Operational Use" the TOE shall identify itself only to a successful authenticated Basic Inspection System or Personalization Agent.

7.1.1.5 OT.Prot_Abuse-Func

"Protection against Abuse of Functionality"

After delivery of the TOE to the MRTD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to (i) disclose critical User Data, (ii) manipulate critical User Data of the IC Embedded Software, (iii) manipulate Soft-coded IC Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE.

Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

7.1.1.6 OT.Prot_Inf_Leak

"Protection against Information Leakage"

The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the MRTD's chip

- 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 and
- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE

7.1.1.7 OT.Prot_Phys-Tamper

"Protection against Physical Tampering"

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the MRTD's chip Embedded Software. This includes protection against attacks with enhanced-basic attack potential by means of

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data)

with a prior

- reverse-engineering to understand the design and its properties and functions.

7.1.1.8 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 has not been proven or tested. This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, or temperature.

7.1.2 Additional Security Objectives for the TOE

7.1.2.1 OT.Chip_Auth_Proof

"Proof of MRTD's chip authenticity"

The TOE must support the Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Chip Authentication as defined in [TR-03110] the chip is genuine and chip and data page belong to each other as defined in [ICAO-9303].The authenticity proof provided by MRTD's chip shall be protected against attacks with high attack potential.

7.1.2.2 OT.AA_Proof

The TOE must support the Inspection Systems to verify the identity and authenticity of MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [ICAO-9303]. The authenticity proof through AA provided by MRTD's chip shall be protected against attacks with high attack potential.

7.2 Security Objectives for the Operational Environment

7.2.1 Issuing State or Organization

The issuing State or Organization will implement the following security objectives of the TOE environment.

7.2.1.1 OE.MRTD_Manufact

"Protection of the MRTD Manufacturing"

Appropriate functionality testing of the TOE shall be used in phase 4 to 6.

During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

7.2.1.2 OE.MRTD_Delivery

"Protection of the MRTD delivery"

Procedures shall ensure protection of TOE material/information under delivery including the following objectives:

- non-disclosure of any security relevant information,
- identification of the element under delivery,
- meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),
- physical protection to prevent external damage,
- secure storage and handling procedures (including rejected TOE's),
- traceability of TOE during delivery including the following parameters:
  - origin and shipment details,
  - reception, reception acknowledgement,
  - location material/information.

Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non-conformance to this process.

Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.

7.2.1.3 OE.Personalization

"Personalization of logical MRTD"

The issuing State or Organization must ensure that the Personalization Agents acting on behalf of the issuing State or Organization (i) establish the correct identity of the holder and create biographical data for the MRTD, (ii) enroll the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and (iii) personalize the

MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

7.2.1.4 OE.Pass_Auth_Sign

"Authentication of logical MRTD by Signature"

The issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity. The issuing State or Organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [ICAO-9303].

7.2.1.5 OE.BAC-Keys

"Cryptographic quality of Basic Access Control Keys"

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the [ICAO-9303] the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Basic Access Keys from the printed MRZ data with enhanced basic attack potential.

7.2.2 Receiving State or Organization

The receiving State or Organization will implement the following security objectives of the TOE environment.

7.2.2.1 OE.Exam_MRTD

"Examination of the MRTD passport book"

The inspection system of the receiving State or Organization must examine the MRTD presented by the Traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO-9303].

7.2.2.2 OE.Passive_Auth_Verif

"Verification by Passive Authentication" The border control officer of the receiving State uses the inspection system to verify the Traveler as MRTD holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and Organizations must manage the Country Signing Public Key and the Document Signer Public Key maintaining their authenticity and availability in all inspection systems.

7.2.2.3 OE.Prot_Logical_MRTD

"Protection of data from the logical MRTD"

The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD

being under Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems).

7.2.3 Additional Security Objectives for the Operational Environment

7.2.3.1 OE.Auth_MRTD

"MRTD Authentication Key"

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the MRTD's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Chip Authentication Public Key by means of the Document Security Object.

7.2.3.2 OE.Exam_Chip_Auth

"Examination of the chip authenticity"

Additionally to the OE.Exam_MRTD, inspection system performs the Chip Authentication to verify the Authenticity of the presented MRTD's chip.

7.2.3.3 OE.Exam_MRTD_AA

Aditionally to the OE.Exam_MRTD, the inspection systems perform the Active Authentication protocol to verify the Authenticity of the presented MRTD's chip.

7.2.3.4 OE.Activ_Auth_Sign

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the MRTD's Active Authentication Key Pair, (ii) ensure the secrecy of the MRTD's Active Authentication Private Key, sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 and (iii) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Active Authentication Public Key by means of the Document Security Object.

7.3 Security Objectives Rationale

7.3.1 Threats

T.Chip_ID The threat T.Chip_ID "Identification of MRTD's chip" addresses the trace of the MRTD movement by identifying remotely the MRTD's chip through the contactless communication interface. This threat is countered as described by the security objective OT.Identification by Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment OE.BAC-Keys.

T.Skimming The threat T.Skimming "Skimming digital MRZ data or the digital portrait" and T.Eavesdropping "Eavesdropping to the communication between TOE and inspection system" address the reading of the logical MRTD trough the contactless interface or listening the communication between the MRTD's chip and a terminal. This threat is countered by the security objective OT.Data_Conf "Confidentiality of personal data" through Basic Access Control using

sufficiently strong derived keys as required by the security objective for the environment OE.BAC-Keys.

T.Eavesdropping The threat T.Eavesdropping "Eavesdropping to the communication between TOE and inspection system" addresses listening to the communication between the MRTD's chip and a terminal. This threat is countered by the security objective OT.Data_Conf "Confidentiality of personal data" through Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment OE.BAC-Keys "Cryptographic quality of Basic Access Control Keys".

T.Forgery The threat T.Forgery "Forgery of data on MRTD's chip" addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective OT.AC_Pers "Access Control for Personalization of logical MRTD" requires the TOE to limit the write access for the logical MRTD to the trustworthy Personalization Agent (cf. OE.Personalization). The TOE will protect the integrity of the stored logical MRTD according the security objective OT.Data_Int "Integrity of personal data" and OT.Prot_Phys-Tamper "Protection against Physical Tampering". The examination of the presented MRTD passport book according to OE.Exam_MRTD "Examination of the MRTD passport book" shall ensure that passport book does not contain a sensitive contactless chip which may present the complete unchanged logical MRTD. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to OE.Pass_Auth_Sign "Authentication of logical MRTD by Signature" and verified by the inspection system according to OE.Passive_Auth_Verif "Verification by Passive Authentication".

T.Abuse-Func The threat T.Abuse-Func "Abuse of Functionality" addresses attacks using the MRTD's chip as production material for the MRTD and misuse of the functions for personalization in the operational state after delivery to MRTD holder to disclose or to manipulate the logical MRTD. This threat is countered by OT.Prot_Abuse-Func "Protection against Abuse of Functionality". Additionally this objective is supported by the security objective for the TOE environment: OE.Personalization "Personalization of logical MRTD" ensuring that the TOE security functions for the initialization and the personalization are disabled and the security functions for the operational state after delivery to MRTD holder are enabled according to the intended use of the TOE.

T.Information_Leakage The threats T.Information_Leakage "Information Leakage from MRTD's chip" is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objective OT.Prot_Inf_Leak "Protection against Information Leakage".

T.Phys-Tamper The threat T.Phys-Tamper "Physical Tampering" is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objective OT.Prot_Phys-Tamper "Protection against Physical Tampering".

T.Malfunction The threat T.Malfunction "Malfunction due to Environmental Stress" is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objective OT.Prot_Malfunction "Protection against Malfunctions".

T.Counterfeit The threat T.Counterfeit "MRTD's chip" addresses the attack of unauthorized copy or reproduction of the genuine MRTD chip. This attack is thwarted by chip an identification and authenticity proof required by OT.Chip_Auth_Proof "Proof of MRTD's chip authenticity" using a

authentication key pair to be generated by the issuing State or Organization. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by OE.Auth_MRTD "MRTD Authentication Key". According to OE.Exam_Chip_Auth the inspection system has to perform the Chip Authentication Protocol to verify the authenticity of the MRTD's chip. This attack is also thwarted by Active Authentication proving the authenticity of the chip as required by OT.AA_Proof using a authentication key pair to be generated by the issuing State or Organization. OE.Activ_Auth_Sign also covers this threat enabling the possibility of performing an Active Authentication which reinforce the security associated to the communication.

7.3.2 Organisational Security Policies

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

P.Personalization The OSP P.Personalization "Personalization of the MRTD by issuing State or Organization only" addresses the (i) the enrolment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment OE.Personalization "Personalization of logical MRTD", and (ii) the access control for the user data and TSF data as described by the security objective OT.AC_Pers "Access Control for Personalization of logical MRTD". Note the manufacturer equips the TOE with the Personalization Agent Key(s) according to OT.Identification "Identification and Authentication of the TOE". The security objective OT.AC_Pers limits the management of TSF data and management of TSF to the Personalization Agent.

P.Personal_Data The OSP P.Personal_Data "Personal data protection policy" requires the TOE (i) to support the protection of the confidentiality of the logical MRTD by means of the Basic Access Control and (ii) enforce the access control for reading as decided by the issuing State or Organization. This policy is implemented by the security objectives OT.Data_Int "Integrity of personal data" describing the unconditional protection of the integrity of the stored data and during transmission. The security objective OT.Data_Conf "Confidentiality of personal data" describes the protection of the confidentiality.

7.3.3 Assumptions

A.MRTD_Manufact The assumption A.MRTD_Manufact "MRTD manufacturing on phase 4 to 6" is covered by the security objective for the TOE environment OE.MRTD_Manufact "Protection of the MRTD Manufacturing" that requires to use security procedures during all manufacturing steps.

