IDEMIA

Taiwan eID Applet CC EAC with AA Configuration

Public Security Target

About IDEMIA

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

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

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

For more information, visit www.idemia.com / Follow @IdemiaGroup on Twitter

DOCUMENT MANAGEMENT

Business Unit – Department	**CI – R&D**
Document type	**FQR**
Document Title	**Taiwan eID Applet CC EAC with AA Configuration – Public Security Target**
FQR No	**110 8498**
FQR Issue	**1**

CONTRIBUTORS

Name	Role	Author	Reviewer	Approver
MESTIRI, Sarra	Security Manager	Yes		
YAP Abraham	Project Leader			

DOCUMENT REVISION

Date	Revision	Modification	Modified by
2018/02/08	1.0	Creation	MESTIRI Sarra

IDEMIA

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

This Security Target Lite aims to satisfy the requirements of Common Criteria level EAL5+, augmented with AVA_VAN.5 and ALC_DVS.2 in defining the security enforcing functions of the Target Of Evaluation and describing the environment in which it operates.

The basis for this composite evaluation is the composite evaluation of Open Platforms COSMOV8.1-N - Platform and configurable JavaCard application, Taiwan eID Applet CC.

The Taiwan eID Applet CC is a custom version of the LDS V10. Some configurations of the applet use a shared library with HICOS application.

The Taiwan eID Applet CC can have different configurations, the presents ST considers the configuration and does not use the shared library with HICOS application:

- EAC V2 with PACE-CAM/TA without CA
- AA

The Taiwan eID Applet CC application code is loaded on the E2Prom of the platform at prepersonalisation or personalisation phase.

The applet works on 2 platforms:

The first is ID-One Cosmo v8.1-N - Standard Platform', embeds the PIV 2.4 Application in ROM.

The second platform, 'ID-One Cosmo v8.1-N Large Platform' embeds the applications PIV 2.4 and IAS ECC V2 Applications in ROM. A new version of the ID-One Cosmo v8.1-N Large platform (ID-One Cosmo v8.1-N R2 Large) also embeds the Taiwan eID Applet CC application in ROM.

The 2 platforms have the same interfaces and covered by a unique security target [54].

All additional applications, romed or loaded in E2prom at pre perso or perso phase are out of the scope of the present evaluation, for example PIV2, IAS ECC V2.

1.1. Security Target Reference

The Security target is identified as follows:

Title: Security Target POLLUX
Name: Taiwan eID Applet CC Security Target EAC AA
Oberthur Technologies registration: FQR 110 8394 Issue 3
Authors: Oberthur Technologies
ST Lite reference: FQR 110 8498 Issue 1
Publication Date for the Public ST-Lite: January 2018

1.2. TOE Reference

Product name:	Taiwan eID Applet CC on ID-One Cosmo v8.1-N	Taiwan eID Applet CC on ID-One Cosmo v8.1-N R2
Commercial name of the TOE 1:	Taiwan eID Applet CC: EAC configuration with AA on ID-One Cosmo v8.1-N - Standard	Not applicable

	Platform	
Commercial name of the TOE 2:	Taiwan eID Applet CC: EAC configuration with AA on ID-One Cosmo v8.1-N Large Platform	Taiwan eID Applet CC: EAC configuration with AA on ID-One Cosmo v8.1-N R2 Large Platform
Memory	E2PROM	ROM
Application Reference Code	202842	202842
Communication protocol	Contact, Contactless and Dual	Contact, Contactless and Dual
ST Cosmo v8.1-N reference	ERATO Security Target FQR 110 7986	ERATO Security Target FQR 110 7986

Table 1: TOE REFERENCES

1.3. TOE Identification

The aim of the paragraphs is to allow the user to identify uniquely the TOE.

The TOE is composed of application [Taiwan eID Applet CC Security Target EAC] and a COSMO v8-1n platform on the IC.

1.3.1.TOE Identification

This chapter presents the means to identify the evaluated application and the Platform.

The **[**Taiwan eID Applet CC Security Target EAC**]** installation command **shall** use the executable load File AID and module AID.

Name	Value
Executable Load File (ELF) AID	A000000077010000071000000000000F
Executable Module AID	A000000077010000071000010000000F
Application AID	A00000024710FF

Table 2: AID Taiwan eID Applet CC Security Target EAC Configuration

1.3.2.Platform Identification

In order to assure the authenticity of the card, the product identification shall be verified by analysing:.

TOE Name	ID-One Cosmo v8.1-N - Standard LDS Platform	ID-One Cosmo v8.1-N Large Platform	ID-One Cosmo v8.1-N R2 Large Platform
Mask / Hardware Identification	083621	084021	084022
Label PVCS code	COSMO_V81N_LDS_STANDARD_PLATFORM_R10	COSMO_V81N_LARGE_PLATFORM_R10	COSMO_V81N_LARGE_PLATFORM_R2
IC reference version	NXP P60D081	NXP P60D145	NXP P60D145

IC ST identification	NXP Secure Smart Card Controller P6021y VB Security Target Lite Rev. 1.51 BSI-DSZ-CC-0955-V2-2016	NXP Secure Smart Card Controller P6022y VB Security Target Lite Rev. 1.52 BSI-DSZ-CC-0973-V2-2016	NXP Secure Smart Card Controller P6022y VB Security Target Lite Rev. 1.52 BSI-DSZ-CC-0973-V2-2016
IC EAL	EAL5 with augmentations: AVA_VAN.5, ALC_DVS.2, ASE_TSS.2	EAL5 with augmentations: AVA_VAN.5, ALC_DVS.2, ASE_TSS.2	EAL5 with augmentations: AVA_VAN.5, ALC_DVS.2, ASE_TSS.2
IC certificate	BSI-DSZ-CC-0955-V2-2016	BSI-DSZ-CC-0973-V2-2016	BSI-DSZ-CC-0973-V2-2016
Date of IC certification	11 October 2016	11 October 2016	11 October 2016
Reference of the Cosmo Platform certificate	ANSSI-CC-017/48	ANSSI-CC-2017/49	ANSSI-CC-2017/49-M01

Table 3: Platform Identification

The evaluated platform allows the loading of patch. The patch reference is specified in the platform ST for ID-One Cosmo v8.1-N and the associated platform certificate. The ID-One Cosmo v8.1-N R2 doesn't include any patch.

1.3.3. Configuration of the platform

In the present evaluation, the loading of application (Java Card Applets) on the platform at use phase is allowed. It can be forbidden if requested by the product issuer.

1.4. Reference documents

[1] Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model", September 2012, Version 3.1 revision 4.

[2] Common Criteria for information Technology Security Evaluation, Part 2: Security Functional requirements", September 2012, Version 3.1 revision 4.

[3] Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance requirements", September 2012, Version 3.1 revision 4.

[4] Composite product evaluation for Smart Cards and similar devices", September 2007, Version 1.0, CCDB-2007-09-001.

[5] JIL - Certification of "open" smart card products - Version 1.1 - 4 February 2013

[6] Joint Interpretation Library - Composite product evaluation- for Smart Cards and similar devices – v1.2

[7] GlobalPlatform Card Specification – Version 2.2.1 – January 2011.

[8] GlobalPlatform Card Mapping Guidelines of existing GP v2.1.1 implementations on v2.2.1 – Version 1.0.1 – January 2011.

[9] GlobalPlatform Card Confidential Card Content Management – Card Specification v 2.2 – Amendment A – Version 1.0.1 – January 2011.

[10] Global Platform Card Technology, Secure Channel Protocol 03, Card - Specification v 2.2 - Amendment D- Version 1.1 - September 2009.

[11] Identification cards - Integrated Circuit(s) Cards with contacts, Part 6: Inter industry data elements for interchange", ISO / IEC 7816-6 (2004).

[12] FIPS PUB 46-3 "Data Encryption Standard", October 25, 1999, National Institute of Standards and Technology

[13] FIPS PUB 81 "DES Modes of Operation", December, 1980, National Institute of Standards and Technology

[14] FIPS PUB 140-2 "Security requirements for cryptographic modules", May 2001, National Institute of Standards and Technology

[15] FIPS PUB 180-3 "Secure Hash Standard", October 2008 , National Institute of Standards and Technology

[16] FIPS PUB 186-3 "Digital Signature Standard (DSS)", June 2009, National Institute of Standards and Technology

[17] FIPS PUB 197, "The Advanced Encryption Standard (AES)", November 26, 2001, National Institute of Standards and Technology

[18] SP800_90 "Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)", March 2007, National Institute of Standards and Technology

[19] NIST Special Publication 800-38B, Recommendation for Block, Cipher Modes of Operation: The CMAC Mode for Authentication, Morris Dworkin, May 2005

[20] CEN/EN14890:2013 Application Interface for smart cards used as Secure Signature Creation

[21] ANSI X9.31 "Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)", 1998, American National Standards Institute

[22] ISO/IEC 9796-1, Public Key Cryptography using RSA for the financial services industry", annex A, section A.4 and A.5, and annex C (1995)

[23] ISO/IEC 9797-1, "Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher", 1999,

International Organization for Standardization

[24] ISO/IEC 9796-2:2002 - Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Mechanisms using a hash-function

[25] ISO/IEC 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002

[26] ISO/IEC 15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002

[27] ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002

[28] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4 Revised November 1, 1993

[29] FIPS Publication 180-2 Secure Hash Standard (+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[30] AMERICAN NATIONAL STANDARD X9.62-1998: Public Key Cryptography For The Financial Services Industry (rDSA), 9 septembre 1998

[31] PKCS#1 The public Key Cryptography standards, RSA Data Security Inc. 1993

[32] IEEE Std 1363a-2004, “Standard Specification of Public Key Cryptography – Amendment 1: Additional techniques”, 2004, IEEE Computer Society.

[33] Référentiel Général de Sécurité version 2.0 – Annexe B1 – Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, Version 2.03 du 21 février 2014

[34] AIS 31 - Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik

[35] European Card for e-Services and national e-ID Applications - IAS ECC v1.0.1

[36] ISO/IEC 7816-4:2013, Identification Cards — Integrated circuit cards— Part 4 : Organization, security and commands for interchange

[37] ISO/IEC 9797-1:2011, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher

[38] ISO 11568-2:2012, Financial services - Key management (retail) - Part 2 : symmetric ciphers, their key management and life cycle

[39] Technical Guideline TR-03111- Elliptic Curve Cryptography Version 2.0

[40] Référentiel général de sécurité, version 2.0 du 21 février 2014 - Annexe B1 - Mécanismes cryptographiques

[41] ISO/IEC 11770-2. Information Technology – Security techniques – Key management – part 2: Mechanisms using symmetric techniques, 1996

[42] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version - 1.1, Date - October 01, 2004, published by authority of the secretary general, International Civil Aviation Organization

[43] ‘ICAO Doc 9303’, Machine Readable Travel Documents, Seventh Edition, 2015 – Security Mechanisms for MRTDs

[44] Development of a logical data structure – LDS for optional capacity expansion technologies Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision – 1.7, published by authority of the secretary general, International Civil Aviation

Organization, LDS 1.7, 2004-05-18

[45] Advanced Security Mechanisms for Machine readable travel documents – Extended Access control (EAC) – TR03110 – v1.11

[46] Annex to Section III Security Standards for Machine Readable Travel Documents Excerpts from ICAO Doc 9303, Part 1 - Machine Readable Passports, Fifth Edition – 2003

[47] BAC- Machine readable travel documents with “ICAO Application”, Basic Access control – BSI-PP-0055 v1.10 25th march 2009

[48] EAC- Machine readable travel documents with “ICAO Application”, Extended Access control – BSI-PP-0056 v1.10 25th march 2009

[49] EAC With PACE- Machine readable travel documents with “ICAO Application”, Extended Access Control with PACE (EAC PP) – BSI-PP-0056 V2 – 2012

[50] MRTD with PACE – PP-0068v2

[51] E-passport: adaptation and interpretation of e-passport Protection Profiles, SGDN/DCSSI/SDR, ref. 10.0.1, February 2007

[52] Embedded Software for Smart Security Devices, Basic and Extended Configurations, ANSSi-CC-PP-2009/02, 1/12/2009

[53] Technical Report, Supplemental Access Control for Machine Readable Travel Documents – version v1.01

[54] ERATO Security Target FQR 110 7986, Oberthur Technologies, 2016

[55] ID-One Cosmo V8.1-n, Application Loading Protection Guidance, FQR: 110 8001, Issue 1, Oberthur Technologies, 2016

[56] ID-One Cosmo V8.1, Applet Security Recommendations, FQR: 110 7999, Issue 3, Oberthur Technologies, 2016

[57] ID-One Cosmo V8.1, Pre-Perso Guide, FQR: 110 7743, Issue 4, Oberthur Technologies, 2017

[58] ID-One Cosmo V8.1, Reference Guide, FQR 110 7744, Issue 4, Oberthur Technologies, 2017

[59] LDS EAC JAVA Applet SOFTWARE REQUIREMENTS SPECIFICATIONS –Oberthur Technologies,11-AA 2015

[60] FQR 220 1038 Ed4 – POLLUX Personalization Manual

[61] FQR 220 1039 Ed2 – POLLUX User Manual

[62] CASTOR Security Target FQR 110 8141 Ed2

1.5. Definitions

DES	Data Encryption Standard
DF	Dedicated File
DH	Diffie Hellman
EAL	Evaluation Assurance Level
EF	Elementary File
EEPROM	Electrically Erasable Programmable Read Only Memory
FID	File identifier
GP	Global Platform
IC	Integrated Chip
ICC	Integrated Chip card
IFD	Interface Device
MAC	Message Authentication code
PIN	Personal Identification Number
PKI	Public Key Infrastructure
ROM	Read Only Memory
RSA	Rivest Shamir Adleman
RSA CRT	Rivest Shamir Adleman – Chinese Remainder Theorem
SCP	Secure Channel Procotol
SHA	Secure hashing Algorithm
TOE	Target of evaluation

1.6. Technical Terms Definition

Term	Definition
Active Authentication	Security mechanism defined in [6] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State or Organization.
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization 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 (BAC)	Security mechanism defined in [6] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical MRTD.
Biographical data (biodata)	The personalized details of the MRTD holder 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.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means.
Country Signing CA Certificate (Ccsca)	Self-signed certificate of the Country Signing CA Public Key (KPuCSCA) issued by CSCA stored in the inspection system.
Document Basic Access Keys	Pair of symmetric (two-key) 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. 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 (SOD)	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).
Eavesdropper	A threat agent with Enhanced-Basic 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.
Extended Access Control (EAC)	Security mechanism identified in [48] by which means the MRTD'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 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.
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 Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer (i.e MRTD packaging responsible).
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 document 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.
Initialisation	Process of writing Initialisation Data (see below) to the TOE.
Initialization 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.
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 a 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).
Issuing State	The Country issuing the MRTD.
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology. The capacity expansion technology used is the MRTD's chip.
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure, as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) (1) personal data of the MRTD holder, (2) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), (3) the digitized portraits (EF.DG2), (4) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and (5) the other data according to LDS (EF.DG5 to EF.DG16). (6) EF.COM and EF.SOD
Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
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.
Machine Readable Visa (MRV)	A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport.
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.
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.
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes - the file structure implementing the LDS

	- the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG14, EF.DG 16, EF.COM and EF.SOD) and - the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAOT.
MRTD's chip Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.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.
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 portrait, signature and biographical data are applied to the document. This may also include the optional biometric data collected during the "Enrolment" (Step 6).
Personalization Agent	The agent acting on the behalf of the issuing State or Organization to personalize the MRTD for the holder by (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) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Key	Symmetric cryptographic authentication key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4/BAC, FIA_UAU.5/BAC and FIA_UAU.6/BAC.
Physical travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) (1) biographical data, (2) data of the machine-readable zone, (3) photographic image and (4) other data.
Pre-Personalisation	Process of writing Pre-Personalisation Data to the TOE including the creation of the MRTD Application (Step 5)
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (i.e IC 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 Active Authentication Key Pair and the Personalization Agent Key Pair.

Pre-personalized MRTD's chip	MRTD's chip equipped with an unique identifier and an unique asymmetric Active Authentication Key Pair of the chip.
Primary Inspection System (PIS)	An inspection system that contains a terminal for the contactless communication with the MRTD's chip and does not implement the terminals part of the Basic Access Control Mechanism.
Random identifier	Random identifier used to establish a communication to the TOE in Phase 3 and 4 preventing the unique identification of the MRTD and thus participates in the prevention of traceability.
Receiving State	The Country to which the Traveler is applying for entry.
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.
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means.
Secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
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.
Travel document	A passport or other official document of identity issued by a State or Organization, which may be used by the rightful holder for international travel.
Traveler	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE.
Unpersonalized MRTD	The MRTD that contains the MRTD Chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalisation Agent from the Manufacturer.
User data	Data created by and for the user, that does not affect the operation of the TSF.
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template.
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.

Table 4: Technical Terms Definition

2. TARGET OF EVALUATION

The product **Taiwan eID Applet CC** is a multi-applicative Javacard product, embeddable in contact and/or contact-less smart card integrated circuits of different form factors. The product can be configured to serve different use cases, during the **Prepersonalization/personalization phases** of the product [60].

The product supports the storage and retrieval of structured information compliant to the Logical Data Structure as specified in [44]. It also provides standard authentication protocols, Extended Access Control [49] PACE [50], Active Authentication,...

It can host two types of applications as mentioned above, namely the IDL and **MRTD**. Moreover, further configuration may also be done to each type of application to serve use cases other than those behaviourally defined in the referenced normative documents.

This product is loaded on the platform, for details see ST [54].

The product uses a sharable interface provided by an application already evaluated. See details in the ST [62]. This shareable interface allows the user to be authenticated by the PKI PIN.

For the use of shareable interface provided by HiCOS application, HiCOS application shall be present on the platform. This is done by loading HiCOS application in EEPROM memory.
This sharable interface is only used in 2 configurations, see details in § 2.1.

The Taiwan eID Applet CC product architecture can be viewed as shown in the following figure:

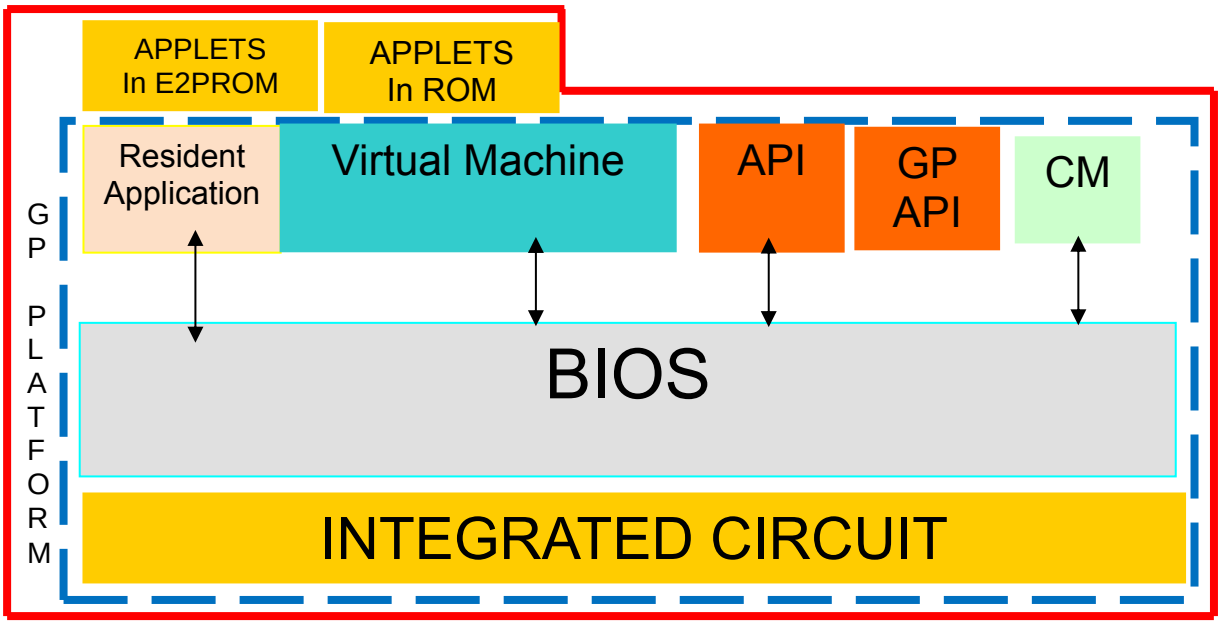


Figure 1: TOE Limits

2.1. TOE Overview

The Target of Evaluation (TOE) addressed by the current Security target is an electronic travel document representing a contactless / contact smart card1 programmed according to ICAO Technical Report "Supplemental Access Control" [53]. This smart card / passport provides the following application:

– the travel document containing the related user data including biometric as well as data needed for authentication including PACE passwords; this application is intended to be used by governmental organisations, amongst other as a machine readable travel document (MRTD).

The TOE described in this security target is the PACE configuration, conformant to **Configuration 4.** The product is composed of the functions: BAC, EAC, AA, CAM, PACE, ... all are presented in the chapter TOE architecture. Only some parts are in the scope of the evaluation of the present configuration.

Applets in ROM are PIV 2.4 and IAS ECC V2.

Different configurations of the TOE are under evaluation. This ST considers only EAC and AA with Secure Messaging (DES + AES) on read DG3+DG4 after EAC.

Configuration	PP Conformity	Chip		Extensions
		P60D081	P60D145	
1	PP 0068 (PACE)	X	X	AA CA CAM
2	PP0056v2 (EAC sur PACE)	X	X	AA CAM PACE-CAM/TA without CA BAC de-activation SM (DES + AES) on read DG3+DG4 After EAC
3	PP 0055 (BAC)	X	X	AA + CA
4	**PP0056v1 (EAC sur BAC)**	**X**	**X**	**AA** **SM (DES + AES) on read DG3+DG4 after EAC**

Table 5: 4 Configurations of the Taiwan eID Applet CC application

The EAC TOE is instantiated during the application Prepersonalization with the creation of the MF / DF required for the EAC configuration.

The shared PIN is not available in the present configuration, as it requires the PACE mechanism, not present in the ST.

The TOE life cycle is described in **§** 3**.**

The TOE identification is described in **§ 1.3.1.**

The TOE scope encompasses the following features:

- Active Authentication
- EAC Authentication
- Prepersonalization phase
- SM (DES + AES) on read DG3+DG4 after EAC

Nevertheless, the TOE in the Taiwan eID Applet CC application embeds other secure functionalities they are not in the scope of this evaluation and are in the scope of other evaluations.

2.1.1. Physical scope

The TOE is physically made up of several components hardware and software. Once constructed, the TOE is a bare microchip with its external interfaces for communication. The physical 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 on several physical medium within an inlay, or eCover; in a plastic card; ...

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

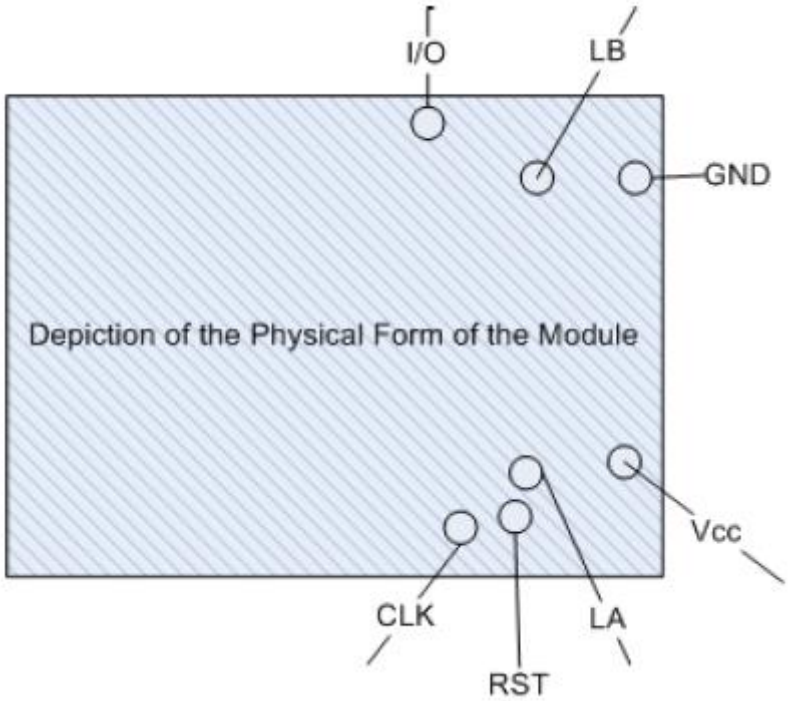


Figure 2: Physical Form

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

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

Table 6: Ports and Interfaces

2.1.2. Required non-TOE hardware/software/firmware

The TOE is an MRTD. It is an independent product and does not need any additional hardware/software/firmware to ensure its security.

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

2.1.3. TOE Usage and major security features

State or organisation issues MRTDs to be used by the holder to prove his/her identity and claiming associated rights. For instance, it can be used to check identity at customs in an MRTD configuration, verifying authenticity of electronic visa stored on the card and correspondence with the holder.

In order to pass successfully the control, the holder presents its personal MRTD to the inspection system to first prove his/her identity. The inspection system is under control of an authorised agent and can be either a desktop device such as those present in airports or a portable device to be used on the field.

The MRTD in context of this security target contains:

Visual (eye readable) biographical data and portrait of the holder printed in the booklet

A separate data summary (MRZ or keydoc data) for visual and machine reading using OCR methods in the Machine Readable Zone (MRZ or keydoc area)

And data elements stored on the TOE's chip for contact-less machine reading.

The authentication of the holder is based on:

The possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and

The Biometric matching performed on the Inspection system using the reference data stored in the MRTD.

When holder has been authenticated the issuing State or Organization can performed extra authentications in order to gain rights required to grant access to some sensitive information such as "visa information"…

The issuing State or Organization ensures the authenticity of the data of genuine MRTDs. The receiving State trusts a genuine MRTD of an issuing State or Organization.

The MRTD can be viewed as the combination:

A physical MRTD in form of paper or plastic with an embedded chip and possibly an antenna. It presents visual readable data including (but not limited to)

- Personal data of the MRTD holder
- The biographical data on the biographical data page of the passport book
- The printed data in the Machine-Readable Zone (MRZ) or keydoc area that identifies the device
- The printed portrait

A logical MRTD as data of the MRTD holder stored according to the Logical Data Structure as specified by ICAO and extended in [44][45][46] on the contactless integrated circuit. It presents contact or contact-less readable data including (but not limited to)

- Personal data of the MRTD holder
- The digital Machine Readable Zone Data (digital MRZ data or keydoc data, DG1)
- The digitized portraits
- The optional biometric reference data of finger(s) or iris image(s) or both
- The other data according to LDS (up to DG24)
- 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 its data. The MRTD as the physical device 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 organisational security measures (e.g. control of materials, personalization procedures). These security measures include the binding of the MRTD's chip to the physical support.

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.

2.2. TOE Definition

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing and provides standard authentication protocols, namely Basic Access Control, Extended Access Control and Active Authentication.

The product can be configured to serve different use cases, during the **Prepersonalization/personalization phases** of the product.

The TOE comprises at least:

- Circuitry of the MRTD's chip (the integrated circuit, IC)
- IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software
- Cosmo V8-1N Standard or Large
- API
- Taiwan eID Applet CC application
- Associated guidance documentation

The platform provides an operational environment for the application: all cryptographic algorithm implementations and associated self-tests, random number and key generation, card lifecycle management, and key storage and protection are provided by the platform. The code for this functionality is contained in the platform ROM. However, the factory configuration of the module constrains the module to the set of services provided by the platform's Card Manager (implementing a standard set of GlobalPlatform services),

Some applications present on the Cosmo v8.1-N Platform are not usable on this TOE such as the PIV applet which is not instantiated.

The applet may be used on a contact mode compliant to ISO/IEC 7816-3 specification or on contactless mode compliant to ISO/IEC 14443 specification.

2.3. TOE Architecture

The TOE is a smartcard, composed of IC, Javacard Platform and the Taiwan eID Applet CC application. Other applications may reside in the TOE.

2.3.1. Integrated Circuit

The TOE is embedded on NXP chips, more information on the chips is given in the related public Security Targets lites identified in table 3 of chapter 1.3.2**.**

2.3.2. JavaCard Platform

The Operating System is based on Java Card Technology and Global Platform technology. His main responsibilities are:

- providing interface between the Integrated Circuit and the applet
- providing to the applet, basic services to access to memories and all needed cryptographic operations
- ensuring global management of the card (loading, installation and deletion of applets) and monitor the security of the card (data integrity and physical attacks counter-measures). For details see [54].

2.3.3. Application Functionalities

This application stores the personal information related to the cardholder of an MRTD or an IDL. It also allows governmental organizations to retrieve these pieces of data.

The applet supports the authentication mechanisms described in ICAO and EAC specifications and ISO/IEC 18013-3 ISO Compliant Driving License specification with a fully configurable access control management over the EFs (EFs).

The applet may be used on a contact mode (compliant to ISO/IEC 7816-3 specification) and/or contactless mode (compliant to ISO/IEC 14443 specification).

The compliancy of the applet to LDS, EAC, or IDL, is achieved provided a correct personalization is performed. The correct authentication mechanisms and access conditions over the EFs must be assigned.

In summary, the applet supports the following authentication mechanisms stated in the ICAO specifications (for MRTD) and the ISO Compliant Driving License standard (for IDL):

- Active Authentication (AA)
- Basic Access Control (BAC)
- Password Authenticated Connection Establishment (PACE)
- Extended Access Control (EAC)
- Chip Authentication Mapping (CAM)

All authentication mechanisms are listed in the following chapters, all are part of the product but only some are part of the present evaluation.

2.3.3.1. 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 1024 bits, 1536 bits or 2048 bits and hashing algorithm of SHA1 or SHA2.
- ECDSA over prime field curves with hashing algorithm of SHA1 or SHA2 and the key sizes 192 to 512.
- AES-256 using ISO/IEC 9797-1 M2 padding method.
- TDES with double and triple length keys using ISO/IEC 9797-1 M2 padding method.

2.3.3.2. Basic Access Control (BAC)

The protocol for Basic Access Control is specified by ICAO [47] 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 ISO/IEC 11770-2 [41] 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 7: BAC Configuration

2.3.3.3. Terminal Authentication

The Terminal Authentication Protocol is a two move challenge-response protocol that provides explicit unilateral authentication of the terminal.