A.MRTD_Delivery The assumption A.MRTD_Delivery "MRTD delivery during phase 4 to 6" is covered by the security objective for the TOE environment OE.MRTD_Delivery "Protection of the MRTD delivery" that requires to use security procedures during delivery steps of the MRTD.

A.Pers_Agent The assumption A.Pers_Agent "Personalization of the MRTD's chip" is covered by the security objective for the TOE environment OE.Personalization "Personalization of logical MRTD"

including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data.

A.Insp_Sys The examination of the MRTD passport book addressed by the assumption A.Insp_Sys "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment OE.Exam_MRTD "Examination of the MRTD passport book". The security objectives for the TOE environment OE.Prot_Logical_MRTD "Protection of data from the logical MRTD will require the Basic Inspection System to implement the Basic Access Control and to protect the logical MRTD data during the transmission and the internal handling.

A.BAC-Keys The assumption is directly covered by the security objective for the TOE environment OE.BAC-Keys "Cryptographic quality of Basic Access Control Keys" ensuring the sufficient key quality to be provided by the issuing State or Organization.

A.Insp_Sys_Chip_Auth The examination of the MRTD passport book addressed by the assumption A.Insp_Sys_Chip_Auth "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment OE.Exam_MRTD "Examination of the MRTD passport book". The security objectives for the TOE environment OE.Prot_Logical_MRTD "Protection of data from the logical MRTD will require the Basic Inspection System to implement the Basic Access Control and to protect the logical MRTD data during the transmission and the internal handling.

It is also covered by the security objectives for the TOE environment OE.Exam_Chip_Auth.

A.Insp_Sys_AA The examination of the MRTD passport book addressed by the assumption A.Insp_Sys_AA "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment OE.Exam_MRTD_AA "Examination of the MRTD passport book".

7.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.Chip_ID	OT.Identification, OE.BAC-Keys	Section 7.3.1
T.Skimming	OT.Data_Conf, OE.BAC-Keys	Section 7.3.1
T.Eavesdropping	OT.Data_Conf, OE.BAC-Keys	Section 7.3.1
T.Forgery	OT.AC_Pers, OT.Data_Int, OT.Prot_Phys-Tamper, OE.Exam_MRTD, OE.Pass_Auth_Sign, OE.Passive_Auth_Verif, OE.Personalization	Section 7.3.1
T.Abuse-Func	OT.Prot_Abuse-Func, OE.Personalization	Section 7.3.1
T.Information_Leakage	OT.Prot_Inf_Leak	Section 7.3.1
T.Phys-Tamper	OT.Prot_Phys-Tamper	Section 7.3.1
T.Malfunction	OT.Prot_Malfunction	Section 7.3.1
T.Counterfeit	OT.Chip_Auth_Proof, OE.Exam_Chip_Auth, OE.Auth_MRTD, OT.AA_Proof, OE.Activ_Auth_Sign	Section 7.3.1

Table 17 Threats and Security Objectives - Coverage

Security Objectives	Threats
OT.AC_Pers	T.Forgery
OT.Data_Int	T.Forgery
OT.Data_Conf	T.Skimming, T.Eavesdropping
OT.Identification	T.Chip_ID
OT.Prot_Abuse-Func	T.Abuse-Func
OT.Prot_Inf_Leak	T.Information_Leakage
OT.Prot_Phys-Tamper	T.Forgery, T.Phys-Tamper
OT.Prot_Malfunction	T.Malfunction
OT.Chip_Auth_Proof	T.Counterfeit
OT.AA_Proof	T.Counterfeit
OE.MRTD_Manufact	
OE.MRTD_Delivery	
OE.Personalization	T.Forgery, T.Abuse-Func
OE.Pass_Auth_Sign	T.Forgery
OE.BAC-Keys	T.Chip_ID, T.Skimming, T.Eavesdropping
OE.Auth_MRTD	T.Counterfeit
OE.Exam_MRTD	T.Forgery
OE.Exam_Chip_Auth	T.Counterfeit
OE.Passive_Auth_Verif	T.Forgery
OE.Prot_Logical_MRTD	
OE.Exam_MRTD_AA	
OE.Activ_Auth_Sign	T.Counterfeit

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

Organisational Security Policies	Security Objectives	Rationale
P.Manufact	OT.Identification	Section 7.3.2
P.Personalization	OE.Personalization, OT.AC_Pers, OT.Identification	Section 7.3.2
P.Personal_Data	OT.Data_Int, OT.Data_Conf	Section 7.3.2

Table 19 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies
OT.AC_Pers	P.Personalization

OT.Data_Int	P.Personal_Data
OT.Data_Conf	P.Personal_Data
OT.Identification	P.Manufact, P.Personalization
OT.Prot_Abuse-Func	
OT.Prot_Inf_Leak	
OT.Prot_Phys-Tamper	
OT.Prot_Malfunction	
OT.Chip_Auth_Proof	
OT.AA_Proof	
OE.MRTD_Manufact	
OE.MRTD_Delivery	
OE.Personalization	P.Personalization
OE.Pass_Auth_Sign	
OE.BAC-Keys	
OE.Auth_MRTD	
OE.Exam_MRTD	
OE.Exam_Chip_Auth	
OE.Passive_Auth_Verif	
OE.Prot_Logical_MRTD	
OE.Exam_MRTD_AA	
OE.Activ_Auth_Sign	

Table 20 **Security Objectives and OSPs - Coverage**

Assumptions	Security Objectives for the Operational Environment	Rationale
A.MRTD_Manufact	OE.MRTD_Manufact	Section 7.3.3
A.MRTD_Delivery	OE.MRTD_Delivery	Section 7.3.3
A.Pers_Agent	OE.Personalization	Section 7.3.3
A.Insp_Sys	OE.Exam_MRTD, OE.Prot_Logical_MRTD	Section 7.3.3
A.BAC-Keys	OE.BAC-Keys	Section 7.3.3
A.Insp_Sys_Chip_Auth	OE.Exam_Chip_Auth, OE.Exam_MRTD, OE.Prot_Logical_MRTD	Section 7.3.3
A.Insp_Sys_AA	OE.Exam_MRTD_AA	Section 7.3.3

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

Security Objectives for the Operational Environment	Assumptions
OE.MRTD_Manufact	A.MRTD_Manufact
OE.MRTD_Delivery	A.MRTD_Delivery
OE.Personalization	A.Pers_Agent
OE.Pass_Auth_Sign	
OE.BAC-Keys	A.BAC-Keys
OE.Auth_MRTD	
OE.Exam_MRTD	A.Insp_Sys, A.Insp_Sys_Chip_Auth
OE.Exam_Chip_Auth	A.Insp_Sys_Chip_Auth
OE.Passive_Auth_Verif	
OE.Prot_Logical_MRTD	A.Insp_Sys, A.Insp_Sys_Chip_Auth
OE.Exam_MRTD_AA	A.Insp_Sys_AA
OE.Activ_Auth_Sign	

Table 22 Security Objectives for the Operational Environment and Assumptions - Coverage

8 Extended Requirements

8.1 Extended Families

8.1.1 Extended Family FPT_EMS - TOE Emanation

8.1.1.1 Description

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

8.1.1.2 Extended Components

Extended Component FPT_EMS.1

Description

This family defines requirements to mitigate intelligible emanations. FPT_EMS.1 TOE Emanation has two constituents: - FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data. - FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Definition

FPT_EMS.1 - TOE Emanation

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

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

8.1.2 Extended Family FIA_API - Authentication Proof of Identity

8.1.2.1 Description

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

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

8.1.2.2 Extended Components

Extended Component FIA_API.1

Description

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

Definition

FIA_API.1 - Authentication Proof of Identity

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

8.1.3 Extended Family FMT_LIM - Limited capabilities

8.1.3.1 Description

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

8.1.3.2 Extended Components

Extended Component FMT_LIM.2

Definition

FMT_LIM.2 - Limited capabilities

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

Extended Component FMT_LIM.1

Definition

FMT_LIM.1 - Limited capabilities

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

8.1.4 Extended Family FAU_SAS - Audit data storage

8.1.4.1 Description

To describe the security functional requirements of the TOE, the family FAU_SAS of the class FAU (Security audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records. The family 'Audit data storage (FAU_SAS)' is specified as follows:

8.1.4.2 Extended Components

Extended Component FAU_SAS.1

Description

Requires the TOE to provide the possibility to store audit data.

Definition

FAU_SAS.1 - Audit storage

FAU_SAS.1.1 The TSF shall provide **[assignment: authorised users]** with the capability to store **[assignment: list of audit information]** in the audit records.

8.1.5 Extended Family FCS_RND - Generation of random numbers

8.1.5.1 Description

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

8.1.5.2 Extended Components

Extended Component FCS_RND.1

Description

Generation of random numbers requires that random numbers meet a defined quality metric.

Definition

FCS_RND.1 - Quality metric for random numbers

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

9 Security Requirements

9.1 Security Functional Requirements

9.1.1 Class FAU Security Audit

FAU_SAS.1 Audit storage

FAU_SAS.1.1 The TSF shall provide **the Manufacturer** with the capability to store **the IC Identification Data** in the audit records.

9.1.2 Class FCS Cryptographic Support

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 **Document Basic Access Key Derivation Algorithm** and specified cryptographic key sizes **112 bit** that meet the following: **[ICAO-9303], normative appendix 5**.