This protocol enables the MRTD chip to verify that the terminal is entitled to access sensitive data. As the terminal may access sensitive data afterwards, all further communication MUST be protected appropriately. Terminal Authentication therefore also authenticates an ephemeral public key chosen by the terminal that was used to set up Secure Messaging with Chip Authentication. The MRTD chip MUST bind the terminal's access rights to Secure Messaging established by the authenticated ephemeral public key of the terminal.

2.3.3.4. Chip Authentication

The Chip Authentication 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 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.

The protocol in version 1 provides implicit authentication of both the MRTD chip itself and the stored data by performing Secure Messaging using the new session keys.

The protocol in Version 2 provides explicit authentication of the MRTD chip by verifying the authentication token and implicit authentication of the stored data by performing Secure Messaging using the new session keys.

2.3.3.5. Password Authenticated Connection Establishment (PACE)

PACE is an access control mechanism that is supplemental to BAC. It is a cryptographically stronger access control mechanism than BAC since it uses asymmetric cryptography compared to BAC's symmetric cryptography.

PACE is realized through 5 commands:
1. MSE SET – AT command
2. GENERAL AUTHENTICATE command – Encrypted Nonce
3. GENERAL AUTHENTICATE command – Map Nonce
4. GENERAL AUTHENTICATE command – Perform Key Agreement
5. GENERAL AUTHENTICATE command – 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 PACE protocol:

Configuration	Mapping	Key Algo	Key Length (in bytes)	Secure Messaging	Auth. Token	Hash Algo
PACE–ECDH–GM–3DES	Generic	3DES 2Key	16	CBC / Retail MAC	Retail MAC	SHA-1
PACE–ECDH–GM–AES–128	Generic	AES	16	CBC / CMAC	CMAC	SHA-1
PACE–ECDH–GM–AES–192	Generic	AES	24	CBC / CMAC	CMAC	SHA-256
PACE–ECDH–GM–AES–256	Generic	AES	32	CBC / CMAC	CMAC	SHA-256
PACE–ECDH–IM–3DES	Integrated	3DES 2Key	16	CBC / Retail MAC	Retail MAC	SHA-1
PACE–ECDH–IM–AES–128	Integrated	AES	16	CBC / CMAC	CMAC	SHA-1
PACE–ECDH–IM–AES–192	Integrated	AES	24	CBC / CMAC	CMAC	SHA-256
PACE–ECDH–IM–AES–256	Integrated	AES	32	CBC / CMAC	CMAC	SHA-256
PACE–ECDH–CAM–AES–128	Chip Authentication	AES	16	CBC / CMAC	CMAC	SHA-1
PACE–ECDH–CAM–AES–192	Chip Authentication	AES	24	CBC / CMAC	CMAC	SHA-256
PACE–ECDH–CAM–AES–256	Chip Authentication	AES	32	CBC / CMAC	CMAC	SHA-256

Table 8: PACE Configuration

2.3.3.6. Extended Access Control (EAC)

EAC is an authentication protocol based on a PKI infrastructure. It further ensures that the IS is authorized to read and/or update data stored in the applet. This authentication mechanism generates a strong secure messaging session through the step of Chip Authentication.

This mechanism is realized by the following steps:

1. Chip Authentication (CA)Chip Authentication is achieved by using a MANAGE SECURITY ENVIRONMENT – SET – Key Agreement Template (MSE SET KAT) command or by using a MANAGE SECURITY ENVIRONMENT – SET – Authentication Template (MSE SET AT) command followed by GENERAL AUTHENTICATE command.

The Chip Authentication mechanism enables the authentication of the chip by using an authenticated DH scheme. It may be realized in two ways:

- Classical DH (DH El Gamal) with key length of 1024, 1536, or 2048 bits
- DH over Elliptic curves over prime fields (ECDH) with the key length supported by the underlying Javacard platform.

2. Certificate Chain Handling

The certificate chain is processed through a series of MANAGE SECURITY ENVIRONMENT – SET – Digital Signature Template (MSE SET DST) and PERFORM SECURITY OPERATION – Verify Certificate (PSO VERIFY) commands.

The chain is done to extract a key from the IS certificate, the key which will be used in the Terminal Authentication.

3. Terminal Authentication (TA)

Terminal Authentication is achieved by using an EXTERNAL AUTHENTICATE command.

The Terminal Authentication mechanism is an authentication of the IS based on a classical challenge/response scheme. The signature scheme may be:
ECDSA SHA-1, ECDSA SHA-224, ECDSA SHA-256, ECDSA SHA-384, or ECDSA SHA-512 on elliptic curves over prime field with key length supported by the underlying Javacard platform
RSA SHA-1, SHA-256, or SHA-512 (PKCS#1 v1.5 or PKCS#1 v2.1 - PSS) with a key length of 1024, 1536, and 2048 bits.

2.3.3.7. PACE-CAM

The Chip Authentication Mapping is a new mapping for PACE which extends the Generic Mapping that integrates Chip Authentication into the PACE protocol. This mapping combines PACE and Chip Authentication into one protocol PACE-CAM, which allows faster execution than the separate protocols (i.e. PACE + CA + TA).

PACE-CAM is realized the same way as § 2.3.3.6. The only difference is that the chip computes the Chip Authentication Data using the chip's static private key then sends this data to the terminal. The terminal verifies the authenticity of the chip using the recovered Chip Authentication Data.

2.3.3.8. Match On-Card (MOC) Verification

MOC verification may be used to grant some access rights to EFs.

This feature relies on the services provided by the CHV Server applet MOC verification is supported if the *CHV Configuration* is properly configured in the install parameter. Once the MOC verification is allowed the applet will permit the use of CHV-related commands that handles biometric and Global PIN credentials.

2.3.3.9. PIN

The product supports the management of card holder credentials such as Cardholder PIN and Global PIN which can be used to grant access rights to EFs or keys. The Cardholder PIN and Global PIN each have its PIN Unblocking Key (Cardholder PUK and Global PUK, respectively). These PINs and corresponding PUKs have to be initialized during personalization if they are used to pdrotect access to EFs and keys.

2.3.3.10. Watermarking

The watermarking feature may be used to restrict the access to the plain image data of particular EF(s). Enabling the watermarking will cause the image data to be corrupted during the reading of the file contents.

The de-watermarking conditions should be configured accordingly and these conditions must be satisfied in order to grant access to the plain image data, details are in the dedicated security Target.

2.3.3.11. Secure Messaging

The TOE supports the ISO Secure Messaging. It provides a secure channel (i.e. encrypted and authenticated) between application and terminal. Secure Messaging can be set up by Chip Authentication, PACE, or Basic Access Control. The provided security level depends on the mechanism used to set up Secure Messaging.

A session is started when secure messaging is established. The session only ends with the release of

secure messaging, e.g. by sending a command without secure messaging.

2.3.3.12. OT Cryptographic library

A dedicated cryptographic library has been developed and designed by Oberthur Technologies.

This cryptographic library is embedded on the TOE to provide the highest security level and best tuned performances. It is implemented at the platform level and are already in the scope of the platform evaluation.

2.3.3.13. Additional applications

Additional java card applications are present in the TOE: PIV 2.4 and IAS ECC V2, … These applications are outside the scope of the present evaluation.

2.3.4. Mechanism included in the scope of the evaluation

All TOE functionalities are presented in the previous chapter.
The present evaluation includes the listed functionalities:

- EAC
- AA
- CAM
- BAC deactivation (additional function)
- Secure Messaging (DES + AES) on read DG3+DG4 after EAC
- Personalization functions

2.4. Reference

The TOE is identified as follows:

Application Guidance	
TOE name (commercial name)	Taiwan eID Applet CC on ID-One Cosmo v8.1-N
Guidance document for preparation	Personalization Manual [60]
Guidance document for operational use	User Manual [61]
Platform Guidance	
Guidance document for Platform Pre-personalisation	COSMO V8.1-N Pre-Perso Guide[57]
Developer of sensitive applications*	COSMO V8.1-N Security Recommendations [56]
Guidance for application developer*	COSMO V8.1-N Reference Guide [58]
Guidance to Issuer of the platform that aims to load applications*	COSMO V8.1-N Application Loading Protection Guidance [55]

Table 9: TOE Guidance REFERENCES

3. TOE LIFE CYCLE

3.1. TOE Life Cycle Overview

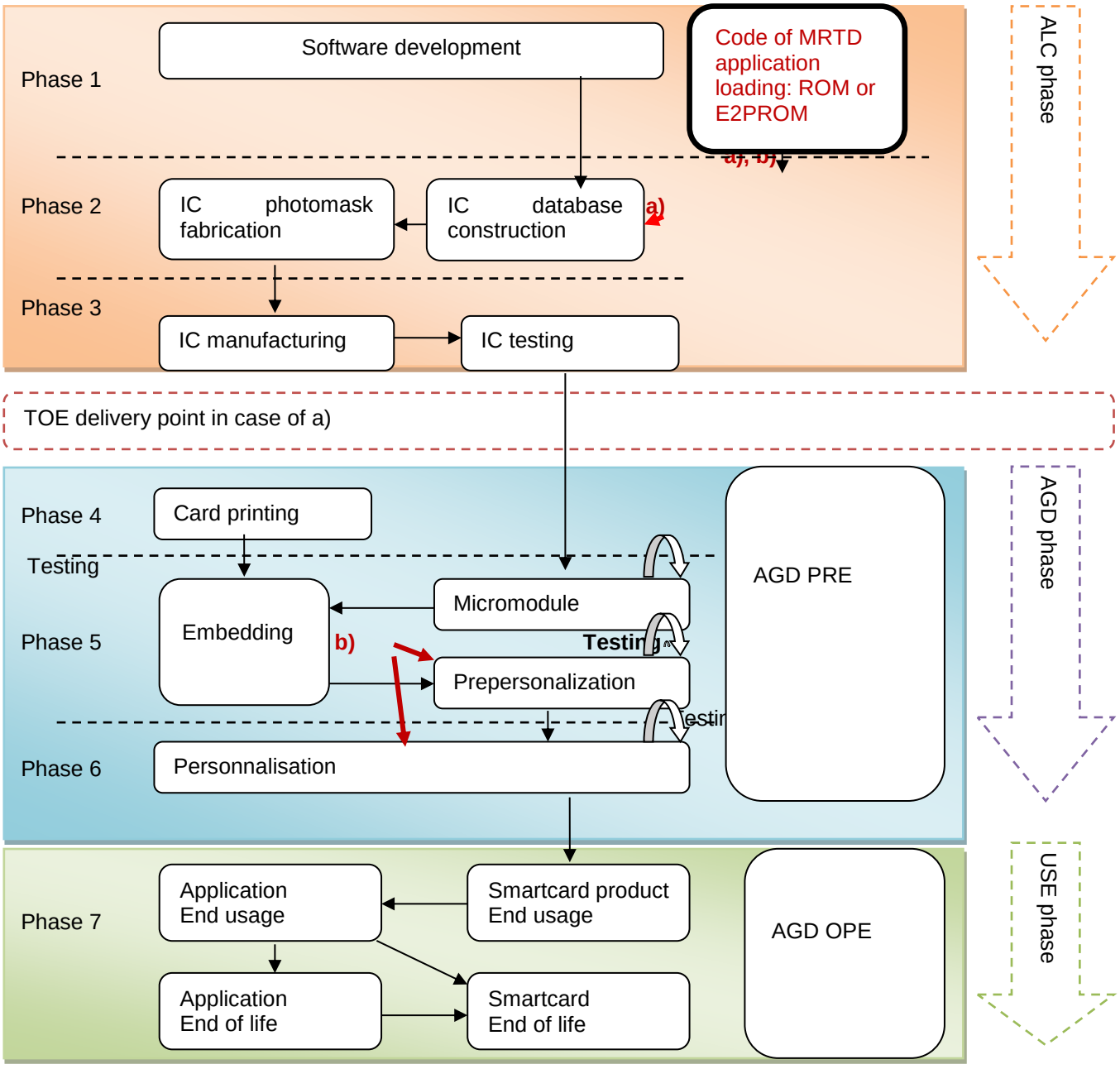


Figure 3: Smartcard product life-cycle for the TOE

The TOE life-cycle classically described in terms of four life-cycle phases, is additionally subdivided into 7 steps.

The roles involved in the different steps are listed in the following table:

Roles	Subjects
IC manufacturer	NXP Semiconductors
TOE developer	Oberthur Technologies
Manufacturer	NXP Semiconductors

	Oberthur Technologies or another agent
Prepersonalizer	Oberthur Technologies or another agent
Personalization Agent	Oberthur Technologies or another agent

Table 10: Roles Identification on the life cycle.

3.2. TOE Life Cycle when the Application code is romed

The table below presents the subjects following TOE life cycle steps in accordance with the standard smart card life cycle, the Protection Profile lifecycle in phases, the TOE delivery point and the coverage in the case a).

Steps	Phase	Subject	Covered by	Sites
Step 1	Development	Oberthur Technologies	ALC R&D sites	-Pessac and Colombes for platform and -Manille for Taiwan eID Applet CC application development
Step 2	Development	NXP Semiconductors	IC certification	IC certification
Step 3	Manufacturing	NXP Semiconductors	IC certification	IC certification
TOE delivery point				
Step 4	Manufacturing	MRD Manufacturer (Prepersonalizer)	AGD_PRE	
Step 5	Manufacturing	MRD Manufacturer (Prepersonalizer)	AGD_PRE	
Step 6	Personalization	Personalization Agent	AGD_PRE	
Step 7	Operational Use	End user	AGD_OPE	

Table 11: Subjects identification following life cycle steps

Details for each phase/step are presented in the following paragraphs.

3.3. Phase 1 “Development”

(Step1) The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.
The TOE includes the Taiwan eID Applet CC application and the Platform.
The LDS is developed at Manille and the platform at Colombes and Pessac.
The sites are audited following MSSR last requirements.

(Step2) The TOE developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the MRTD application and the guidance documentation associated with these TOE components.

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the eMRTD application and the guidance documentation is securely delivered to the Manufacturer.

3.4. Phase 2 “Manufacturing”

(Step3) In a first step the TOE integrated circuit is produced containing the travel document’s chip Dedicated Software and the parts of the travel document’s chip Embedded Software in the non-volatile

non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as travel document material during the IC manufacturing and the *delivery process to the Manufacturer. The IC is securely delivered from the IC manufacture to the* Manufacturer. If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM). The IC manufacturer adds initialization data in EEPROM and keys (MSK, LSK).

The end of step 3 is the TOE delivery.

(Step4) The Manufacturer combines the IC with hardware for the contact based / contactless interface in the travel document unless the travel document consists of the card only.

(Step5) The Manufacturer (i) adds the IC Embedded Software (ii) creates the eMRTD application, and (iii) equips travel document's chips with pre-personalization Data.

The pre-personalised travel document together with the IC Identifier is securely delivered from the Manufacturer to the Personalization Agent. The Manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

3.5. Phase 3 "Personalization of the travel document"

(Step6) The personalization of the travel document includes:
(i) the survey of the travel document holder's biographical data,
(ii) the enrolment of the travel document holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
(iii) the personalization of the visual readable data onto the physical part of the travel document,
(iv) the writing of the TOE User Data and TSF Data into the logical travel document and
(v) configuration of the TSF if necessary.

The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of
(i) the digital MRZ data (EF.DG1),
(ii) the digitized portrait (EF.DG2), and
(iii) the Document security object. The signing of the Document security object by the Document signer finalizes the personalization of the genuine travel document for the travel document holder.
The personalised travel document (together with appropriate guidance for TOE use if necessary) is handed over to the travel document holder for operational use.

3.5.1. Loading of application

The platform can host 2 kinds of applications: Evaluated sensitive applications and validated basic applications. Once the application is evaluated or validated, it is securely delivered to manufacturing site. This delivery ensures the integrity and confidentiality of the application code and data. Then applications code and data are securely stored.
The delivery, storage and loading of any application are covered by audited Organisational measures (ALC).

Applications can be loaded at pre issuance at step 5 or at step 6 or in post issuance.

3.5.2. Applet pre-personalisation (phase 6)

This phase is performed by the Personalisation Agent, which controls the TOE. During this phase, the javacard applet is prepared as required by P.TOE_Construction.
All along this phase, the TOE is self-protected as it requires the authentication of the Personalisation Agent prior to any operation.

3.5.3. TOE personalisation (phase 6)

This phase is performed by the Personalisation Agent, which controls the TOE, which is in charge of the javacard applet personalisation.
All along this phase, the TOE is self-protected as it requires the authentication of the Personalisation Agent prior to any operation.
This phase may not necessarily take place in a manufacturing site, but may be performed anywhere. The Personalisation Agent is responsible for ensuring a sufficient level of security during this phase.
The javacard applet is personalized according to guidance document [57].

At the end of phase 6, the TOE is constructed.

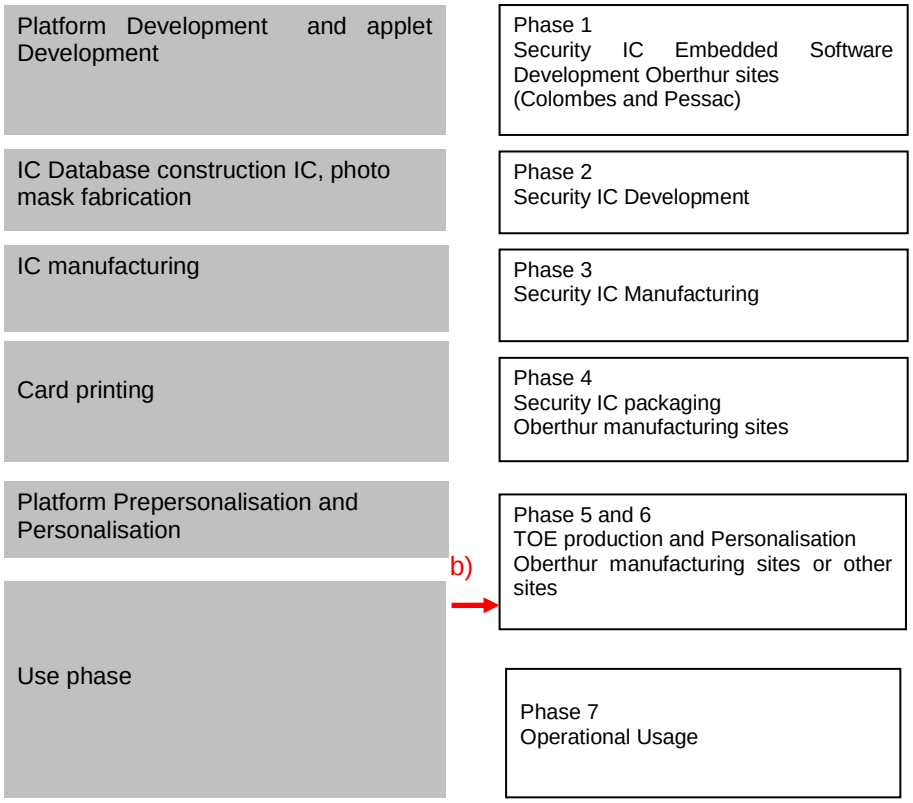
3.6. Phase 4 "Operational Use"

(Step7) The TOE is used as a travel document's chip by the traveller and the inspection systems in the "Operational Use" phase. The user data can be read according to the security policy of the issuing State or Organisation and can be used according to the security policy of the issuing State but they can never be modified.

Note that the personalization process and its environment may depend on specific security needs of an issuing State or Organisation. All production, generation and installation procedures after TOE delivery up to the "Operational Use" (phase 4) have to be considered in the product evaluation process under AGD assurance class. Therefore, the Security Target has to outline the split up of P.Manufact, P.Personalization and the related security objectives into aspects relevant before vs. after TOE delivery. Some production steps, e.g. Step 4 in Phase 2 may also take place in the Phase 3.

3.7. TOE Life Cycle when the Application code is loaded in E2prom

This chapter presents when the application in loaded in E2prom, case b.



!

Figure 4: Smartcard product life-cycle for the TOE when the application is loaded in E2prom.

When the Taiwan eID Applet CC application is loaded on the Platform at Phase 5; the entity responsible of the loading is the manufacturer:

- The Manufacturer (phase 5) loads the Taiwan eID Applet CC application code (ii) creates the eMRTD application, and (iii) equips travel document's chips with pre-personalization Data.
- The pre-personalised travel document together with the IC Identifier is securely delivered from the Manufacturer to the Personalization Agent. The Manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent (AGD_PRE).

When the Taiwan eID Applet CC application is loaded on the Platform at Phase 6; the entity responsible of the loading is the Personalization Agent:

- The Personalization Agent (phase 6) loads the Taiwan eID Applet CC application code (ii) creates the eMRTD application, and (iii) equips travel document's chips with pre-personalization Data.
- The MRTD is also personalized, in this step, as defined in the chapter 3.5.3.
- The personalization phase can also occur in phase 7, by the Issuer.

When the Taiwan eID Applet CC application is loaded on the Platform at Phase 7; the entity responsible of the loading is the issuer, the Prepersonalization and the personalisation of the MRTD is under the Issuer responsibility. All required information is securely given (application code and AGD_PRE and AGD_OPE). The loading follows Platform requirements as defined in the COSMO V8.1-N Application Loading Protection Guidance [55].

Step	Possible operations	Required document form the platform	Required document form the application
Step 5	MRD Manufacturer (Prepersonalizer) Loading and Prepersonalization	COSMO V8.1-N Application Loading Protection Guidance [55]	Application code Personalization Manual [60]
Step 6	Loading and Prepersonalization and personalisation	COSMO V8.1-N Application Loading Protection Guidance [55]	Application code Personalization Manual [60]
Step 7	Loading and Prepersonalization and personalisation	COSMO V8.1-N Application Loading Protection Guidance [55]	Application code Personalization Manual [60] User Manual [61]

Table 12: Required inputs for each case

4. CONFORMANCE CLAIM

4.1. Conformance claim

This security target claims conformance to the Common Criteria version 3.1, revision 4 ([1][2][3]).
The conformance to the Common Criteria is claimed as follows:

CC	Conformance rationale
Part 1	Strict conformance
Part 2	Conformance to the extended[1] 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	Strict conformance to Part 3. The product claims conformance to EAL 5, augmented with: ALC_DVS.2 “Sufficiency of security measures” AVA_VAN.5 ”Advanced methodical vulnerability analysis”

Table 13: Conformance Rationale

4.2. Protection Profile claims

This security target claims a strict conformance to the following protection profile:

- BSI-CC-PP-0056-V1.10-2009: ”Machine Readable Travel Document with “ICAO Application”, Extended Access control” [48]

4.3. Protection Profile Additions

The rationale between the SPD, taking into account the additional elements of the SPD, and the Objectives and Objectives on the operational environment are given in the paragraph Rationales.

4.3.1. SFR dispatch versus PP

The following table present a rationale between the SFR driven from the protection profile versus the SFR from this security target:

SFR from the PP	Dispatch in the ST (detailed SFR in chapter 8]
FAU_SAS.1	FAU_SAS.1/MP
FCS_CKM.1	FCS_CKM.1/CA_DH_SM_3DES FCS_CKM.1/CA_ECDH_SM_3DES FCS_CKM.1/CA_DH_SM_AES FCS_CKM.1/CA_ECDH_SM_AES FCS_CKM.1/BAC
FCS_CKM.4	FCS_CKM.4/Global
FCS_COP.1/SHA	FCS_COP.1/CA_SHA_SM_3DES FCS_COP.1/CA_SHA_SM_AES FCS_COP.1/TA_SHA_ECC FCS_COP.1/TA_SHA_RSA FCS_COP.1/BAC_SHA

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

SFR from the PP	Dispatch in the ST (detailed SFR in chapter 8]
FCS_COP.1/SYM	FCS_COP.1/CA_SYM_SM_3DES FCS_COP.1/CA_SYM_SM_AES FCS_COP.1/BAC_AUTH FCS_COP.1/BAC_ENC FCS_COP.1/BAC_MAC
FCS_COP.1/MAC	FCS_COP.1/CA_MAC_SM_3DES FCS_COP.1/CA_MAC_SM_AES
FCS_COP.1/SIG_VER	FCS_COP.1/TA_SIG_VER_ECC FCS_COP.1/TA_SIG_VER_RSA
FCS_RND.1	FCS_RND.1/Global
FIA_UID.1	FIA_UID.1/CA
FIA_UAU.1	FIA_UAU.1/CA
FIA_UAU.4	FIA_UAU.4/MP_3DES FIA_UAU.4/MP_AES FIA_UAU.4/TA FIA_UAU.4/BAC
FIA_UAU.5	FIA_UAU.5/CA_3DES FIA_UAU.5/CA_AES FIA_UAU.5/EAC FIA_UAU.5/MP_3DES FIA_UAU.5/MP_AES
FIA_UAU.6	FIA_UAU.6/CA
FIA_API.1	FIA_API.1/CA
FDP_ACC.1	FDP_ACC.1/EAC
FDP_ACF.1	FDP_ACF.1/EAC
FDP_UCT.1	FDP_UCT.1/CA FDP_UCT.1/BAC
FDP_UIT.1	FDP_UIT.1/CA FDP_UIT.1/BAC
FMT_SMF.1	FMT_SMF.1/MP
FMT_SMR.1	FMT_SMR.1/MP FMT_SMR.1/TA
FMT_LIM.1	FMT_LIM.1/Global FMT_LIM.1/EAC FMT_LIM.1/BAC
FMT_LIM.2	FMT_LIM.2/Global FMT_LIM.2/EAC FMT_LIM.2/BAC
FMT_MTD.1/INI_ENA	FMT_MTD.1/MP_INI_ENA
FMT_MTD.1/INI_DIS	FMT_MTD.1/MP_INI_DIS
FMT_MTD.1/CVCA_INI	FMT_MTD.1/TA_CVCA_INI
FMT_MTD.1/CVCA_UPD	FMT_MTD.1/TA_CVCA_UPD
FMT_MTD.1/DATE	FMT_MTD.1/TA_CVCA_DATE
FMT_MTD.1/KEY_WRITE	FMT_MTD.1/BAC_KEY_WRITE
FMT_MTD.1/CAPK	FMT_MTD.1/CA_KEY_WRITE
FMT_MTD.1/KEY_READ	FMT_MTD.1/MP_KEY_READ FMT_MTD.1/BAC_KEY_READ FMT_MTD.1/CA_KEY_READ
FMT_MTD.3	FMT_MTD.3/EAC
FPT_EMS.1	FPT_EMS.1/Global FPT_EMS.1/MP FPT_EMS.1/CA FPT_EMS.1/MP_Add_code
FPT_FLS.1	FPT_FLS.1/Global
FPT_TST.1	FPT_TST.1/Global FPT_TST.1/CA FPT_TST.1/TA FPT_TST.1/BAC
FPT_PHP.3	FPT_PHP.3.1/Global
FAU_SAS.1	FAU_SAS.1/MP

SFR from the PP	Dispatch in the ST (detailed SFR in chapter 8]
FCS_CKM.1	FCS_CKM.1/CA_DH_SM_3DES FCS_CKM.1/CA_ECDH_SM_3DES FCS_CKM.1/CA_DH_SM_AES FCS_CKM.1/CA_ECDH_SM_AES FCS_CKM.1/BAC
FCS_CKM.4	FCS_CKM.4/Global

Table 14: PP SFR

4.3.2. Overview of the SFR defined in this ST

Notation:
For optimisation and ease read, all the SFR presented in chapter Security Functional Requirements have extensions as presented here:
SFR (**/Global)** that are global to the product (shared between the various TOE)
SFR (/**MP**) that are dedicated for the Personalization phases
SFR (/**AA**) that are dedicated for Active Authentication
SFR (/**BAC**) that are dedicated for Basic Access Control
SFR (/**CA**) that are dedicated for Chip Authentication
SFR (/**TA**) that are dedicated for Terminal Authentication
SFR (/**EAC**) that are dedicated for Extended Access Control

4.3.3. Complete overview of the SFR

From the PP, the following table lists the SFR defined in the ST with the generic notation.

SFR from the PP
FAU_SAS.1; FCS_CKM.1; FCS_CKM.4; FCS_COP.1/SHA ; FCS_COP.1/SYM ; FCS_COP.1/MAC ; FCS_COP.1/SIG_VER ; FCS_RND.1; FIA_UID.1; FIA_UAU.1; FIA_UAU.4 ; FIA_UAU.5; FIA_UAU.6 ; FIA_API.1 ; FDP_ACC.1 ; FDP_ACF.1 ; FDP_UCT.1 ; FDP_UIT.1 ; FMT_SMF.1; FMT_SMR.1; FMT_LIM.1; FMT_LIM.2 FMT_MTD.1/INI_ENA ; FMT_MTD.1/INI_DIS ; FMT_MTD.1/CVCA_INI ; FMT_MTD.1/CVCA_UPD ; FMT_MTD.1/DATE ; FMT_MTD.1/KEY_WRITE ; FMT_MTD.1/CAPK; FMT_MTD.1/KEY_READ; FMT_MTD.3; FPT_EMS.1 ; FPT_FLS.1; FPT_TST.1; FPT_PHP.3

Table 15: SFR from the PP

The following table presents the additional SFRs and express its functionality.

Section	Additional SFR
MP	FCS_CKM.1/MP ; FCS_COP.1/MP ; FDP_ACC.2/MP ; FDP_ACF.1/MP ; FDP_ITC.1/MP ; FDP_UCT.1/MP ; FDP_UIT.1/MP ; FIA_AFL.1/MP ; FIA_UAU.1/MP ; FIA_UID.1/MP ; FIA_UAU.4/MP ; FIA_UAU.5/MP ; FMT_MTD.1/MP ; FTP_ITC.1/MP ; FMT_MTD.1/MP_KEY_READ ; FMT_MTD.1/MP_KEY_WRITE
Active Authentication	FCS_COP.1/AA ; FDP_DAU.1/AA ; FDP_ITC.1/AA ; FMT_MTD.1/AA_KEY_READ ; FMT_MOF.1/AA ; FMT_MTD.1/AA_KEY_WRITE

Section	Additional SFR
Additional functionality	FMT_MTD.1/SM_LVL, FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE, FMT_MTD.1/UPD_FILE

Table 16: Additional SFR

The following table presents Global SFR overview:

Global SFR	Additional?	ST generic notation
FCS_CKM.4/Global	No	FCS_CKM.4
FCS_RND.1/Global	No	FCS_RND.1
FMT_LIM.1/Global	No	FMT_LIM.1
FMT_LIM.2/Global	No	FMT_LIM.2
FPT_EMS.1/Global	No	FPT_EMS.1
FPT_FLS.1/Global	No	FPT_FLS.1
FPT_TST.1/Global	No	FPT_TST.1
FPT_PHP.3/Global	No	FPT_PHP.3

Table 17: Global SFR overview

The following table presents the dedicated SFRs for Active Authentication (AA)

Active Auth. SFR	AdditionalSFR?	ST generic notation
FCS_COP.1/AA_DSA FCS_COP.1/AA_ECDSA	Yes	FCS_COP.1/AA
FDP_DAU.1/AA	Yes	FDP_DAU.1/AA
FDP_ITC.1/AA	Yes	FDP_ITC.1/AA
FMT_MTD.1/AA_KEY_READ	Yes	FMT_MTD.1/AA_KEY_READ
FPT_EMS.1/AA	No	FPT_EMS.1
FMT_MOF.1/AA	Yes	FMT_MOF.1/AA
FMT_MTD.1/AA_KEY_WRITE	Yes	FMT_MTD.1/AA_KEY_WRITE

Table 18: Additional SFR for the Active Authentication

The following table presents the SFRs for BAC PP, all are issued from the PP.