FCS_CKM.1/AA Cryptographic key generation

FCS_CKM.1.1/AA 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
ECC	**192, 224, 256, 320, 384, 512 and 521**	**[IEEE_1363]**
RSA	**1536, 1792, 2048, 2560, 3072, 3584 and 4096**	**[ANSI_X9.31]**

FCS_CKM.1/CA Cryptographic key generation

FCS_CKM.1.1/CA 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
Chip Authentication Protocol Version 1 [TR-03110-1] based on the ECDH protocol compliant to [TR-03111] in combination with 112 bits 3DES or 128, 192 or 256 bits AES	**192, 224, 256, 320, 384, 512 and 521 bits**	**[TR-03111]**
Chip Authentication Protocol Version 1 [TR-03110-1] based on the DH protocol compliant to [TR-03110-1] in combination with 112 bits 3DES or 128, 192 or 256 bits AES	**2048 bits**	**[TR-03110-1] and [RSA-PKCS#3]**

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **zeroisation** that meets the following: **none**.

FCS_COP.1/SHA Cryptographic operation

FCS_COP.1.1/SHA The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1** and cryptographic key sizes **none** that meet the following: **[FIPS_180_3]**.

FCS_COP.1/ENC Cryptographic operation

FCS_COP.1.1/ENC The TSF shall perform **secure messaging (BAC) – encryption and decryption** in accordance with a specified cryptographic algorithm **Triple-DES in CBC mode** and cryptographic key sizes **112 bit** that meet the following: **[FIPS_46_3] and [ICAO-9303]; normative appendix 5, A5.3 [ICAO-9303]**.

FCS_COP.1/AUTH Cryptographic operation

FCS_COP.1.1/AUTH The TSF shall perform **symmetric authentication – encryption and decryption** in accordance with a specified cryptographic algorithm **Triple-DES** and cryptographic key sizes **112 bit** that meet the following: **[FIPS_46_3]**.

FCS_COP.1/MAC Cryptographic operation

FCS_COP.1.1/MAC The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic algorithm **Retail MAC** and cryptographic key sizes **112 bit** that meet the following: **[ISO_9797_1] (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)**.

FCS_COP.1/CA_SHA Cryptographic operation

FCS_COP.1.1/CA_SHA The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1 and SHA-256** and cryptographic key sizes **none** that meet the following: **[FIPS_180_3]**.

FCS_COP.1/CA_ENC Cryptographic operation

FCS_COP.1.1/CA_ENC The TSF shall perform **secure messaging – encryption and decryption** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key Size(s)]** that meet the following: **[Standard]**

Algorithm	Key Size(s)	Standard
Triple-DES in CBC mode	**112 bit**	**[FIPS_46_3]**
AES in CBC mode	**128, 192 and 256 bit**	**[FIPS_197]**

FCS_COP.1/CA_MAC Cryptographic operation

FCS_COP.1.1/CA_MAC The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key Size(s)]** that meet the following: **[Standard]**

Algorithm	Key Size(s)	Standard
Retail MAC	**112 bit**	**[ISO_9797_1]**
AES CMAC	**128, 192 and 256 bit**	**[NIST_800_38B]**

FCS_COP.1/AA Cryptographic operation

FCS_COP.1.1/AA 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: **[standard]**

Cryptographic Operation	Cryptographic Algorithm	Cryptographic Key Sizes(bits)	Standard
Digital Signature Creation	**ECDSA**	**192 to 521 over prime field curves**	**[ISO_9796-2], [RSA-PKCS#3], [FIPS_180_2] and [X.92]**
Digital Signature Creation	**RSA signature**	**1536, 1792, 2048, 2560, 3072, 3584 and 4096**	**[ISO_9796-2]**

FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet **the deterministic random number generation specified by FCS_RNG.1 Quality metric for random numbers of [PTF-ST].**

9.1.3 Class FIA Identification and Authentication

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

- **to read the Initialization Data in Stage 2 "Production",**
- **to read the random identifier in Stage 3 "Preparation",**
- **to read the random identifier in Stage 4 "Operational"**

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_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

- **to read the Initialization Data in Stage 2 "Production",**
- **to read the random identifier in Stage 3 "Preparation",**

- **to read the random identifier in Stage 4 "Operational"**

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.

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to

- **Basic Access Control Authentication Mechanism,**
- **Authentication Mechanisms based on:**
  - **Triple-DES.**

FIA_UAU.5/BAC Multiple authentication mechanisms

FIA_UAU.5.1/BAC The TSF shall provide

- **Basic Access Control Authentication Mechanism,**
- **Symmetric Authentication Mechanism based on Triple-DES**

to support user authentication.

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

- **The TOE accepts the authentication attempt as Personalization Agent by one of the following mechanism(s) the Symmetric Authentication Mechanism with the Personalization Agent Key,**
- **The TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.**

FIA_UAU.5/CA Multiple authentication mechanisms

FIA_UAU.5.1/CA The TSF shall provide

- **Secure messaging in MAC-ENC mode,**
- **Key agreement protocol DH and ECDH during Chip Authentication Protocol v.1 according to [TR-03110]**

to support user authentication.

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

- **After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of**

secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1.

FIA_UAU.6/BAC Re-authenticating

FIA_UAU.6.1/BAC The TSF shall re-authenticate the user under the conditions **each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism.**

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 successful run of the Chip Authentication Protocol shall be verified as being sent by the inspection system (GIS).**

FIA_AFL.1/BAC Authentication failure handling

FIA_AFL.1.1/BAC The TSF shall detect when **an administrator configurable positive integer within range of acceptable values 0 to 255 consecutive** unsuccessful authentication attempts occur related to **BAC authentication protocol.**

FIA_AFL.1.2/BAC When the defined number of unsuccessful authentication attempts has been **met and surpassed**, the TSF shall **wait for an increasing time during the Mutual Authentication**.

FIA_API.1/CA Authentication Proof of Identity

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

FIA_API.1/AA Authentication Proof of Identity

FIA_API.1.1/AA The TSF shall provide a **Active Authentication** to prove the identity of the **TOE**.

9.1.4 Class FDP User Data Protection

FDP_ACC.1/BAC Subset access control

FDP_ACC.1.1/BAC The TSF shall enforce the **Basic Access Control SFP** on **terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD.**

FDP_ACC.1/CA Subset access control

FDP_ACC.1.1/CA The TSF shall enforce the **CA Access Control SFP** on **terminals gaining read and modify access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD.**

FDP_ACF.1/BAC Security attribute based access control

FDP_ACF.1.1/BAC The TSF shall enforce the **Basic Access Control SFP** to objects based on the following:

- **Subjects:**
  - **Personalization Agent,**
  - **Basic Inspection System,**
  - **Terminal,**
- **Objects:**
  - **data EF.DG1 to EF.DG16 of the logical MRTD,**
  - **data in EF.COM,**
  - **data in EF.SOD,**
- **Security attributes:**
  - **authentication status of terminals.**

FDP_ACF.1.2/BAC The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **the successfully authenticated Personalization Agent is allowed to write and read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,**
- **the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD.**

FDP_ACF.1.3/BAC The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/BAC The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- **Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,**

- **Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD,**
- **The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4.**

FDP_ACF.1/CA Security attribute based access control

FDP_ACF.1.1/CA The TSF shall enforce the **CA Control SFP** to objects based on the following:

- **Subjects:**
  - **General Inspection System,**
  - **Terminal,**
- **Objects:**
  - **data EF.DG1 to EF.DG16 of the logical MRTD,**
  - **data in EF.COM,**
  - **data in EF.SOD,**
- **Security attributes**
  - **authentication status of terminals.**

FDP_ACF.1.2/CA The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **the successfully authenticated General Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD.**

FDP_ACF.1.3/CA The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/CA The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- **Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,**
- **Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD,**
- **The General Inspection System is not allowed to read the data in EF.DG3 and EF.DG4.**

FDP_UCT.1/BAC Basic data exchange confidentiality

FDP_UCT.1.1/BAC The TSF shall enforce the **Basic Access Control SFP** to **transmit and receive** user data in a manner protected from unauthorised disclosure.

FDP_UCT.1/CA Basic data exchange confidentiality

FDP_UCT.1.1/CA [Editorially Refined] The TSF shall enforce the **CA Access Control SFP** to **transmit and receive** user data in a manner protected from unauthorised disclosure **after Chip Authentication**.

FDP_UIT.1/BAC Data exchange integrity

FDP_UIT.1.1/BAC The TSF shall enforce the **Basic Access Control SFP** to **transmit and receive** user data in a manner protected from **modification, deletion, insertion and replay** errors.

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

FDP_UIT.1/CA Data exchange integrity

FDP_UIT.1.1/CA [Editorially Refined] The TSF shall enforce the **CA Access Control SFP** to **transmit and receive** user data in a manner protected from **modification, deletion, insertion and replay** errors **after Chip Authentication protocol**.

FDP_UIT.1.2/CA [Editorially Refined] The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred **after Chip Authentication protocol.**

9.1.5 Class FMT Security Management

FMT_MOF.1/PROT Management of security functions behaviour

FMT_MOF.1.1/PROT The TSF shall restrict the ability to **enable** the functions

- **Chip Authentication,**

to **the Manufacturer**.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- **Initialization**
- **Pre-personalization**
- **Personalization**
- **Chip Authentication protocol.**

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- **Manufacturer**
- **Personalization Agent**
- **Basic Inspection System**
- **General Inspection System.**

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application Note:

This SFR also applies to the refinement of the role Manufacturer.

FMT_LIM.1 Limited capabilities

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced

Deploying Test Features after TOE Delivery does not allow

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

FMT_LIM.2 Limited availability

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced

Deploying Test Features after TOE Delivery does not allow

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

FMT_MTD.1/INI_ENA Management of TSF data

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to **write** the **Initialization Data and Pre-personalization 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 **disable read access for users to** the **Initialization Data** to **the Personalization Agent**.