BAC SFR	Additional?	ST generic notation
FCS_CKM.1/BAC	No	FCS_CKM.1
FCS_COP.1/BAC_AUTH FCS_COP.1/BAC_ENC FCS_COP.1/BAC_MAC	No	FCS_COP.1/AUTH FCS_COP.1/ENC FCS_COP.1/MAC
FCS_COP.1/BAC_SHA	No	FCS_COP.1/SHA
FDP_UCT.1/BAC	No	FDP_UCT.1
FDP_UIT.1/BAC	No	FDP_UIT.1
FMT_MTD.1/BAC_KEY_READ	No	FMT_MTD.1/KEY_READ
FMT_LIM.1/BAC	No	FMT_LIM.1
FMT_LIM.2/BAC	No	FMT_LIM.2
FPT_TST.1/BAC	No	FPT_TST.1
FMT_MTD.1/BAC_KEY_WRITE	No	FMT_MTD.1/KEY_WRITE
FDP_ACC.1/BAC	No	FDP_ACC.1
FDP_ACF.1/BAC	No	FDP_ACF.1
FMT_SMR.1/BAC	No	FMT_SMR.1
FIA_AFL.1/BAC	No	FIA_AFL.1
FIA_UAU.6/BAC	No	FIA_UAU.6
FIA_UID.1/BAC	No	FIA_UID.1
FIA_UAU.1/BAC	No	FIA_UAU.1

BAC SFR	Additional?	ST generic notation
FIA_UAU.4/BAC	No	FIA_UAU.4
FIA_UAU.5/BAC	No	FIA_UAU.5

Table 19: BAC SFR overview

CA SFR overview:

CA SFR	Additional?	ST generic notation
FIA_API.1/CA	No	FIA_API.1
FCS_CKM.1/CA_DH_SM_3DES FCS_CKM.1/CA_ECDH_SM_3DES FCS_CKM.1/CA_DH_SM_AES FCS_CKM.1/CA_ECDH_SM_AES	No	FCS_CKM.1
FCS_COP.1/CA_SHA_SM_3DES FCS_COP.1/CA_SYM_SM_3DES FCS_COP.1/CA_MAC_SM_3DES FCS_COP.1/CA_SHA_SM_AES FCS_COP.1/CA_SYM_SM_AES FCS_COP.1/CA_MAC_SM_AES	No	FCS_COP.1
FIA_UAU.1/CA	No	FIA_UAU.1
FIA_UAU.5/CA_3DES FIA_UAU.5/CA_AES	No	FIA_UAU.5
FIA_UAU.6/CA	No	FIA_UAU.6
FIA_UID.1/CA	No	FIA_UID.1
FPT_EMS.1/CA	No	FPT_EMS.1
FPT_TST.1/CA	No	FPT_TST.1
FMT_MTD.1/CA_KEY_WRITE	No	FMT_MTD.1/CAPK
FMT_MTD.1/CA_KEY_READ	No	FMT_MTD.1/KEY_READ
FDP_UCT.1/CA	No	FDP_UCT.1
FDP_UIT.1/CA	No	FDP_UIT.1

Table 20: CA SFR overview

TA SFR	Additional?	ST generic notation
FCS_COP.1/TA_SHA_ECC FCS_COP.1/TA_SHA_RSA FCS_COP.1/TA_SIG_VER_ECC FCS_COP.1/TA_SIG_VER_RSA	No	FCS_COP.1
FIA_UAU.4/TA	No	FIA_UAU.4
FMT_MTD.1/TA_CVCA_UPD	No	FMT_MTD.1/CVCA_UPD
FMT_MTD.1/TA_CVCA_DATE	No	FMT_MTD.1/DATE
FPT_TST.1/TA	No	FPT_TST.1
FMT_SMR.1/TA	No	FMT_SMR.1
FMT_MTD.1/TA_CVCA_INI	No	FMT_MTD.1/CVCA_INI

Table 21: TA SFR overview

EAC SFR	Additional?	Dispatch in the ST
FDP_ACC.1/EAC	No	FDP_ACC.1
FDP_ACF.1/EAC	No	FDP_ACF.1
FMT_MTD.3/EAC	No	FMT_MTD.3
FIA_UAU.5/EAC	No	FIA_UAU.5
FMT_LIM.1/EAC	No	FMT_LIM.1

FMT_LIM.2/EAC	No	FMT_LIM.2

Table 22: EAC SFR overview

Additional fonctionality SFR	Additional?	Dispatch in the ST
FDP_ACC.1/UPD_FILE	No	FDP_ACC.1/UPD_FILE
FDP_ACF.1/UPD_FILE	No	FDP_ACF.1/UPD_FILE
FMT_MTD.1/UPD-FILE	No	FMT_MTD.1/UPD-FILE
FMT_MTD.1/SM_LVL	No	FMT_MTD.1/SM_LVL

Table 23: Additional functionality SFR overview

4.3.4. Overview of the additional protocols

4.3.4.1. Active Authentication

The additional functionality of Active Authentication (AA) is based on the ICAO PKI V1.1 and the related on-card generation of RSA and ECC keys.
It implies the following addition to the standard PP:

- Additional Threats: **§ 5.3.2**
- Additional Objective: **§ 6.1.2**
- Additional OSP: **§ 5.4.2**
- Additional Assumptions: **§ 5.5.2**

4.3.4.2. Prepersonalization phase

The prepersonalization phase has been reinforced in this Security Target, with the following elements. This functionality is usable in phase 5 and phase 6. Once the product is locked, stated as personalized, it is no more possible to perform this operation.

4.3.5. Rationale for the additions

In order to be compliant with the CEM, a rationale is given for the additional Objectives on the Environment, such as to demonstrate that they neither mitigates a threat or fulfil an OSP.

4.3.5.1. OE for AA rationale

The objectives **OE.Exam_MRTD_AA, OE.Prot_Logical_MRTD_AA, OE.Activ_Auth_Verif** and **OE.Activ_Auth_Sign** define additional requirements on the operational environment for the Active Authentication Protocol which is not in the original scope of the PP BAC. This OE is only linked to threat and OSP for the Active Authentication and has no links with those of the PP.

4.3.5.2. Assumption for AA rationale

The **A.Insp_Sys_AA is added, this assumption is only linked to Active Authentication mechanism as the** Inspection System **has to implement** the mechanism and shall verify the authenticity of the MRTD's chip during inspection using the signature returned by the TOE during Active Authentication.

5. SECURITY PROBLEM DEFINITION

5.1. Subjects

SFR	Before phase 5	Phase 5	Phase 6	Phase 7
PP BAC subjects				
Manufacturer	x	x		
Personalization Agent			x	
Terminal		x	x	x
Inspection System				x
MRTD Holder				x
Traveler				x
Attacker	x	x	x	x
Additional subjects				
IC Developer	x			
Software Developer	x			
Prepersonalizer (refinement of Manufacturer. It corresponds to the MRTD manufacturer)		x		

Table 24: Subjects and phases

5.1.1. PP EAC

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 cycle phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
This entity is commensurate with 'Manufacturer' in [47].

Personalisation Agent
An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities:

- Establishing the identity of the travel document holder for the biographic data in the travel document
- Enrolling the biometric reference data of the travel document holder
- Writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [43]
- Writing the document details data
- Writing the initial TSF data
- Signing the Document Security Object defined in [43] (in the role of DS).

Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer.
This entity is commensurate with 'Personalisation agent' in [47].

Application Note
Personalization Agent is refered as the Personalizer in the Security Target

Document Verifier
The Document Verifier (DV) enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations in the form of the Document Verifier Certificates.

Terminal
A terminal is any technical system communicating with the TOE either through the contact interface or through the contactless interface.

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.

Country Verifying Certification Authority (CVCA)
The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organization with respect to the protection of sensitive biometric reference data stored in the MRTD. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link-Certificates.

Travel document holder (MRTD holder)
A person for whom the travel document Issuer has personalised the travel document. This entity is commensurate with 'MRTD Holder' in [47]. Please note that a travel document holder can also be an attacker.

Travel document presenter (Traveler)
A person presenting the travel document to a terminal and claiming the identity of the travel document holder. This external entity is commensurate with 'Traveller' in [47]. Please note that a travel document presenter can also be an attacker (s. below).

Attacker
A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the assets having to be maintained. The attacker is assumed to possess an at most high attack potential.
Please note that the attacker might 'capture' any subject role recognised by the TOE.
This external entity is commensurate with 'Attacker' in [47].

5.1.2. Additional Subjects

IC Developer
Developer of the IC.

TOE Developer
Developer of part of the TOE source code.

Prepersonalizer
Agent in charge of the Prepersonalization. This agent corresponds to the MRTD manufacturer as described in [47].

5.2. Assets

All these data may be sorted out in two different categories:
If they are specific to the user, they are User data.
If they ensure the correct behaviour of the application, they are TSF Data.

5.2.1. User data

Logical MRTD data
The logical MRTD data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [43]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG 16 contain personal data of the MRTD holder. The Chip Authentication Public Key (CAPK) in EF.DG 14 is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.
The Active Authentication Public Key (AAPK) Info in DG 15 is used by the inspection system for Active Authentication of the chip.

The current EAC Security Target is dedicated to the protection of both Active Authentication EF.DG15 (see below) and sensitive biometric EF.DG3&4.
The other one (and associated keys) are described and managed in the related BAC Security Target.

User Data	Description
CPLC Data	Data uniquely identifying the chip. They are considered as user data as they enable to track the holder
Personnal Data of the MRTD holder (EF.DGx, except EF.DG15)	Contains identification data of the holder
Document Security Object (SOD) in EF.SOD	Contain a certificate ensuring the integrity of the file stored within the MRTD and their authenticity. It ensures the data are issued by a genuine country
Common data in EF.COM	Declare the data the travel document contains. This data is optional and may be absent in the TOE
Active Authentication Public Key in EF.DG15 (AAPK)	Contains public data enabling to authenticate the chip thanks to the Active Authentication
Chip Authentication Public Key in EF.DG14 (CAPK)	Contains public data enabling to authenticate the chip thanks to the Chip Authentication Protocol
Updatable Data	Data other than Personal Data, Biometric Data, EF.COM, EF.SOD, CA_PK, CA_SK, AA_PK, AA_SK, CPLC, TOE_ID, Pre-Perso_K, Perso_K, Session_K, Configuration Data which can be modified in Operational Use phase.

Table 25: User Data

Authenticity of the travel document's chip
The authenticity of the travel document's chip personalised by the issuing State or Organisation for the travel document holder is used by the traveller to prove his possession of a genuine travel document.

5.2.2. TSF data

TSF Data	Description
TOE_ID	Data enabling to identify the TOE

TSF Data	Description
Prepersonalizer reference authentication data	Private key enabling to authenticate the Prepersonalizer
Personalization Agent reference authentication Data	Private key enabling to authenticate the Personalization Agent
Basic Access Control (BAC) Key	Master keys used to established a trusted channel between the Basic Inspection Terminal and the travel document
Active Authentication private key (AAK)	Private key the chip uses to perform an Active Authentication
Chip Authentication private key (CAK)	Private key the chip uses to perform a Chip Authentication
Session keys for the secure channel	Session keys used to protect the communication in confidentiality, authenticity and integrity
Life Cycle State	Life Cycle state of the TOE

Table 26: TSF Data

5.3. Threats

This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the TOE method of use in the operational environment and the assets stored in or protected by the TOE.

Application note: The threats T.Chip_ID and T.Skimming (cf [47]) are averted by the mechanisms described in the BAC PP which cannot withstand an attack with high attack potential thus these are not addressed here. T.Chip_ID addresses the threat of tracing the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface. T.Skimming addresses the threat of imitating the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. Both attacks are conducted by an attacker who cannot read the MRZ or who does not know the physical MRTD in advance.

5.3.1. PP EAC

T.Read_Sensitive_Data
Adverse action
An attacker tries to gain the sensitive biometric reference data through the communication interface of the MRTD's chip. The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [47]) in respect of the attack path (communication interface) and the motivation (to get data stored on the MRTD's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing Document Basic Access Keys) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the MRTD's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical MRTD as well.
Threat agent
Having high attack potential, knowing the Document Basic Access Keys, being in possession of a legitimate MRTD
Asset
Confidentiality of sensitive logical MRTD (i.e. biometric reference) data

T.Forgery
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.

T.Counterfeit

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 traveller 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

T.Abuse-Func

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.

T.Information_Leakage

Adverse action

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

Threat agent

having high attack potential.

Asset

confidentiality of User Data and TSF-data of the travel document.

Application note: 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 Differential Electromagnetic Analysis (DEMA) and Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis)..

T.Phys-Tamper

Adverse action

An attacker may perform physical probing of the travel document in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the travel document in order to alter (I) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the travel document.
Threat agent
having high attack potential, being in possession of one or more legitimate travel documents.
Asset
integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document.

Application note: Physical tampering may be focused directly on the disclosure or manipulation of the user data (e.g. authentication key of the travel document) 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 a direct interaction with the travel document's internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of the user data and the TSF data may also be a pre-requisite. The modification may result in the deactivation of a security function, the biometric reference data for the inspection system) or the TSF data (e.g.

T.Malfunction
Adverse action
An attacker may cause a malfunction the travel document's hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE' hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the travel document outside the normal operating conditions, exploiting errors in the travel document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.
Threat agent
having high attack potential, being in possession of one or more legitimate travel documents, having information about the functional operation.
Asset
integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document.

Application note: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the threat T.PhysTamper) assuming a detailed knowledge about TOE's internals.

5.3.2. AA

T.Counterfeit
The definition is in the previous chapter.

5.3.3. Additional Threats

T.Forgery_Supplemental_Data "Forgery of supplemental data stored in the TOE"
Adverse action
An attacker alters fraudulently the data stored in files other than EF.DG1 to EF.DG16, EF.COM and EF document security object. This may lead the extended inspection system (EIS) using these data to be deceived.
Threat agent
having high attack potential, being in possession of one or more legitimate MRTDs.
Asset
authenticity of data stored in files other than EF.DG1 to EF.DG16, EF.COM and EF document security object

5.4. Organisational Security Policies

The TOE shall comply with the following Organisational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organisation upon its operations.

5.4.1. PP EAC

P.BAC-PP
The issuing States or Organizations ensures that successfully authenticated Basic Inspection Systems have read access to logical MRTD data DG1, DG2, DG5 to DG16 the "ICAO Doc 9303" [43] as well as to the data groups Common and Security Data. The MRTD is successfully evaluated and certified in accordance with the "Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control" [47] in order to ensure the confidentiality of standard user data and preventing the traceability of the MRTD data.