FMT_MTD.1/KEY_WRITE Management of TSF data

FMT_MTD.1.1/KEY_WRITE The TSF shall restrict the ability to **write** the **Document Basic Access Keys** to **the Personalization Agent**.

FMT_MTD.1/KEY_READ Management of TSF data

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to **read** the **Document Basic Access Keys and Personalization Agent Keys** to **none**.

FMT_MTD.1/CAPK Management of TSF data

FMT_MTD.1.1/CAPK The TSF shall restrict the ability to **load or generate** the **Chip Authentication Keys** to **the Personalization Agent**.

FMT_MTD.1/AAPK Management of TSF data

FMT_MTD.1.1/AAPK The TSF shall restrict the ability to **load or generate** the **Active Authentication Keys** to **the Personalization Agent**.

FMT_MTD.1/AA_CA_KEY_READ Management of TSF data

FMT_MTD.1.1/AA_CA_KEY_READ The TSF shall restrict the ability to **read** the **Active Authentication and Chip Authentication Private Key** to **none**.

9.1.6 Class FPT Protection of the Security Functions

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **power variations, timing variations and electromagnetic radiations during command execution** in excess of **non useful information** enabling access to **Personalization Agent Keys** and

- **Chip Authentication Private Key,**

- **Active Authentication: Private Key (AAK).**

FPT_EMS.1.2 The TSF shall ensure **unauthorized users** are unable to use the following interface **smart card circuit contacts** to gain access to **Personalization Agent Keys** and

- **Chip Authentication Private Key,**
- **Active Authentication: Private Key (AAK).**

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:

- **Exposure to out-of-range operating conditions where therefore a malfunction could occur,**
- **failure detected by TSF according to FPT_TST.1.**

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **at the conditions**

- **At reset**

to demonstrate the correct operation of **the TSF**.

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

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

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.

9.2 Security Assurance Requirements

The assurance components for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 4 (EAL4) and augmented by taking the following component: ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, and ATE_DPT.3.

9.2.1 ADV Development

9.2.1.1 ADV_ARC Security Architecture

ADV_ARC.1 Security architecture description

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

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

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

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

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

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

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

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

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.1.2 ADV_FSP Functional specification

ADV_FSP.5 Complete semi-formal functional specification with additional error information

ADV_FSP.5.1D The developer shall provide a functional specification.

ADV_FSP.5.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.5.1C The functional specification shall completely represent the TSF.

ADV_FSP.5.2C The functional specification shall describe the TSFI using a semi-formal style.

ADV_FSP.5.3C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.5.4C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.5.5C The functional specification shall describe all actions associated with each TSFI.

ADV_FSP.5.6C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP.5.7C The functional specification shall describe all error messages that do not result from an invocation of a TSFI.

ADV_FSP.5.8C The functional specification shall provide a rationale for each error message contained in the TSF implementation yet does not result from an invocation of a TSFI.

ADV_FSP.5.9C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.5.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.5.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

9.2.1.3 ADV_IMP Implementation representation

ADV_IMP.1 Implementation representation of the TSF

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

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

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

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

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

ADV_IMP.1.1E The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

9.2.1.4 ADV_TDS TOE design

ADV_TDS.4 Semiformal modular design

ADV_TDS.4.1D The developer shall provide the design of the TOE.

ADV_TDS.4.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.4.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.4.2C The design shall describe the TSF in terms of modules, designating each module as SFR-enforcing, SFR-supporting, or SFR-non-interfering.

ADV_TDS.4.3C The design shall identify all subsystems of the TSF.

ADV_TDS.4.4C The design shall provide a semiformal description of each subsystem of the TSF, supported by informal, explanatory text where appropriate.

ADV_TDS.4.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.4.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

ADV_TDS.4.7C The design shall describe each SFR-enforcing and SFR-supporting module in terms of its purpose and relationship with other modules.

ADV_TDS.4.8C The design shall describe each SFR-enforcing and SFR-supporting module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing or SFR-supporting modules.

ADV_TDS.4.9C The design shall describe each SFR-non-interfering module in terms of its purpose and interaction with other modules.

ADV_TDS.4.10C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

ADV_TDS.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.4.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

9.2.1.5 ADV_INT TSF internals

ADV_INT.2 Well-structured internals

ADV_INT.2.1D The developer shall design and implement the entire TSF such that it has well-structured internals.

ADV_INT.2.2D The developer shall provide an internals description and justification.

ADV_INT.2.1C The justification shall describe the characteristics used to judge the meaning of ``well-structured''.

ADV_INT.2.2C The TSF internals description shall demonstrate that the entire TSF is well-structured.

ADV_INT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_INT.2.2E The evaluator shall perform an internals analysis on the TSF.

9.2.2 AGD Guidance documents

9.2.2.1 AGD_OPE Operational user guidance

AGD_OPE.1 Operational user guidance

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

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

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

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

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

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

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

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

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.2.2 AGD_PRE Preparative procedures

AGD_PRE.1 Preparative procedures

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

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

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

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

9.2.3 ALC Life-cycle support

9.2.3.1 ALC_CMC CM capabilities

ALC_CMC.4 Production support, acceptance procedures and automation

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

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

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

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

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

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

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

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

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

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

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

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

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

ALC_CMC.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.3.2 ALC_CMS CM scope

ALC_CMS.5 Development tools CM coverage

ALC_CMS.5.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.5.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.

ALC_CMS.5.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.5.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_CMS.5.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.3.3 ALC_DEL Delivery

ALC_DEL.1 Delivery procedures

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

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

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

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.3.4 ALC_DVS Development security

ALC_DVS.2 Sufficiency of security measures

ALC_DVS.2.1D The developer shall produce and provide development security documentation.

ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.2.2C The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

ALC_DVS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.2.2E The evaluator shall confirm that the security measures are being applied.

9.2.3.5 ALC_LCD Life-cycle definition

ALC_LCD.1 Developer defined life-cycle model

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

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

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

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

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.3.6 ALC_TAT Tools and techniques

ALC_TAT.2 Compliance with implementation standards

ALC_TAT.2.1D The developer shall provide the documentation identifying each development tool being used for the TOE.

ALC_TAT.2.2D The developer shall document and provide the selected implementation-dependent options of each development tool.

ALC_TAT.2.3D The developer shall describe and provide the implementation standards that are being applied by the developer.

ALC_TAT.2.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.2.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.2.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

ALC_TAT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_TAT.2.2E The evaluator shall confirm that the implementation standards have been applied.

9.2.4 ASE Security Target evaluation

9.2.4.1 ASE_CCL Conformance claims

ASE_CCL.1 Conformance claims

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

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

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

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

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

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

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

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

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

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

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

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

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.4.2 ASE_ECD Extended components definition

ASE_ECD.1 Extended components definition

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

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

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

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

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

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

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

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

9.2.4.3 ASE_INT ST introduction

ASE_INT.1 ST introduction

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

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

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

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

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

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

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

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

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

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

9.2.4.4 ASE_OBJ Security objectives

ASE_OBJ.2 Security objectives

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

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

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

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

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

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

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

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

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.4.5 ASE_REQ Security requirements

ASE_REQ.2 Derived security requirements

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

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

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

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

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

ASE_REQ.2.4C All operations shall be performed correctly.

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

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

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

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

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

ASE_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.4.6 ASE_SPD Security problem definition

ASE_SPD.1 Security problem definition

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

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

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

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

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

ASE_SPD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.4.7 ASE_TSS TOE summary specification

ASE_TSS.1 TOE summary specification

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

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

ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

9.2.5 ATE Tests

9.2.5.1 ATE_COV Coverage

ATE_COV.2 Analysis of coverage

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

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

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

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.5.2 ATE_DPT Depth

ATE_DPT.3 Testing: modular design

ATE_DPT.3.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.3.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and modules in the TOE design.

ATE_DPT.3.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

ATE_DPT.3.3C The analysis of the depth of testing shall demonstrate that all TSF modules in the TOE design have been tested.

ATE_DPT.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.5.3 ATE_FUN Functional tests

ATE_FUN.1 Functional testing

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

ATE_FUN.1.2D The developer shall provide test documentation.

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

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

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

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

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2.5.4 ATE_IND Independent testing

ATE_IND.2 Independent testing - sample

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

9.2.6 AVA Vulnerability assessment

9.2.6.1 AVA_VAN Vulnerability analysis

AVA_VAN.3 Focused vulnerability analysis

AVA_VAN.3.1D The developer shall provide the TOE for testing.

AVA_VAN.3.1C The TOE shall be suitable for testing.

AVA_VAN.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.3.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.3.3E The evaluator shall perform an independent, focused vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA_VAN.3.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Enhanced-Basic attack potential.

9.3 Security Requirements Rationale

9.3.1 Objectives

9.3.1.1 Security Objectives for the TOE

OT.AC_Pers The security objective OT.AC_Pers "Access Control for Personalization of logical MRTD" addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR FDP_ACC.1/BAC and FDP_ACF.1/BAC as follows: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD.

The following paragraph is extracted from [PP_BAC] and has been refined according to the technical characteristics of this TOE. The refinement is right after.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated either by using the BAC mechanism (FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC) with the personalization key or for reasons of interoperability with the [PP_EAC] by using the symmetric authentication mechanism (FCS_COP.1/AUTH)6.

In case of using the BAC mechanism the SFR FIA_UAU.6/BAC describes the re-authentication and FDP_UCT.1/BAC and FDP_UIT.1/BAC the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC for the ENC_MAC_Mode.

Note: As BAC mechanism is not supported for the authentication of the terminal as Personalization Agent, the following two paragraphs have been added to demonstrate that symmetric authentication used in Personalization phase fulfills the OT.AC_Pers.

The authentication of the terminal as Personalization Agent is performed by TSF according to SFR FIA_UAU.4 and FIA_UAU.5/BAC. The Personalization Agent can be authenticated by using the symmetric authentication mechanism (FCS_COP.1/AUTH) with the personalization key.

The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization) setting the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data. The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensure together with the SFR FCS_CKM.4, FPT_EMS.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

The following parts are added to integrate the personalization of the different keys in the OT.AC_Pers.

Only the Personalization Agent is allowed to set the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE. The SFR FMT_MTD.1/KEY_READ prevents read access to the Document Basic Access Keys and ensure together with the SFR FCS_CKM.4, FPT_EMS.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

Only the Personalization Agent is allowed to set the Chip Authentication Private Key according to the SFR FMT_MTD.1/CAPK and the Active Authentication Private Key according to FMT_MTD.1/AAPK. The SFR FMT_MTD.1/AA_CA_KEY_READ prevents read access to the Chip Authentication Private Key and Active Authentication Private Key and ensure together with the SFR FCS_CKM.4, FPT_EMS.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

OT.Data_Int The security objective OT.Data_Int "Integrity of personal data" requires the TOE to protect the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFRs (FDP_ACC.1/BAC, FDP_ACC.1/CA) and (FDP_ACF.1/BAC, FDP_ACF.1/CA) in the same way: only the Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2/BAC, rule 1) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4/BAC). The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR FIA_UAU.4, FIA_UAU.5/BAC and FIA_UAU.6/BAC using FCS_COP.1/AUTH.

The security objective OT.Data_Int "Integrity of personal data" requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data by means of the BAC mechanism. The SFR FIA_UAU.6/BAC, FDP_UCT.1/BAC and FDP_UIT.1/BAC requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FMT_MTD.1/KEY_WRITE requires the Personalization Agent to establish the Document Basic Access Keys in a way that they cannot be read by anyone in accordance to FMT_MTD.1/KEY_READ.

The following part is added to integrate the Manufacturing and Personalization phases in the OT_Data_Int.

The following part is added to integrate the Chip Authentication mechanism in the coverage of the OT.Data_Int.

The inspection system is also able to detect any modification of the transmitted logical MRTD data by means of the Chip Authentication mechanism. The SFR FIA_UAU.6/CA, FDP_UCT.1/CA and FDP_UIT.1/CA requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/CA FCS_COP.1/CA_SHA, FCS_RND.1 (for key generation), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode. The SFR FMT_MTD.1/CAPK requires the Personalization Agent to establish the Chip Authentication Private Key in a way that it cannot be read by anyone in accordance to FMT_MTD.1/AA_CA_KEY_READ. FCS_CKM.4 enforces the destruction of Secure Messaging session keys.

OT.Data_Conf The security objective OT.Data_Conf "Confidentiality of personal data" requires the TOE to ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. In case of failed authentication attempts FIA_AFL.1/BAC enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The read access to the logical MRTD data is defined by the FDP_ACC.1/BAC and FDP_ACF.1/BAC along with FDP_ACF.1/CA and FDP_ACC.1/CA: the successful authenticated Personalization Agent is allowed to read the data of the logical MRTD (EF.DG1 to EF.DG16). The successful authenticated Basic Inspection System is allowed to read the data of the logical MRTD (EF.DG1, EF.DG2 and EF.DG5 to EF.DG16). The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys).

The SFR FIA_UAU.4 prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5/BAC enforces the TOE to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Moreover, the SFR FIA_UAU.6/BAC requests secure messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism

which includes the protection of the transmitted data in ENC_MAC_Mode by means of the cryptographic functions according to FCS_COP.1/ENC and FCS_COP.1/MAC (cf. the SFR FDP_UCT.1/BAC and FDP_UIT.1/BAC). (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA and FCS_RND.1 establish the key management for the secure messaging keys. The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.

The following part is added to integrate the Manufacturing and Personalization phases in the OT_Data_Conf.

The following parts are added to integrate the Chip Authentication mechanism and the Symmetric Authentication mechanism used in Personalization phase in the coverage of the OT.Data_Conf.

The SFR FIA_UAU.5/CA enforces the TOE to accept only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism. Moreover, the SFR FIA_UAU.6/CA requests secure messaging after successful authentication of the chip which includes the protection of the transmitted data in ENC_MAC_Mode by means of the cryptographic functions according to FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (cf. the SFR FDP_UCT.1/CA and FDP_UIT.1/CA). (for key generation), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode. The SFR FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/CA_SHA and FCS_RND.1 establish the key management for the secure messaging keys. The SFR FMT_MTD.1/CAPK addresses the key management and FMT_MTD.1/AA_CA_KEY_READ prevents reading of the Chip Authentication Private Key.

OT.Identification The security objective OT.Identification "Identification and Authentication of the TOE" address the storage of the IC Identification Data uniquely identifying the MRTD's chip in its non-volatile memory. This will be ensured by TSF according to SFR FAU_SAS.1.

Furthermore, the TOE shall identify itself only to a successful authenticated Basic Inspection System in Phase 4 "Operational Use". The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 "Operational Use" violates the security objective OT.Identification. The SFR FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the MRTD's chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt. In case of failed authentication attempts FIA_AFL.1/BAC enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

OT.Prot_Abuse-Func The security objective OT.Prot_Abuse-Func "Protection against Abuse of Functionality" is ensured by the SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other features which may not be used after TOE Delivery.

OT.Prot_Inf_Leak The security objective OT.Prot_Inf_Leak "Protection against Information Leakage" requires the TOE to protect confidential TSF data stored and/or processed in the MRTD's chip against disclosure

- 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, which is addressed by the SFR FPT_EMS.1,
- by forcing a malfunction of the TOE, which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE, which is addressed by the SFR FPT_PHP.3.

OT.Prot_Phys-Tamper The security objective OT.Prot_Phys-Tamper "Protection against Physical Tampering" is covered by the SFR FPT_PHP.3.

OT.Prot_Malfunction The security objective OT.Prot_Malfunction "Protection against Malfunctions" is covered by (i) the SFR FPT_TST.1 which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, and (ii) the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

OT.Chip_Auth_Proof The security objective OT.Chip_Auth_Proof "Proof of MRTD's chip authenticity" is ensured by the Chip Authentication Protocol activated by FMT_MOF.1/PROT and provided by FIA_API.1/CA proving the genuineness of the TOE. The Chip Authentication Protocol defined by FCS_CKM.1/CA is performed using a TOE internally stored confidential private key. Confidentiality of this key is ensured by FMT_MTD.1/CAPK and FMT_MTD.1/AA_CA_KEY_READ. The Chip Authentication Protocol [TR-03110] requires additional TSF according to FCS_COP.1/CA_SHA (for the derivation of the session keys) using FCS_RND.1, FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging).

OT.AA_Proof The security objective OT.AA_Proof is ensured by the Active Authentication Protocol as defined in FIA_API.1/AA. The FCS_CKM.1/AA provides key generation for Active Authentication. The Active Authentication relies on FCS_COP.1/AA and FCS_RND.1. It is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/AAPK. It ensures that the Active Authentication Keys cannot be read as per FMT_MTD.1/AA_CA_KEY_READ.

9.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
OT.AC_Pers	FCS_CKM.4, FCS_COP.1/AUTH, FCS_RND.1, FIA_UAU.4, FIA_UAU.5/BAC, FDP_ACC.1/BAC, FDP_ACF.1/BAC, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ, FMT_MTD.1/CAPK, FMT_MTD.1/AA_CA_KEY_READ, FPT_EMS.1, FPT_FLS.1, FPT_PHP.3, FCS_COP.1/SHA, FCS_CKM.1, FIA_UAU.6/BAC, FDP_UCT.1/BAC, FDP_UIT.1/BAC, FCS_COP.1/ENC, FCS_COP.1/MAC, FMT_MTD.1/AAPK	Section 9.3.1
OT.Data_Int	FCS_CKM.1, FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/MAC, FCS_COP.1/CA_SHA, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FIA_UAU.4, FIA_UAU.5/BAC, FIA_UAU.6/BAC, FIA_UAU.6/CA, FDP_ACC.1/BAC, FDP_ACF.1/BAC, FDP_UCT.1/BAC, FDP_UCT.1/CA, FDP_UIT.1/BAC, FDP_UIT.1/CA, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ, FMT_MTD.1/CAPK, FMT_MTD.1/AA_CA_KEY_READ, FDP_ACC.1/CA, FDP_ACF.1/CA, FCS_RND.1	Section 9.3.1
OT.Data_Conf	FCS_CKM.1, FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/MAC, FCS_COP.1/CA_SHA, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_RND.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5/BAC, FIA_UAU.5/CA, FIA_UAU.6/BAC, FIA_UAU.6/CA,	Section 9.3.1

	FIA_AFL.1/BAC, FDP_ACC.1/BAC, FDP_ACF.1/BAC, FDP_UCT.1/BAC, FDP_UCT.1/CA, FDP_UIT.1/BAC, FDP_UIT.1/CA, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ, FMT_MTD.1/CAPK, FMT_MTD.1/AA_CA_KEY_READ, FDP_ACC.1/CA, FDP_ACF.1/CA	
OT.Identification	FAU_SAS.1, FIA_UID.1, FIA_UAU.1, FIA_AFL.1/BAC, 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_EMS.1, FPT_FLS.1, FPT_TST.1, FPT_PHP.3	Section 9.3.1
OT.Prot_Phys-Tamper	FPT_PHP.3	Section 9.3.1
OT.Prot_Malfunction	FPT_FLS.1, FPT_TST.1	Section 9.3.1
OT.Chip_Auth_Proof	FCS_CKM.1/CA, FCS_COP.1/CA_SHA, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_RND.1, FIA_API.1/CA, FMT_MTD.1/CAPK, FMT_MTD.1/AA_CA_KEY_READ, FMT_MOF.1/PROT	Section 9.3.1
OT.AA_Proof	FCS_COP.1/AA, FCS_RND.1, FMT_MTD.1/AAPK, FCS_CKM.1/AA, FIA_API.1/AA, FMT_MTD.1/AA_CA_KEY_READ	Section 9.3.1