Application note: The organizational security policy P.Personal_Data drawn from the 'ICAO Doc 9303' [43] is addressed by the [47] (cf. P.BAC-PP). The confidentiality of the personal data other than EF.DG3 and EF.DG4 is ensured by the BAC mechanism. Note the BAC mechanisms may not resist attacks with high attack potential (cf. [47]). The TOE shall protect the sensitive biometric reference data in EF.DG3 and EF.DG4 against attacks with high attack potential. Due to the different resistance the protection of EF.DG3 and EF.DG4 on one side and the other EF.SOD, EF.COM, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 are addressed separated protection profiles, which is assumed to result in technically separated evaluations (at least for classes ASE and VAN) and certificates.

P.Sensitive_Data
The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the MRTD holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the MRTD is presented to the inspection system (Extended Inspection Systems). The issuing State or Organization authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The MRTD's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication.

P.Manufact

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.

P.Personalization
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.

5.4.2. AA

P.Activ_Auth

The terminal implements the Active Authentication protocol as described in [43].

5.5. Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

5.5.1. PP EAC

A.MRTD_Manufact
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).

A.MRTD_Delivery
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.

A.Pers_Agent
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.

A.Insp_Sys
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. 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. The General Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism. The Extended Inspection System in addition to the General Inspection System (i) supports 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.

A.Signature_PKI
The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical MRTD. The issuing State or Organization runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the MRTDs. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organizations.

A.Auth_PKI
The issuing and receiving States or Organizations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organizations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organizations. The issuing States or Organizations distribute the public keys of their Country Verifying Certification Authority to their MRTD's chip.

5.5.2. Assumptions for Active Authentication

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.

6. SECURITY OBJECTIVES

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment. The security objectives for the TOE environment are separated into security objectives for the development and production environment and security objectives for the operational environment.

6.1. 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.

6.1.1. SO from PP EAC

OT.AC_Pers
The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [43] 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.

Application note:
The OT.AC_Pers implies that the data of the LDS groups written during personalisation for travel document holder (at least EF.DG1 and EF.DG2) can not be changed using write access after personalisation.

OT.Data_Int
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 the integrity of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication data.

OT.Sens_Data_Conf
The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) by granting read access only to authorized Extended Inspection Systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the certificate chain to the Country Verifier Certification Authority of the issuing State or Organization. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks with high attack potential.

OT.Identification
The TOE must provide means to store IC Identification and Pre-Personalization Data in its nonvolatile 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). The storage of the Prepersonalization data includes writing of the Personalization Agent Key(s).

OT.CA_Proof
The TOE must support the General 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. The authenticity proof provided by the MRTD's chip shall be protected against attacks with high attack potential.

OT.Prot_Abuse-Func
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
- (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.

OT.Prot_Inf_Leak
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.

OT.Prot_Phys-Tamper
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.

OT.Prot_Malfunction
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.

6.1.2. SO for AA

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 [43]. The authenticity proof through AA provided by MRTD’s chip shall be protected against attacks with high attack potential.

OT.Data_Int_AA
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 the integrity of the logical MRTD data during their transmission to the General Inspection System after Active Authentication.

6.1.3. Additional SO

OT.Update_File “Modification of file in Operational Use Phase”
During Operational Use phase, the TOE must allow the modification of Updatable Data if the write access to these objects is fulfilled by the Terminal.

OT.AC_SM_Level “Access control to sensitive biometric reference data according to SM level”
During Operational Use phase, the TOE must allow read access to sensitive biometric data only if the Secure Messaging level reaches or exceeds the one specified in the biometric data Access Conditions data object.

6.2. Security objectives for the Operational Environment

6.2.1. PP EAC

6.2.1.1. Issuing State or Organization

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

OE.MRTD_Manufact
Appropriate functionality testing of the TOE shall be used in step 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.ok

OE.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 rejectd 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.

OE.Personalization
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.

OE.Pass_Auth_Sign
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 [43].

OE.Auth_Key_MRTD
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

- (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.

OE.Authoriz_Sens_Data
The issuing State or Organization has to establish the necessary public key infrastructure in order to limit the access to sensitive biometric reference data of MRTD's holders to authorized receiving States or Organizations. The Country Verifying Certification Authority of the issuing State or Organization generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.

OE.BAC_PP
It has to be ensured by the issuing State or Organization, that the TOE is additionally successfully evaluated and certified in accordance with the "Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control" [47]. This is necessary to cover the BAC mechanism ensuring the confidentiality of standard user data and preventing the traceability of the MRTD data. Note that due to the differences within the assumed attack potential the addressed evaluation and certification is a technically separated process.

6.2.1.2. Receiving State or Organization

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

OE.Exam_MRTD
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 [43].

OE.Passive_Auth_Verif
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.

OE.Prot_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).

OE.Ext_Insp_Systems
The Document Verifier of receiving States or Organizations authorizes Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive biometric reference data of the logical MRTD. The Extended Inspection System authenticates themselves to the MRTD's chip for access to the sensitive biometric reference data with its private Terminal Authentication Key and its Inspection System Certificate.

6.2.2. OE for AA

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.

OE.Prot_Logical_MRTD_AA
Aditionally to the OE.Prot_Logical_MRTD, the inspection system prevents eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Active Authentication Protocol.

OE.Activ_Auth_Verif
In addition to the verification by passive authentication, the inspection systems may use the verification by Active Authentication, which offers a stronger guaranty of the authenticity of the MRTD.

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. EXTENDED REQUIREMENTS

7.1. Extended family FAU_SAS - Audit data storage

7.1.1. Extended components FAU_SAS.1

Description: see [47].

FAU_SAS.1 Audit storage

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

Dependencies: No dependencies.

Rationale: see [47]

7.2. Extended family FCS_RND - Generation of random numbers

7.2.1. Extended component FCS_RND.1

Description: see [47]

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].
Dependencies: No dependencies.
Rationale: See [47]

7.3. Extended family FIA_API – Authentication proof of identity

7.3.1. Extended component FIA_API.1

Description: see [48]

FIA_API.1 Quality metric for random numbers

FIA_API.1.1 The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: authorized user or role].
Dependencies: No dependencies.
Rationale: See [48]

7.4. Extended family FMT_LIM - Limited capabilities and availability

7.4.1. Extended component FMT_LIM.1

Description: see [47]

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].

Dependencies: (FMT_LIM.2)

Rationale: See [47]

7.4.2. Extended component FMT_LIM.2

Description: See [47]

FMT_LIM.2 Limited availability

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

Dependencies: (FMT_LIM.1)

Rationale: See [47]

7.5. Extended family FPT_EMS - TOE Emanation

7.5.1. Extended component FPT_EMS.1

Description: see [47]

FPT_EMS.1 TOE Emanation

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

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

Dependencies: No dependencies.

Rationale: See [47]

8. SECURITY REQUIREMENTS

8.1. Security Functional Requirements

This chapter presents the Security Functional Requirements to take into account within the TOE configuration presented in this security target. It is composed of the following elements:

- **Global SFR** that are applicable to all the passports configuration
- **MP SFR** for covering the phase Manufacturing and Personalization described in the Passport Protection Profile.
- **Active Authentication SFR** that cover the Active Authentication Protocol
- **BAC SFR** that cover the Basic Access Control
- **CA SFR** that cover the Chip Authentication Protocol
- **TA SFR** that cover the Terminal Authentication Protocol (note: Terminal Authentication Protocol is only available with the Extended Access Control)
- **EAC SFR** that cover the Extended Access Control (note: EAC protocol is a combination of TA and CA, this chapter only contains SFR that cannot be strictly applied to one or another)
- And **Additional SFRs** to cover additional functionalities of the TOE. See chapter 8.1.8.

8.1.1. Global SFR

This chapter covers the common SFR that are shared between the different parts of the embedded application on the product.

FCS_CKM.4/Global Cryptographic key destruction

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

FCS_RND.1/Global Quality metric for random numbers

FCS_RND.1.1/Global The TSF shall provide a mechanism to generate random numbers that meet

1. The requirement to provide an entropy of at least 7.976 bits in each byte, following AIS 31[34] and
2. The requirement of **FIPS SP800-90 [18]**for random number generation.

FMT_LIM.1/Global Limited capabilities

FMT_LIM.1.1/Global 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:

1. User Data to be manipulated
2. TSF data to be disclosed or manipulated
3. Software to be reconstructed
4. Substantial information about construction of TSF to be gathered which may enable other attacks

FMT_LIM.2/Global Limited availability

FMT_LIM.2.1/Global 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

1. User Data to be manipulated
2. TSF data to be disclosed or manipulated

3. Software to be reconstructed
4. Substantial information about construction of TSF to be gathered which may enable other attacks

FPT_EMS.1/Global TOE Emanation

FPT_EMS.1.1/Global The TOE shall not emit power variations, timing variations during command execution in excess of non useful information enabling access to
1. EF.COM, EF.SOD and EF.DG1 to EF.DG16

FPT_EMS.1.2/Global The TSF shall ensure any **unauthorized users** are unable to use the following interface **smart card circuit contacts** to gain access to
1. EF.COM, EF.SOD and EF.DG1 to EF.DG16

FPT_FLS.1/Global Failure with preservation of secure state

FPT_FLS.1.1/Global The TSF shall preserve a secure state when the following types of failures occur:
1. Exposure to out-of-range operating conditions where therefore a malfunction could occur
2. Failure detected by TSF according to FPT_TST.1.

FPT_TST.1/Global TSF testing

FPT_TST.1.1/Global The TSF shall run a suite of self tests to demonstrate the correct operation of **the TSF, at the conditions:**

At reset
Before any cryptographic operation
When accessing a DG or any EF
Prior to any use of TSF data
Before execution of any command

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

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

FPT_PHP.3/Global Resistance to physical attack

FPT_PHP.3.1/Global The TSF shall resist **physical manipulation and physical probing** to the **TSF** by responding automatically such that the SFRs are always enforced.

8.1.2. Product configuration SFR

This chapter adds some requirements on Manufacturing and Personalization SFR.

FCS_CKM.1/MP Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[cryptographic key generation algorithm]** and specified cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic key generation algorithm	Key length (bits)	Standards
MSK derivation from initial MSK loaded in phase 1 using SHA 256	256	None

FCS_COP.1/MP_ENC_3DES Cryptographic operation

FCS_COP.1.1/MP_ENC_3DES 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	Algo	Key length (bits)	Standard
Secure Messaging – encryption and decryption	3DES in CBC mode	112	[13][12]

FCS_COP.1/MP_ENC_AES Cryptographic operation

FCS_COP.1.1/MP_ENC_AES 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	Algo	Key length (bits)	Standard
Secure Messaging – encryption and decryption	AES in CBC mode	128, 192 and 256	[17]

FCS_COP.1/MP_MAC_3DES Cryptographic operation

FCS_COP.1.1/MP_MAC_3DES 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	Algo	Key length (bits)	Standard
Secure Messaging – MAC	3DES RMAC	112	[15][13][12]

FCS_COP.1/MP_MAC_AES Cryptographic operation

FCS_COP.1.1/MP_MAC_AES 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	Algo	Key length (bits)	Standard
Secure Messaging MAC	AES	128, 192 and 256	[17]

FCS_COP.1/MP_AUTH_3DES Cryptographic operation

FCS_COP.1.1/MP_AUTH_3DES 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	Algo	Key length (bits)	Standard
Card Manufacturer Authentication (MSK)	3DES	112	[12]

FCS_COP.1/MP_AUTH_AES Cryptographic operation

FCS_COP.1.1/MP_AUTH_AES 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	Algo	Key length (bits)	Standard
Card Manufacturer Authentication (MSK)	AES	128, 192 and 256	[17]

FCS_COP.1/MP_SHA Cryptographic operation

FCS_COP.1.1/MP_SHA 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	Algo	Key length (bits)	Standard
Hashing	SHA256	None	[29]

FDP_ACC.2/MP Complete access control

FDP_ACC.2.1/MP The TSF shall enforce the **Prepersonalization Access Control** on **all subjects and all objects** and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/MP The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1/MP Security attribute based access control

FDP_ACF.1.1/**MP** The TSF shall enforce the **Prepersonalization Access Control** to objects based on the following **Prepersonalizer Authentication (AS_AUTH_MSK_STATUS).**

FDP_ACF.1.2/MP The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **AS_AUTH_MSK_STATUS=TRUE (EXTERNAL AUTHENTICATE)**.

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

FDP_ACF.1.4/MP The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**.

Application Note
This SFR enforces access control over all the operation in phase 5.

AS_AUTH_MSK_STATUS is related to authentication status or the prepersonalizer. If the Authentication is successful, the AS_AUTH_MSK_STATUS is set to true. Otherwise the AS_AUTH_MSK_STATUS is set to false.

FDP_ITC.1/MP Import of user data without security attributes

FDP_ITC.1.1/MP The TSF shall enforce the **Prepersonalization access control** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/MP The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/MP The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **none**.

Application Note
This SFR control import of data in phase 5.
This SFR ensures also the MSK diversification, which is performs once, at first command, without any security requirements preliminary to this action.

FDP_UCT.1/MP Basic data exchange confidentiality

FDP_UCT.1.1/MP The TSF shall enforce the **Prepersonalization access control** to **receive** user data in a manner protected from unauthorised disclosure.

FDP_UIT.1/MP Data exchange integrity

FDP_UIT.1.1/MP The TSF shall enforce the **Prepersonalization Access Control SFP** to **receive** user data in a manner protected from **modification** errors

FDP_UIT.1.2/MP [Editorially refined] The TSF shall be able to determine on receipt of user data, whether modification of some pieces of the application sent by the Prepersonalizer has occurred

FIA_AFL.1/MP Authentication failure handling

FIA_AFL.1.1/MP The TSF shall detect when **3** unsuccessful authentication attempts occur related to **authentication of**
1. Prepersonalizer
FIA_AFL.1.2/MP When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **forbid any authentication attempt as Personalizer**.

FIA_UAU.1/MP Timing of authentication

FIA_UAU.1.1/MP The TSF shall allow **GET DATA, SELECT FILE** on behalf of the user to be performed before the user is authenticated.

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

FIA_UID.1/MP Timing of identification

FIA_UID.1.1/MP The TSF shall allow **GET DATA, SELECT FILE** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2/MP The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4/MP_3DES Single-use authentication mechanisms

FIA_UAU.4.1/MP_3DES The TSF shall prevent reuse of authentication data related to
1. Authentication Mechanisms based on 3DES

FIA_UAU.4/MP_AES Single-use authentication mechanisms

FIA_UAU.4.1/MP_AES The TSF shall prevent reuse of authentication data related to
1. Authentication Mechanisms based on AES

FIA_UAU.5/MP_3DES Multiple authentication mechanisms

FIA_UAU.5.1/MP_3DES The TSF shall provide
1. Symmetric Authentication Mechanism based on 3DES
to support user authentication.

FIA_UAU.5.2/MP_3DES The TSF shall authenticate any user's claimed identity according to the
1. The TOE accepts the authentication attempt as Personalization Agent by the Symmetric Authentication Mechanism with the Personalization Agent Key

FIA_UAU.5/MP_AES Multiple authentication mechanisms

FIA_UAU.5.1/MP_AES The TSF shall provide
1. Symmetric Authentication Mechanism based on AES to support user authentication.