Table 23 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives
FAU_SAS.1	OT.Identification
FCS_CKM.1	OT.AC_Pers, OT.Data_Int, OT.Data_Conf
FCS_CKM.1/AA	OT.AA_Proof
FCS_CKM.1/CA	OT.Data_Int, OT.Data_Conf, OT.Chip_Auth_Proof
FCS_CKM.4	OT.AC_Pers, OT.Data_Int, OT.Data_Conf
FCS_COP.1/SHA	OT.AC_Pers, OT.Data_Int, OT.Data_Conf
FCS_COP.1/ENC	OT.AC_Pers, OT.Data_Int, OT.Data_Conf
FCS_COP.1/AUTH	OT.AC_Pers, OT.Data_Int
FCS_COP.1/MAC	OT.AC_Pers, OT.Data_Int, OT.Data_Conf
FCS_COP.1/CA_SHA	OT.Data_Int, OT.Data_Conf, OT.Chip_Auth_Proof
FCS_COP.1/CA_ENC	OT.Data_Int, OT.Data_Conf, OT.Chip_Auth_Proof
FCS_COP.1/CA_MAC	OT.Data_Int, OT.Data_Conf, OT.Chip_Auth_Proof
FCS_COP.1/AA	OT.AA_Proof
FCS_RND.1	OT.AC_Pers, OT.Data_Int, OT.Data_Conf, OT.Chip_Auth_Proof, OT.AA_Proof
FIA_UID.1	OT.Data_Conf, OT.Identification
FIA_UAU.1	OT.Data_Conf, OT.Identification

FIA_UAU.4	OT.AC_Pers, OT.Data_Int, OT.Data_Conf
FIA_UAU.5/BAC	OT.AC_Pers, OT.Data_Int, OT.Data_Conf
FIA_UAU.5/CA	OT.Data_Conf
FIA_UAU.6/BAC	OT.AC_Pers, OT.Data_Int, OT.Data_Conf
FIA_UAU.6/CA	OT.Data_Int, OT.Data_Conf
FIA_AFL.1/BAC	OT.Data_Conf, OT.Identification
FIA_API.1/CA	OT.Chip_Auth_Proof
FIA_API.1/AA	OT.AA_Proof
FDP_ACC.1/BAC	OT.AC_Pers, OT.Data_Int, OT.Data_Conf
FDP_ACC.1/CA	OT.Data_Int, OT.Data_Conf
FDP_ACF.1/BAC	OT.AC_Pers, OT.Data_Int, OT.Data_Conf
FDP_ACF.1/CA	OT.Data_Int, OT.Data_Conf
FDP_UCT.1/BAC	OT.AC_Pers, OT.Data_Int, OT.Data_Conf
FDP_UCT.1/CA	OT.Data_Int, OT.Data_Conf
FDP_UIT.1/BAC	OT.AC_Pers, OT.Data_Int, OT.Data_Conf
FDP_UIT.1/CA	OT.Data_Int, OT.Data_Conf
FMT_MOF.1/PROT	OT.Chip_Auth_Proof
FMT_SMF.1	OT.AC_Pers, OT.Data_Int, OT.Data_Conf
FMT_SMR.1	OT.AC_Pers, OT.Data_Int, OT.Data_Conf
FMT_LIM.1	OT.Prot_Abuse-Func
FMT_LIM.2	OT.Prot_Abuse-Func
FMT_MTD.1/INI_ENA	OT.Identification
FMT_MTD.1/INI_DIS	OT.Identification
FMT_MTD.1/KEY_WRITE	OT.AC_Pers, OT.Data_Int, OT.Data_Conf
FMT_MTD.1/KEY_READ	OT.AC_Pers, OT.Data_Int, OT.Data_Conf
FMT_MTD.1/CAPK	OT.AC_Pers, OT.Data_Int, OT.Data_Conf, OT.Chip_Auth_Proof
FMT_MTD.1/AAPK	OT.AC_Pers, OT.AA_Proof
FMT_MTD.1/AA_CA_KEY_READ	OT.AC_Pers, OT.Data_Int, OT.Data_Conf, OT.Chip_Auth_Proof, OT.AA_Proof
FPT_EMS.1	OT.AC_Pers, OT.Prot_Inf_Leak
FPT_FLS.1	OT.AC_Pers, OT.Prot_Inf_Leak, OT.Prot_Malfunction
FPT_TST.1	OT.Prot_Inf_Leak, OT.Prot_Malfunction
FPT_PHP.3	OT.AC_Pers, OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper

Table 24 SFRs and Security Objectives

9.3.3 Dependencies

9.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FAU_SAS.1	No Dependencies	
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/ENC, FCS_COP.1/MAC
FCS_CKM.1/AA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/AA
FCS_CKM.1/CA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1, FCS_CKM.1/CA
FCS_COP.1/SHA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4
FCS_COP.1/ENC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/AUTH	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/CA_SHA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4
FCS_COP.1/CA_ENC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/CA, FCS_CKM.4
FCS_COP.1/CA_MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/CA, FCS_CKM.4
FCS_COP.1/AA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/AA, FCS_CKM.4
FCS_RND.1	No Dependencies	
FIA_UID.1	No Dependencies	
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FIA_UAU.4	No Dependencies	

FIA_UAU.5/BAC	No Dependencies	
FIA_UAU.5/CA	No Dependencies	
FIA_UAU.6/BAC	No Dependencies	
FIA_UAU.6/CA	No Dependencies	
FIA_AFL.1/BAC	(FIA_UAU.1)	FIA_UAU.1
FIA_API.1/CA	No Dependencies	
FIA_API.1/AA	No Dependencies	
FDP_ACC.1/BAC	(FDP_ACF.1)	FDP_ACF.1/BAC
FDP_ACC.1/CA	(FDP_ACF.1)	FDP_ACF.1/CA
FDP_ACF.1/BAC	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/BAC
FDP_ACF.1/CA	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/CA
FDP_UCT.1/BAC	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/BAC
FDP_UCT.1/CA	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/CA
FDP_UIT.1/BAC	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/BAC
FDP_UIT.1/CA	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/CA
FMT_MOF.1/PROT	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_SMF.1	No Dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1
FMT_LIM.1	(FMT_LIM.2)	FMT_LIM.2
FMT_LIM.2	(FMT_LIM.1)	FMT_LIM.1
FMT_MTD.1/INI_ENA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/INI_DIS	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/KEY_WRITE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1

FMT_MTD.1/CAPK	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/AAPK	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/AA_CA_KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FPT_EMS.1	No Dependencies	
FPT_FLS.1	No Dependencies	
FPT_TST.1	No Dependencies	
FPT_PHP.3	No Dependencies	

Table 25 SFRs Dependencies

Rationale for the exclusion of Dependencies

The dependency FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1/SHA is discarded. The hash algorithm required by FCS_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.

The dependency FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1/CA_SHA is discarded. The hash algorithm required by FCS_COP.1/CA_SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.

The dependency FMT_MSA.3 of FDP_ACF.1/BAC is discarded. The access control TSF according to FDP_ACF.1/BAC uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

The dependency FMT_MSA.3 of FDP_ACF.1/CA is discarded. The access control TSF according to FDP_ACF.1/CA uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UCT.1/BAC is discarded. The SFR FDP_UCT.1/BAC requires the use of secure messaging between the MRTD and the BIS. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UCT.1/CA is discarded. The SFR FDP_UCT.1/CA requires the use of secure messaging between the MRTD and the BIS. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from

other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UIT.1/BAC is discarded. The SFR FDP_UIT.1/BAC requires the use of secure messaging between the MRTD and the BIS. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UIT.1/CA is discarded. The SFR FDP_UIT.1/CA requires the use of secure messaging between the MRTD and the BIS. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

9.3.3.2 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_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
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.3	(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

9.3.4 Rationale for the Security Assurance Requirements

The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

9.3.5 ADV_FSP.5 Complete semi-formal functional specification with additional error information

The TOE actually target an EAL5 + ALC_DVS.2 and AVA_VAN.5 and is only limited to EAL4+ due to the restriction of [PP_BAC] on AVA_VAN level.

Other MRTDs TOE are targeting the same physical scope are not affected by this limitation and provide the full EAL5+ set of SARs. This EAL5+ is required to reach a higher level of assurance due to sensitivity of ID documents.

9.3.6 ADV_INT.2 Well-structured internals

The TOE actually target an EAL5 + ALC_DVS.2 and AVA_VAN.5 and is only limited to EAL4+ due to the restriction of [PP_BAC] on AVA_VAN level.

Other MRTDs TOE are targeting the same physical scope are not affected by this limitation and provide the full EAL5+ set of SARs. This EAL5+ is required to reach a higher level of assurance due to sensitivity of ID documents.

9.3.7 ADV_TDS.4 Semiformal modular design

The TOE actually target an EAL5 + ALC_DVS.2 and AVA_VAN.5 and is only limited to EAL4+ due to the restriction of [PP_BAC] on AVA_VAN level.

Other MRTDs TOE are targeting the same physical scope are not affected by this limitation and provide the full EAL5+ set of SARs. This EAL5+ is required to reach a higher level of assurance due to sensitivity of ID documents.

9.3.8 ALC_CMS.5 Development tools CM coverage

The TOE actually target an EAL5 + ALC_DVS.2 and AVA_VAN.5 and is only limited to EAL4+ due to the restriction of [PP_BAC] on AVA_VAN level.

Other MRTDs TOE are targeting the same physical scope are not affected by this limitation and provide the full EAL5+ set of SARs. This EAL5+ is required to reach a higher level of assurance due to sensitivity of ID documents.

9.3.9 ALC_DVS.2 Sufficiency of security measures

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the MRTD's development and manufacturing especially for the secure handling of the MRTD's material.

The component ALC_DVS.2 augmented to EAL4 has no dependencies to other security requirements

9.3.10 ALC_TAT.2 Compliance with implementation standards

The TOE actually target an EAL5 + ALC_DVS.2 and AVA_VAN.5 and is only limited to EAL4+ due to the restriction of [PP_BAC] on AVA_VAN level.

Other MRTDs TOE are targeting the same physical scope are not affected by this limitation and provide the full EAL5+ set of SARs. This EAL5+ is required to reach a higher level of assurance due to sensitivity of ID documents.

9.3.11 ATE_DPT.3 Testing: modular design

The TOE actually target an EAL5 + ALC_DVS.2 and AVA_VAN.5 and is only limited to EAL4+ due to the restriction of [PP_BAC] on AVA_VAN level.

Other MRTDs TOE are targeting the same physical scope are not affected by this limitation and provide the full EAL5+ set of SARs. This EAL5+ is required to reach a higher level of assurance due to sensitivity of ID documents.

10 TOE Summary Specification

10.1 TOE Summary Specification

Access Control in Reading

This function controls access to read functions and enforces the security policy for data retrieval. Prior to any data retrieval, it authenticates the actor trying to access the data, and checks the access conditions are fulfilled as well as the life cycle state. It ensures that at any time, the following keys are never readable:

- Pre-personalization Agent keys and Personalization Agent keys,
- BAC keys,
- CA private key
- AAK (Active Authentication Keys)

In the Operational Use phase:

The terminal can read user data, the Document Security Object, (EF.COM, EF.SOD, EF.DG1 to EF.DG16) only after BAC or CA respectively authentication and through a valid secure channel as defined by [ICAO-9303].

In the Production and preparation stage: The Manufacturer can read the Initialization Data in Stage 2 "Production". The pre-personalization agent and the Personalization Agent can read only the random identifier in Stage 3 "Preparation" stored in the TOE. Other data-elements can only be read after they are authenticated by the TOE (using their authentication keys).

It controls read access prior to authentication and identification as defined by FIA_UID.1 and FIA_UAU.1.

It ensures as well that no other part of the memory can be accessed at any time.

Access Control in Writing

This function controls access to write functions (in NVM) and enforces the security policy for data writing. Prior to any data update, it authenticates the actor, and checks the access conditions are fulfilled as well as the life cycle state.

Regarding the file structure:

In the Production and preparation stage: The Manufacturer can write all the Initialization and data for the Pre-personalization. The Personalization Agent can write through a valid secure channel all the data Document Basic Access Keys and Active Authentication Keys after it is authenticated by the TOE (using its authentication keys). The Pre-Personalization Agent can write through a valid secure channel data to be used by the personalization agent (after it is authenticated by the TOE using its authentication keys). The Pre-personalization agent is only active after delivery. The key that is written in the TOE for authentication purposes during manufacturing in meant for the pre-personalization agent. The Pre-personalization agent (which is seen as a sub-role of the Personalization agent) will refresh this key.

In the Operational Use phase: It is not possible to create any files (system or data files). Furthermore, it is not possible to update any files (system or data files) as defined by the security policy in [ICAO-9303].

Active Authentication

This security functionality ensures the Active Authentication is performed as described in [ICAO-9303] (if it is activated by the personalizer).

Basic Access Control

This TSF provides the Basic Access Control, authentication and session keys generation to be used by the security function Secure Messaging, as described in [ICAO-9303].

The BAC Session Keys are derived from the MRZ of the MRTD's chip: this is done using SHA-1 (FCS_COP.1/SHA). The authentication initialization requires that the MRTD's chip generate 8 bytes challenge (nonce rPICC) that is read by the Basic Inspection System (FIA_UAU.1). The MRTD BAC authentication stages also require TDES encryption of 32 bytes of concatenated data and a Retail MAC computation over the 32 bytes of encryption output (FCS_COP.1/MAC). The Basic Inspection System also generated a pair (KPCD, rPCD). The use of challenges enforces a protection against replay (FIA_UAU.4). Completion of the BAC Authentication protocol means that a Secure Messaging session, in ENC_MAC_Mode (FCS_COP.1/ENC), is started with the session keys (K_{ENC} and K_{MAC}) derived according to [ICAO-9303] from the common master secret K_{Master} = K_{PICC} XOR K_{PCD} and a Send Sequence Counter SSC derived from r_{PICC} and r_{PCD} (FCS_CKM.1/BAC). All further communication with the TOE is handled by the security function Secure Messaging, enforcing confidentiality and integrity over transferred data (FIA_UAU.5/BAC). In case the BAC authentication protocol fails (the TOE being unable to identify the Terminal as being a legitimate Basic Inspection System) the TOE records one authentication failure. If the Terminal reaches the amount of consecutive authentication failures that is configured by the administrator, the BAC Authentication Key is delayed (FIA_AFL.1/BAC). The implementation contributes also to FDP_ACC.1/BAC and by FDP_ACF.1/BAC for read and write access control management and FMT_SMR.1 for security roles.

Chip Authentication

This TSF provides the Chip Authentication, authentication and session keys generation to be used by Secure Messagig, as described in [TR-03110]. The session keys are obtained using SHA-1 or SHA-256 (FCS_COP.1/CA_SHA).

It also handles key generation based on ECDH and DH (FCS_CKM.1/CA).

MRTD Personalization

This security functionality ensures that the TOE, when delivered to the Personalization Agent, provides and requires authentication for data exchange. This function allows to:

- Manage symmetric authentication using Personalization Agent keys,
- Write the Document Basic Acces Keys,
- Enable and disable Active Authentication,
- Determine the number of failed consecutive attempts allowed for the BAC protocol,
- Load or generate Active Authentication Keys,
- Load user data,
- Load or generate Chip Authentication keys.

Physical Protection

This Security Function protects the TOE against physical attacks, so that the integrity and confidentiality of the TOE is ensured, including keys, user data and TOE life cycle. It detects physical tampering, responds automatically, and also controls the emanations sent out by the TOE. It furthermore prevents deploying test features after TOE delivery. This SF also preserve a secure state when any failure is detected or a malfunction occurs.

MRTD Pre-personalization

This security functionality ensures that the TOE, when delivered to the Manufacturer, provides and requires an authentication mechanism for data exchange. This authentication is based on Triple DES symmetric authentication mechanism. This function allows to:

- Manage symmetric authentication using Pre-personalization Agent keys,
- Store the IC identification data,
- Enable Chip Authentication,
- Load Personalization Agent keys.

Secure Messaging

This security functionality ensures the confidentiality, authenticity and integrity of the communication between the TOE and the interface device. In the operational phase, after a successful Authentication Procedure (i.e. BAC or CA), a secure channel is established, based on Triple DES algorithm in case of BAC and based on Triple DES/AES algorithms in case of CA, such that the TOE is able to verify the integrity and authenticity of exchanged data. The protocols can be configured to protect the exchanges integrity and/or confidentiality. If an error occurs in the secure messaging layer, the session keys are destroyed.

Self Tests

The TOE performs self-tests to verify the integrity of the TSF data:

- At Reset. The implementation contributes to FPT_TST.1

Cryptographic Support

This Security Function provides the following cryptographic features:

- Document Basic Access Key Generation with key size 112 bits
- Key generation based on ECDH compliant to [TR_03111] with key sizes 192, 224, 256, 320, 384, 512 and 521 bits in combination with 112 bits 3DES or 128, 192 or 256 bits AES.
- Key generation based on DH with key size 2048 bits.
- RSA Key generation with key sizes 1536, 1792, 2048, 2560, 3072, 3584 and 4096
- ECC key Pair generation with key sizes 192, 224, 256, 320, 384, 512 and 521
- Secure messaging - BAC (encryption and decryption) using Triple DES in CBC mode (key size 112 bits).
- Secure messaging - BAC (message authentication code) using Triple DES Retail MAC with key size 112 bits.
- 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).
- Secure messaging (message authentication code) using:
  - Triple DES Retail MAC with key size 112 bits.
  - AES CMAC with key sizes 128,192 and 256 bits.
- Digital signature generation using:
  - ECDSA with key sizes 192 to 521 bits.
  - RSA with key sizes 1536, 1792, 2048, 2560, 3072, 3584 and 4096 bits.
- Symmetric Authentication (encryption and decryption) using Triple DES with key size 112 bits.
- Hashing in accordance with SHA-1 and SHA-256.

- The deterministic random number generation specified by FCS_RNG.1 Quality metric for random numbers of [PTF-ST].

Clear Residual Information

This security function ensures clearing of sensitive information

- Authentication state is securely cleared in case an error is detected or a new authentication is attempted
- Authentication data related to Active Authentication, Chip authentication, and BAC authentication data is securely cleared to prevent reuse
- Session keys are securely erased in case an error is detected or the secure communication session is closed

10.2 SFRs and TSS

10.2.1 SFRs and TSS - Rationale

Class FAU Security Audit

FAU_SAS.1 is met by MRTD Pre-personalization based on authentication of pre-personalization agent.