FIA_UAU.5.2/MP_AES The TSF shall authenticate any user's claimed identity according to the
1. The TOE accepts the authentication attempt as Personalization Agent by the Symmetric Authentication Mechanism with Personalization Agent Key

FMT_MTD.1/MP Management of TSF data

FMT_MTD.1.1/MP The TSF shall restrict the ability to switch the TOE life cycle from phase 5 to phase 6 to the Prepersonalizer.

FTP_ITC.1/MP Inter-TSF trusted channel

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

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

FTP_ITC.1.3/MP The TSF shall initiate communication via the trusted channel for:
1. Personalization Agent key storage
2. Life cycle transition from Prepersonalization to Personalization phase

FMT_MTD.1/MP_INI_ENA Management of TSF data

FMT_MTD.1.1/MP_INI_ENA The TSF shall restrict the ability to write the Initialization Data and Prepersonalization Data to the Prepersonalizer.

FMT_MTD.1/MP_INI_DIS Management of TSF data

FMT_MTD.1.1/MP_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/MP_KEY_READ Management of TSF data

FMT_MTD.1.1/MP_KEY_READ The TSF shall restrict the ability to read the [data] to [authorized identified roles]:

TSF Data	Authorized Identified roles
MSK	None
Personalization Agent Keys	None

FMT_MTD.1/MP_KEY_WRITE Management of TSF data

FMT_MTD.1.1/MP_KEY_WRITE The TSF shall restrict the ability to write the [data] to [authorized identified roles]:

TSF Data	Authorized Identified roles
MSK	IC manufacturer (created by the developer)
Personalization Agent Keys	None

FAU_SAS.1/MP Audit storage

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

FMT_SMF.1/MP Specification of Management Functions

FMT_SMF.1.1/MP The TSF shall be capable of performing the following management functions:
1. Initialization
2. Pre-personalization
3. Personalization

FMT_SMR.1/MP Security roles

FMT_SMR.1.1/MP The TSF shall maintain the roles
1. Manufacturer
2. Personalization Agent

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

FPT_EMS.1/MP TOE Emanation

FPT_EMS.1.1/MP The TOE shall not emit power variations, timing variations during command execution in excess of non useful information enabling access to
1. Prepersonalizer Key
2. Personalization Agent Key
3. MSK

FPT_EMS.1.2/MP The TSF shall ensure any **unauthorized users** are unable to use the following interface **smart card circuit contacts** to gain access to
1. Prepersonalizer Key
2. Personalization Agent Key
3. MSK

8.1.3. Active Authentication SFR

FCS_COP.1/AA_DSA Cryptographic operation

FCS_COP.1.1/AA_DSA 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]**:

Operation	Algorithm	Key length (bits)	Standard
Digital Signature Creation	RSA signature (CRT) with SHA1, 224, 256, 384, 512	1024, 1536 and 2048.	[24]

FCS_COP.1/AA_ECDSA Cryptographic operation

FCS_COP.1.1/AA_ECDSA 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]**:

Operation	Algo	Key length (bits)	Standard
Digital Signature Creation	ECDSA with SHA1, 224, 256, 384, 512	192 to 512 over prime field curves	[24] [28][29][30]

FDP_DAU.1/AA Basic Data Authentication

FDP_DAU.1.1/AA The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **the TOE itself**.

FDP_DAU.1.2/AA The TSF shall provide **any users** with the ability to verify evidence of the validity of the indicated information.

Refinement:
Evidence generation and ability of verifying it constitute the Active Authentication protocol.

FDP_ITC.1/AA Import of user data without security attributes

FDP_ITC.1.1/AA The TSF shall enforce the **Active Authentication Access Control SFP** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/AA The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/AA The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **none**.

FMT_MTD.1/AA_KEY_READ Management of TSF data

FMT_MTD.1.1/AA_KEY_READ The TSF shall restrict the ability to **read** the **AAK** to **none**.

FPT_EMS.1/AA TOE Emanation

FPT_EMS.1.1/AA The TOE shall not emit power variations, timing variations during command execution in excess of non useful information enabling access to
1. Active Authentication: Private Key (AAK)

FPT_EMS.1.2/AA The TSF shall ensure any **unauthorized users** are unable to use the following interface **smart card circuit contacts** to gain access to
1. Active Authentication: Private Key (AAK)

FMT_MOF.1/AA Management of security functions behaviour

FMT_MOF.1.1/AA The TSF shall restrict the ability to disable and enable the functions TSF Active Authentication to Personalization Agent.

FMT_MTD.1/AA_KEY_WRITE Management of TSF data

FMT_MTD.1.1/AA_KEY_WRITE The TSF shall restrict the ability to write the AAK to Personalization Agent.

8.1.4. Basic Access Control SFR

FCS_CKM.1/BAC Cryptographic key generation

FCS_CKM.1.1/BAC The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[cryptographic key generation algorithm]** and specified cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic key generation algorithm	Key length (bits)	Standards
Document Basic Access Key Derivation Algorithm	112	[43]

FCS_COP.1/BAC_AUTH Cryptographic operation

FCS_COP.1.1/BAC_AUTH 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	Algo	Key length (bits)	Standard
Symmetric authentication, encryption and decryption	3DES	112	[12]

FCS_COP.1/BAC_SHA Cryptographic operation

FCS_COP.1.1/BAC_SHA 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	Algo	Key length (bits)	Standard
Hashing	SHA1	None	[29]

FCS_COP.1/BAC_ENC Cryptographic operation

FCS_COP.1.1/BAC_ENC 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	Algo	Key length (bits)	Standard
Secure Messaging (BAC) – encryption and decryption	3DES in CBC mode	112	[17][12]

FCS_COP.1/BAC_MAC Cryptographic operation

FCS_COP.1.1/BAC_MAC 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	Algo	Key length (bits)	Standard
Secure Messaging MAC	Retail MAC	112	[47]

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_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

FMT_MTD.1/BAC_KEY_READ Management of TSF data

FMT_MTD.1.1/BAC_KEY_READ The TSF shall restrict the ability to read the [data] to [authorized identified roles]:

TSF Data	Authorized Identified roles
Document Access Keys	None

FMT_LIM.1/BAC Limited capabilities

FMT_LIM.1.1/BAC 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

1. User Data to be disclosed

FMT_LIM.2/BAC Limited availability

FMT_LIM.2.1/BAC 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
1. User Data to be disclosed

FPT_TST.1/BAC TSF testing

FPT_TST.1.1/BAC The TSF shall run a suite of self tests to demonstrate the correct operation of **the TSF, at the conditions:**
When performing a BAC authentication

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

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

FMT_MTD.1/BAC_KEY_WRITE Management of TSF data

FMT_MTD.1.1/BAC_KEY_WRITE The TSF shall restrict the ability to [selection the [list of TSF data] to [authorized identified roles]:

	List of TSF data	Authorised role
Write	Document Basic Access Keys	Personalization Agent

8.1.5. Chip Authentication SFR

FIA_API.1/CA Authentication Proof of Identity

FIA_API.1.1/CA The TSF shall provide a **Chip Authentication protocol according [48] to** prove the identity of the TOE.

FCS_CKM.1/CA_DH_SM_3DES Cryptographic key generation

FCS_CKM.1.1/CA_DH_SM_3DES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[cryptographic key generation algorithm]** and specified cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic key generation algorithm	Key length (bits)	Standards
Algorithm based on the Key Diffie-Hellman key derivation protocol compliant to PKCS#3	112	[28]

FCS_CKM.1/CA_DH_SM_AES Cryptographic key generation

FCS_CKM.1.1/CA_DH_SM_AES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[cryptographic key generation algorithm]** and specified cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic key generation algorithm	Key length (bits)	Standards
Algorithm based on the Key Diffie-Hellman key derivation protocol compliant to PKCS#3	128, 192, 256	[28]

FCS_CKM.1/CA_ECDH_SM_3DES Cryptographic key generation

FCS_CKM.1.1/CA_ECDH_SM_3DES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[cryptographic key generation algorithm]** and specified cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic key generation algorithm	Key length (bits)	Standards
Algorithm based on ECDH key derivation protocol compliant to ISO 15946	112	[39]

FCS_CKM.1/CA_ECDH_SM_AES Cryptographic key generation

FCS_CKM.1.1/CA_ECDH_SM_AES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[cryptographic key generation algorithm]** and specified cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic key generation algorithm	Key length (bits)	Standards
Algorithm based on ECDH key derivation protocol compliant to ISO 15946	128, 192, 256	[39]

FCS_COP.1/CA_SHA_SM_3DES Cryptographic key generation

FCS_COP.1.1/CA_SHA_SM_3DES The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
SHA1	None	[29]

FCS_COP.1/CA_SHA_SM_AES Cryptographic key generation

FCS_COP.1.1/CA_SHA_SM_AES The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
SHA1	None	[29]

FCS_COP.1/CA_SYM_SM_3DES Cryptographic key generation

FCS_COP.1.1/CA_SYM_SM_3DES The TSF shall perform **SM encryption and decryption** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
3DES CBC mode	112	[48]

FCS_COP.1/CA_SYM_SM_AES Cryptographic key generation

FCS_COP.1.1/CA_SYM_SM_AES The TSF shall perform **SM encryption and decryption** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
AES	128, 192 and 256	[48]

FCS_COP.1/CA_MAC_SM_3DES Cryptographic key generation

FCS_COP.1.1/CA_MAC_SM_3DES The TSF shall perform **SM message authentication code** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
3DES Retail MAC	112	[15]

FCS_COP.1/CA_MAC_SM_AES Cryptographic key generation

FCS_COP.1.1/CA_MAC_SM_AES The TSF shall perform **SM message authentication code** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
AES CMAC	128, 192 and 256	[48]

FIA_UAU.1/CA Timing of authentication

FIA_UAU.1.1/CA The TSF shall allow:
1. To establish the communication channel
2. To read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
3. To identify themselves by selection of the authentication key
4. To carry out the Chip Authentication Protocol
on behalf of the user to be performed before the user is authenticated.

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

FIA_UAU.5/CA_3DES Multiple authentication mechanisms

FIA_UAU.5.1/CA_3DES The TSF shall provide
1. Secure Messaging in MAC-ENC mode
2. Symmetric Authentication Mechanism based on 3DES
to support user authentication.

FIA_UAU.5.2/CA_3DES The TSF shall authenticate any user's claimed identity according to the
1. After run of the Chip Authentication Protocol 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.

FIA_UAU.5/CA_AES Multiple authentication mechanisms

FIA_UAU.5.1/CA_AES The TSF shall provide
1. Secure Messaging in MAC-ENC mode
2. Symmetric Authentication Mechanism based on AES
to support user authentication.

FIA_UAU.5.2/CA_AES The TSF shall authenticate any user's claimed identity according to the
1. After run of the Chip Authentication Protocol 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.

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 CA shall be verified as being sent by the inspection system.**

FIA_UID.1/CA Timing of identification

FIA_UID.1.1/CA The TSF shall allow
1. To establish the communication channel
2. To read the Initialization Data if it is not disbled by TSF according to FMT_MTD.1/INI_DIS
3. To carry out th Chip Authentication Protocol
on behalf of the user to be performed before the user is identified.

FIA_UID.1.2/CA The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FPT_EMS.1/CA TOE Emanation

FPT_EMS.1.1/CA The TOE shall not emit **power variations, timing variations during command execution** in excess of **non useful information** enabling access to
1. Chip Authentication: Session Keys, Private Key (CAK)

FPT_EMS.1.2/CA The TSF shall ensure any **unauthorized users** are unable to use the following interface **smart card circuit contacts** to gain access to
1. Active Authentication: Session Keys, Private Key (CAK)

FPT_TST.1/CA TSF testing

FPT_TST.1.1/CA The TSF shall run a suite of self tests to demonstrate the correct operation of **the TSF, at the conditions:**
When performing the Chip Authentication

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

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

FMT_MTD.1/CA_KEY_WRITE Management of TSF data

FMT_MTD.1.1/CA_KEY_WRITE The TSF shall restrict the ability to **write** the **CAK** to **Personalization Agent.**

FMT_MTD.1/CA_KEY_READ Management of TSF data

FMT_MTD.1.1/CA_KEY_READ The TSF shall restrict the ability to **read** the **CAK** to **none**.

FDP_UCT.1/CA Basic data exchange confidentiality

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

FDP_UIT.1/CA Data exchange integrity

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

8.1.6. Terminal Authentication SFR

FCS_COP.1/TA_SHA_RSA Cryptographic key generation

FCS_COP.1.1/TA_SHA_RSA The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
SHA1, SHA256 and SHA 512	**None**	**[29]**

FCS_COP.1/TA_SHA_SM_ECC Cryptographic key generation

FCS_COP.1.1/TA_SHA_SM_ECC The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
SHA1, SHA224, SHA256, SHA384 and SHA512	**None**	**[29]**

FCS_COP.1/TA_SIG_VER_RSA Cryptographic key generation

FCS_COP.1.1/TA_SIG_VER_RSA The TSF shall perform **digital signature verification** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
RSA coupled with SHA	**From 1024 to 4096, with a step of 256**	**[45]**

FCS_COP.1/TA_SIG_VER_ECC Cryptographic key generation

FCS_COP.1.1/TA_SIG_VER_ECC The TSF shall perform **digital signature verification** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
ECC coupled with SHA	**From 192 to 521**	**[45]**

FIA_UAU.4/TA Single-use authentication mechanisms

FIA_UAU.4.1/TA The TSF shall prevent reuse of authentication data related to
1. Terminal Authentication Protocol

FMT_MTD.1/TA_CVCA_UPD Management of TSF data

FMT_MTD.1.1/TA_CVCA_UPD The TSF shall **restrict** the ability **to update** the
1. Country Verifying Certification Authority Public Key
2. Country Verifying Certification Authority Certificate
to **Country Verifying Certification Authority.**

FMT_MTD.1/TA_DATE Management of TSF data

FMT_MTD.1.1/TA_DATE The TSF shall **restrict** the ability **to modify** the **Current Date** to
1. Country Verifying Certification Authority
2. Document Verifier
3. Domestic Extended Inspection System

FPT_TST.1/TA TSF testing

FPT_TST.1.1/TA The TSF shall run a suite of self tests to demonstrate the correct operation of **the TSF, at the conditions:**

- **When using the CVCA Root key**
- **When verifying a certificate with an extracted public key**
- **When performing a Terminal authentication**

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

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

FMT_SMR.1/TA Security roles

FMT_SMR.1.1/TA The TSF shall maintain the roles
1. Country Verifying Certification Authority
2. Document Verifier
3. Domestic Extended Inspection System
4. Foreign Extended Inspection System

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

FMT_MTD.1/TA_CVCA_INI Management of TSF data

FMT_MTD.1.1/TA_CVCA_INI The TSF shall **restrict** the ability **to write** the
1. Initial Country Verifying Certification Authority Public Key
2. Initial Country Verifying Certification Authority Certificate
3. Initial Current Date
to **the Personalization Agent**

8.1.7. Extended Access Control SFR

FDP_ACC.1/EAC Subset access control

FDP_ACC.1.1/EAC The TSF shall enforce the **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_ACF.1/EAC Security attribute based access control

FDP_ACF.1.1/EAC The TSF shall enforce the **Access Control SFP** to objects based on the following:
1. Subjects
- **a. Personalization Agent**
- **b. Extended Inspection System**
- **c. Terminal**

2. Objects
- **a. Data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD**
- **b. Data EF.DG3 and EF.DG4 of the logical MRTD**
- **c. Data in EF.COM**
- **d. Data in EF.SOD**

3. Security attributes
- **a. Authentication status of terminals**
- **b. Terminal Authorization**

FDP_ACF.1.2/EAC The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
1. 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
2. The successfully authenticated EIS with the read access to DG3 (Fingerprint) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG3 of the logical MRTD
3. The successfully authenticated EIS with the read access to DG4 (Iris) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG4 of the logical MRTD

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

FDP_ACF.1.4/EAC The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
1. A terminal authenticated as CVCA is not allowed to read data in the EF.DG3
2. A terminal authenticated as CVCA is not allowed to read data in the EF.DG4
3. A terminal authenticated as DV is not allowed to read data in the EF.DG3
4. A terminal authenticated as DV is not allowed to read data in the EF.DG4
5. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD
6. Any terminal not being successfully authenticated as Extended Inspection System is not allowed to read any of the EF.DG3 to EF.DG4 of the logical MRTD

Application Note:
Note the BAC mechanism controls the read access of the EF.COM, EF.SOD, EF.DG1, EF.DG2, EF.DG5 to EF.DG16 of the logical MRTD. According to P.BAC-PP this security features of the MRTD are not subject of this protection profile.