Class FCS `Cryptographic Support`

FCS_CKM.1 is met by Cryptographic Support and Basic Access Control

FCS_CKM.1/AA is met by Cryptographic Support and Active Authentication

FCS_CKM.1/CA is met by Cryptographic Support and Chip Authentication

FCS_CKM.4 is met by Clear Residual Information and Secure Messaging that destroys the session keys upon closure of a secure messaging session.

FCS_COP.1/SHA is met by Cryptographic Support and Basic Access Control

FCS_COP.1/ENC is met by Cryptographic Support, Secure Messaging and Basic Access Control

FCS_COP.1/AUTH is met by Cryptographic Support and MRTD Personalization

FCS_COP.1/MAC is met by Cryptographic Support, Secure Messaging and Basic Access Control

FCS_COP.1/CA_SHA is met by Cryptographic Support and Chip Authentication

FCS_COP.1/CA_ENC is met by Cryptographic Support, Secure Messaging and Chip Authentication

FCS_COP.1/CA_MAC is met by Cryptographic Support, Secure Messaging and Chip Authentication

FCS_COP.1/AA is met by Cryptographic Support and Active Authentication

FCS_RND.1 is met by Cryptographic Support

Class FIA Identification and Authentication

FIA_UID.1 is met by Access Control in Reading

FIA_UAU.1 is met by Access Control in Reading

FIA_UAU.4 is met by Clear Residual Information that prevents reuse of any authentication data

FIA_UAU.5/BAC is met by Basic Access Control and MRTD Personalization

FIA_UAU.5/CA is met by Chip Authentication

FIA_UAU.6/BAC is met by Secure Messaging

FIA_UAU.6/CA is met by Secure Messaging

FIA_AFL.1/BAC is met by Basic Access Control and MRTD Personalization

FIA_API.1/CA is met by Chip Authenticaion

FIA_API.1/AA is met by Active Authentication

Class FDP User Data Protection

FDP_ACC.1/BAC is met by Access Control in Writing and Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanism provided by Basic Access Control and MRTD Personalization

FDP_ACC.1/CA is met by Access Control in Writing and Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanism provided Chip Authentication

FDP_ACF.1/BAC is met by Access Control in Writing and Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanism provided by Basic Access Control and MRTD Personalization

FDP_ACF.1/CA is met by Access Control in Writing and Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanism provided Chip Authentication

FDP_UCT.1/BAC is met by Secure Messaging

FDP_UCT.1/CA is met by Secure Messaging

FDP_UIT.1/BAC is met by Secure Messaging

FDP_UIT.1/CA is met by Secure Messaging

Class FMT Security Management

FMT_MOF.1/PROT is met by MRTD Pre-personalization.

FMT_SMF.1 is met by Chip Authentication, MRTD Personalization and MRTD Pre-personalization.

FMT_SMR.1 is met by Basic Access Control, MRTD Personalization and MRTD Pre-personalization

FMT_LIM.1 is met by Physical Protection

FMT_LIM.2 is met by Physical Protection

FMT_MTD.1/INI_ENA is met by Access Control in Writing and MRTD Pre-personalization

FMT_MTD.1/INI_DIS is met byAccess Control in Reading and MRTD Personalization

FMT_MTD.1/KEY_WRITE is met by MRTD Personalization

FMT_MTD.1/KEY_READ is met by Access Control in Reading that ensures nobody can read the keys

FMT_MTD.1/CAPK is met by MRTD Personalization that allows the user to load or create Chip Authentication keys

FMT_MTD.1/AAPK is met by MRTD Personalization that allows the user to load or create Active Authentication keys

FMT_MTD.1/AA_CA_KEY_READ is met by Access Control in Reading

Class FPT Protection of the Security Functions

FPT_EMS.1 is met by Physical Protection

FPT_FLS.1 is met by Physical Protection

FPT_TST.1 is met by Physical Protection

FPT_PHP.3 is met by Physical Protection

10.2.2 Association tables of SFRs and TSS

Security Functional Requirements	TOE Summary Specification
FAU_SAS.1	MRTD Pre-personalization
FCS_CKM.1	Cryptographic Support, Basic Access Control
FCS_CKM.1/AA	Cryptographic Support, Active Authentication
FCS_CKM.1/CA	Cryptographic Support, Chip Authentication
FCS_CKM.4	Clear Residual Information, Secure Messaging
FCS_COP.1/SHA	Basic Access Control, Cryptographic Support
FCS_COP.1/ENC	Basic Access Control, Cryptographic Support, Secure Messaging
FCS_COP.1/AUTH	MRTD Personalization, Cryptographic Support
FCS_COP.1/MAC	Basic Access Control, Secure Messaging, Cryptographic Support
FCS_COP.1/CA_SHA	Chip Authentication, Cryptographic Support
FCS_COP.1/CA_ENC	Secure Messaging, Chip Authentication, Cryptographic Support
FCS_COP.1/CA_MAC	Secure Messaging, Chip Authentication, Cryptographic Support
FCS_COP.1/AA	Active Authentication, Cryptographic Support
FCS_RND.1	Basic Access Control
FIA_UID.1	Access Control in Reading
FIA_UAU.1	Access Control in Reading
FIA_UAU.4	Clear Residual Information
FIA_UAU.5/BAC	Basic Access Control, MRTD Personalization
FIA_UAU.5/CA	Chip Authentication
FIA_UAU.6/BAC	Secure Messaging
FIA_UAU.6/CA	Secure Messaging
FIA_AFL.1/BAC	Basic Access Control, MRTD Personalization
FIA_API.1/CA	Chip Authentication
FIA_API.1/AA	Chip Authentication
FDP_ACC.1/BAC	Access Control in Reading, Access Control in Writing, Basic Access Control, MRTD Personalization
FDP_ACC.1/CA	Access Control in Writing, Chip Authentication, Secure Messaging

FDP_ACF.1/BAC	Access Control in Reading, Access Control in Writing, Basic Access Control, MRTD Personalization
FDP_ACF.1/CA	Chip Authentication
FDP_UCT.1/BAC	Secure Messaging
FDP_UCT.1/CA	Secure Messaging
FDP_UIT.1/BAC	Secure Messaging
FDP_UIT.1/CA	Secure Messaging
FMT_MOF.1/PROT	MRTD Pre-personalization
FMT_SMF.1	Chip Authentication, MRTD Personalization, MRTD Pre-personalization
FMT_SMR.1	Basic Access Control, MRTD Personalization, MRTD Pre-personalization
FMT_LIM.1	Physical Protection
FMT_LIM.2	Physical Protection
FMT_MTD.1/INI_ENA	Access Control in Writing, MRTD Pre-personalization
FMT_MTD.1/INI_DIS	Access Control in Reading, MRTD Personalization
FMT_MTD.1/KEY_WRITE	MRTD Personalization
FMT_MTD.1/KEY_READ	Access Control in Reading
FMT_MTD.1/CAPK	MRTD Personalization
FMT_MTD.1/AAPK	Access Control in Writing, MRTD Personalization
FMT_MTD.1/AA_CA_KEY_READ	Access Control in Reading
FPT_EMS.1	Physical Protection
FPT_FLS.1	Physical Protection
FPT_TST.1	Self Tests
FPT_PHP.3	Physical Protection

Table 27 SFRs and TSS - Coverage

TOE Summary Specification	Security Functional Requirements
Access Control in Reading	FIA_UID.1, FIA_UAU.1, FDP_ACC.1/BAC, FDP_ACF.1/BAC, FMT_MTD.1/INI_DIS, FMT_MTD.1/KEY_READ, FMT_MTD.1/AA_CA_KEY_READ
Access Control in Writing	FDP_ACC.1/BAC, FDP_ACC.1/CA, FDP_ACF.1/BAC, FMT_MTD.1/INI_ENA, FMT_MTD.1/AAPK
Active Authentication	FCS_CKM.1/AA, FCS_COP.1/AA
Basic Access Control	FCS_CKM.1, FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/MAC, FCS_RND.1, FIA_UAU.5/BAC, FIA_AFL.1/BAC, FDP_ACC.1/BAC, FDP_ACF.1/BAC, FMT_SMR.1

Chip Authentication	FCS_CKM.1/CA, FCS_COP.1/CA_SHA, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FIA_UAU.5/CA, FIA_API.1/CA, FIA_API.1/AA, FDP_ACC.1/CA, FDP_ACF.1/CA, FMT_SMF.1
MRTD Personalization	FCS_COP.1/AUTH, FIA_UAU.5/BAC, FIA_AFL.1/BAC, FDP_ACC.1/BAC, FDP_ACF.1/BAC, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/INI_DIS, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/CAPK, FMT_MTD.1/AAPK
Physical Protection	FMT_LIM.1, FMT_LIM.2, FPT_EMS.1, FPT_FLS.1, FPT_PHP.3
MRTD Pre-personalization	FAU_SAS.1, FMT_MOF.1/PROT, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/INI_ENA
Secure Messaging	FCS_CKM.4, FCS_COP.1/ENC, FCS_COP.1/MAC, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FIA_UAU.6/BAC, FIA_UAU.6/CA, FDP_ACC.1/CA, FDP_UCT.1/BAC, FDP_UCT.1/CA, FDP_UIT.1/BAC, FDP_UIT.1/CA
Self Tests	FPT_TST.1
Cryptographic Support	FCS_CKM.1, FCS_CKM.1/AA, FCS_CKM.1/CA, FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/MAC, FCS_COP.1/CA_SHA, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_COP.1/AA
Clear Residual Information	FCS_CKM.4, FIA_UAU.4

Table 28 TSS and SFRs - Coverage