FMT_MTD.3/EAC Secure TSF data

FMT_MTD.3.1/EAC [Editorially Refined] The TSF shall ensure that only secure values of **the certificate chain** are accepted for **TSF data of the Terminal Authentication Protocol and the Access Control.**

Refinement:
The Certificate chain is valid if and only if:
1- The digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE
2- The digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE
3- The digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE.

The Inspection System Public Key contained in the Inspection System Certificate in a valid certificate chain is a secure value for the authentication reference data of the Extended Inspection System.

The intersection of the Certificate Holder Authorizations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorization of a successful authenticated Extended Inspection System.

FIA_UAU.5/EAC Multiple authentication mechanisms

FIA_UAU.5.1/EAC The TSF shall provide
1. Terminal Authentication Protocol
2. Secure messaging in MAC-ENC mode
to support user authentication.

FIA_UAU.5.2/EAC The TSF shall authenticate any user's claimed identity according to the
1. 1. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses the public key presented during the Chip Authentication Protocol and the secure messaging established by the Chip Authentication Mechanism

FMT_LIM.1/EAC Limited capabilities

FMT_LIM.1.1/EAC 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
1. Sensitive User Data (EF.DG3 and EF.DG4) to be disclosed (not available for BAC)

FMT_LIM.2/EAC Limited availability

FMT_LIM.2.1/EAC 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

1. User Data to be disclosed

8.1.8. Additional SFR

FDP_ACC.1 "Subset access control"

FDP_ACC.1.1/UPD_FILE
The TSF shall enforce the UPD_FILE Access Control SFP on terminals gaining write, read and modification access to data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD.

FDP_ACF.1 "Basic Security attribute based access control"

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

1. **Subjects:**
   a. **Personalization Agent,**
   b. **Extended Inspection System,**
   c. **Terminal,**
2. **Objects:**
   a. **data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD**
3. **Security attributes**
   a. **authentication status of terminals,**

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

1. **the Personalization Agent is allowed to write, read and modify the data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD,**
2. **the successfully authenticated Extended Inspection System with the name corresponding to the one (or beginning of the one) set following FMT_MTD.1.1/UPD_FILE is allowed to modify the data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD.**

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

1. the Personalization Agent is allowed to write, read and modify the data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD,
2. the successfully authenticated Extended Inspection System with the name corresponding to the one (or beginning of the one) set following FMT_MTD.1.1/UPD_FILE is allowed to modify the data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD.

FDP_ACF.1.3/UPD_FILEThe TSF shall explicitly authorise access of subjects to objects based on the f additional rules: none.

FMT_MTD.1 Management of TSF data".

FMT_MTD.1.1/UPD_FILE The TSF shall restrict the ability to **set the name (or beginning of the name) of the terminal allowed to modify files in phase 7, and identifiers of these files (different from EF.COM, EF.SOD, EF.DG1 to EF.DG16) to the Personalization Agent.**
Application note: Name of the terminal is the Card Holder Reference (CHR) of the EIS.
Beginning of the name is a string of the left most significant bytes of the CHR of the EIS.

FMT_MTD.1.1/SM_LVL The TSF shall restrict the ability to **set the minimum Secure Messaging level required to access DG 3 and DG 4 to the Personalization Agent**.

Application Note: Possible secure messaging levels are: DES, AES 128, AES 192 or AES 256.

8.2. Security Assurance Requirements

The security assurance requirement level is EAL5+ augmented with ALC_DVS.2, AVA_VAN.5.

8.2.1. Rationale for augmentation

8.2.1.1. 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.

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE. This assurance component is a higher hierarchical component to EAL5 (only ALC_DVS.1). Due to the nature of the TOE, there is a need for any justification of the sufficiency of these procedures to protect the confidentiality and integrity of the TOE.

The component ALC_DVS.2 augmented to EAL5 has no dependencies to other security requirements.

8.2.1.2. AVA_VAN.5 Advanced methodical vulnerability analysis

Due to the definition of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by the AVA_VAN.5 component.
Advanced methodical vulnerability analysis is based on highly detailed technical information. The attacker is assumed to be thoroughly familiar with the specific implementation of the TOE. The attacker is presumed to have a high level of technical sophistication. AVA_VAN.5 has dependencies with ADV_ARC.1 "Security architecture description", ADV_FSP.4 "Complete functional specification", ADV_IMP.1 "Implementation representation of the TSF", ADV_TDS.3 "Basic modular design", AGD_PRE.1 "Preparative procedures" and AGD_OPE.1 "Operational user Guidance" and ATE_DPT.1 "Testing: basic design".

All these dependencies are satisfied by EAL5.

9. TOE SUMMARY SPECIFICATION

9.1. 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:

- BAC keys
- Chip Authentication keys
- Active Authentication private key
- Personalization Agent keys
- MSK and LSK
- CVCA keys

It controls access to the CPLC data as well:
It ensures the CPLC data can be read during the personalization phase
It ensures it cannot be readable in free mode at the end of the personalization step.

Regarding the file structure:

In the operational use:

- The terminal can read user data (except DG3 & DG4), the Document Security Object, EF.CVA, EF.COM only after PACE authentication and through a valid secure channel.
- When the EAC was successfully performed, the terminal can only read the DG3 & DG4 provided the access rights are sufficient throught a valid secure channel.

In the personalization phase:

- The Personalization Agent can read all the data stored in the TOE after it is authenticated by the TOE (using its authentication keys).
- The TOE is uniquely identified by a random number, generated at each reset. This unique identifier is called (PUPI).

It ensures as well that no other part of the memory can be accessed at anytime

Access Control in writing

This function controls access to write functions (in EEPROM) 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.
It ensures as well the CPLC data cannot be written anymore once the TOE is personalized.

Regarding the file structure:

In the operational use:

It is not possible to create any files (system or data files). Furthermore, it is not possible to update any system files. However the application data is still accessed internally by the application for its own needs.
The root CVCA key files and temporary key files are updated internally by the application according to the authentication mechanism described in [45].

In the personalization phase

The Personalization Agent can create and write through a valid secure channel all the data files it needs after it is authenticated by the TOE (using its authentication keys).

Active Authentication
This security functionality ensures the Active Authentication is performed as described in [45]. (if it is activated by the personnaliser).

Chip Authentication
This security functionality ensures the Chip Authentication is performed as described in [45]. (if it is activated by the personnaliser). It could be used as an alternative of Active Authentication to reinforce the Authentication of the Chip. It differs from an EAC not performing the Terminal Authentication.

EAC mechanism
This security functionality ensures the EAC is correctly performed. In particular:
- It handles the certificate verification
- The management of the current date (update and control towards the expiration date of the incoming certificate)
- The signature verification (in the certificate or in the challenge/response mechanism)

It can only be performed once the TOE is personalized with the chip authentication keys & Root CVCA key(s) the Personnalization Agent loaded during the personalization phase. Furthermore, this security functionalities ensure that the authentication is performed as described in [45].
This security functionality ensures the session keys for secure messaging are destroyed at each successful Chip Authentication step.
The TOE handles an error counter; after several failures in attempting to strongly authenticate the GIS (the error limit is reached). The TOE also implements countermeasures to protect the TOE; it takes more and more time for the TOE to reply to subsequent wrong GIS authentication attempts.

Personalization
This security functionality ensures the TOE, when delivered to the Personnalization Agent, demands an authentication prior to any data exchange. This authentication is based on a symmetric Authentication mechanism based on a Triple DES or AES algorithm. This TSF can use a Secure Messaging described in the TSF Secure Messaging.

Physical protection
This security functionality protects the TOE against physical attacks.

Prepersonalization
This security functionality ensures the TOE, when delivered to the Prepersonalization Agent, demands an authentication prior to any data exchange. This authentication is based on a symmetric Authentication mechanism based on a Triple DES or AES algorithm. This function is in charge of pre-initializing the product. This TSF can use a Secure Messaging described in the TSF Secure Messaging.

Safe state management
This security functionalities ensures that the TOE gets back to a secure state when
- an integrity error is detected by F.SELFTESTS
- a tearing occurs (during a copy of data in EEPROM)

This security functionality ensures that such a case occurs, the TOE is either switched in the state "kill card" or becomes mute.

Secure Messaging
This security functionality ensures the confidentiality, authenticity & integrity of the communication between the TOE and the IFD.
After a successful PACE authentication and successful Chip Authentication, a secure channel is established based on Triple DES algorithm, and after a successful Chip Authentication , a secure channel is (re)established based on Symmetric algorithms (Triple DES, AES128, 192 or 256)
This security functionality ensures:
- No commands were inserted, modified nor deleted within the data flow
- The data exchanged remain confidential
- The issuer of the incoming commands and the destinatory of the outgoing data is the one that was authenticated (through PACE or EAC)

If an error occurs in the secure messaging layer, the session keys are destroyed.
This Secure Messaging can be combined with the Active Authentication.
This TSF can provide a GP Secure Messaging (SCP02 or SCP03) for the Prepersonalization or Personalization.

Self tests
The TOE performs self tests to verify the integrity on the TSF data:
- Before the TSF data usage
- The integrity of keys and sensitive data is ensured

9.2. Link between the SFR and the TSF

The following chapters present the rationales between security objective and security requirements. For ease reading some requirements are merged.

- FIA_UAU.4/MP represents the 2 SFRS: FIA_UAU.4/MP_3DES and FIA_UAU.4/MP_AES
as the 2 sfrs have the same functionalities, single use authentication mechanisms are used with the same scope. The only difference is the used algorithms.

- FIA_UAU.5/MP represents the 2 SFRS: FIA_UAU.5/MP_3DES and FIA_UAU.5/MP_AES
as the 2 sfrs have the same functionalities, Multiple use authentication mechanisms are used with the same scope. The only difference is the used algorithms.

- FCS_COP.1/MP represents the 7 SFRS: FCS_COP.1/MP_AUTH_3DES,
FCS_COP.1/MP_AUTH_AES, FCS_COP.1/MP_ENC_3DES, FCS_COP.1/MP_ENC_AES,
FCS_COP.1/MP_MAC_3DES, FCS_COP.1/MP_MAC_AES and FCS_COP.1/MP_SHA.

All the SFRs provide equivalent service at personalisation phase: cryptographic authentication of the personalisation. The differences are related to algorithms used for the authentication.

	FAU_SAS.1	FCS_CKM.1	FCS_CKM.4	FCS_COP.1/SHA	FCS_COP.1/SYM	FCS_COP.1/MAC	FCS_COP.1/SIG_VER	FCS_RND.1	FIA_UID.1	FIA_UAU.1	FIA_UAU.4	FIA_UAU.5	FIA_UAU.6	FIA_API.1	FDP_ACC.1	FDP_ACF.1	FDP_UCT.1	FDP_UIT.1	FMT_SMF.1	FMT_SMR.1	FMT_LIM.1	FMT_LIM.2	FMT_MTD.1/INI_ENA	FMT_MTD.1/INI_DIS	FMT_MTD.1/CVCA_INI	FMT_MTD.1/CVCA_UPD	FMT_MTD.1/DATE	FMT_MTD.1/KEY_WRITE	MT_MTD.1/CAPK	FMT_MTD.1/KEY_READ	FMT_MTD.3	FPT_EMS.1	FPT_FLS.1	FPT_TST.1	FPT_PHP.3
Access Control in reading									x	x	x	x	x		x	x	x	x						x						x	x				
Access Control in writing															x				x				x		x	x	x	x	x						
Active Authentication				x				x							x	x												x		x		x			
EAC mechanism			x	x		x	x	x	x	x	x	x	x	x		x	x	x								x	x				x	x			
Personalization				x				x											x													x			
Physical protection	x																				x	x													x
Prepersonalization				x		x		x	x										x													x			
Safe state management	x																		x	x	x	x											x		
Secure Messaging		x	x	x	x	x		x	x	x	x	x	x																					
Self tests								x																										x	

Table 27: Link between SFR from the EAC PP and TSF

	FCS_CKM.1/MP	FCS_COP.1/MP	FDP_ACC.2/MP	FDP_ACF.1/MP	FDP_ITC.1/MP	FDP_UCT.1/MP	FDP_UIT.1/MP	FIA_AFL.1/MP	FIA_UAU.1/MP	FIA_UID.1/MP	FIA_UAU.4/MP	FIA_UAU.5/MP	FMT_MTD.1/MP	FTP_ITC.1/MP	FMT_MTD.1/MP_KEY_READ	FMT_MTD.1/MP_KEY_WRITE
Access Control in reading			X	X					X	X					X	
Access Control in writing			X	X	X				X	X			X			X
Active Authentication																
EAC mechanism																
Personalization		X									X	X				
Physical protection																
Prepersonalization	X	X						X			X	X				
Safe state management																
Secure Messaging						X	X							X		
Self tests																

Table 28: Link between Additional SFR for MP and TSF

	FCS_COP.1/AA	FDP_DAU.1/AA	FDP_ITC.1/AA	FMT_MOF.1/AA	FMT_MTD.1/AA_KEY_WRITE	FMT_MTD.1/AA_KEY_READ
Access Control in reading						X
Access Control in writing			X	X	X	
Active Authentication	X	X	X	X	X	X

Table 29: Link between SFR for AA and TSF

	FDP_ACC.1/UPD_FILE	FDP_ACF.1/UPD_FILE	FMT_MTD.1/UPD_FILE	FMT_MTD.1.1/SM_LVL
Access Control in reading	x	x	x	x
Access Control in writing	x	x	x	x
Active Authentication				
EAC mechanism	x	x	x	
Personalization	x	x	x	x

Physical protection				
Prepersonalization	x	x	x	x
Safe state management				
Secure Messaging				
Self tests				

Table 30: Link between TSF and SFR of the Additions: UPD_FILE and SM_LVL

10. TOE RATIONALES SECURITY OBJECTIVES RATIONALE

Rationales are not provided in this public version.

11. ANNEX B: COMPOSITION WITH THE UNDERLYING JAVACARD OPEN PLATFORM

This annex discusses the composition with the underlying javacard platform [54] according to [6].This part is removed from the ST lite.