	Reference	D1390182	Release	1.2p <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level	Public	Pages	68

Sealys eTravel SCOSTA-CL V4 on NXP P60D081 Security Target Lite



	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

TABLE OF CONTENTS

1. REFERENCE DOCUMENTS	5
1.1. EXTERNAL REFERENCES [ER].....	5
1.2. INTERNAL REFERENCES [IR].....	5
2. ACRONYMS AND GLOSSARY	7
3. SECURITY TARGET INTRODUCTION	12
3.1. SECURITY TARGET IDENTIFICATION.....	12
3.2. TOE IDENTIFICATION	12
3.3. TOE OVERVIEW.....	13
4. TOE DESCRIPTION	14
4.1. TOE INTENDED USAGE	14
4.2. TOE BOUNDARIES	15
4.3. TOE LIFE-CYCLE.....	16
4.4. TOE ACTORS AND SITES	19
5. CONFORMANCE CLAIMS	20
6. SECURITY PROBLEM DEFINITION	21
6.1. ASSETS.....	21
6.2. USERS / SUBJECTS	21
6.3. THREATS.....	22
6.4. ORGANISATIONAL SECURITY POLICIES	24
6.5. SECURE USAGE ASSUMPTIONS.....	25
6.6. COMPOSITION TASKS – SECURITY PROBLEM DEFINITION PART	26
6.6.1. <i>Statement of Compatibility – Threats part</i>	26
6.6.2. <i>Statement of compatibility – OSPs part</i>	29
6.6.3. <i>Statement of compatibility – Assumptions part</i>	29
7. SECURITY OBJECTIVES	31
7.1. SECURITY OBJECTIVES FOR THE TOE.....	31
7.2. SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT	33
7.3. SECURITY OBJECTIVES RATIONALE	35
7.3.1. <i>Threats, OSPs and Assumptions coverage – Mapping table</i>	35
7.3.2. <i>Threats coverage – Rationale</i>	36
7.3.3. <i>OSP coverage – Rationale</i>	37
7.3.4. <i>Assumptions coverage – Rationale</i>	37
7.4. COMPOSITION TASKS – OBJECTIVES PART	37
7.4.1. <i>Statement of compatibility – TOE Objectives part</i>	37
7.4.2. <i>Statement of compatibility – ENV Objectives part</i>	41
8. EXTENDED COMPONENTS DEFINITION	43
8.1. EXTENDED FAMILY FAU_SAS – AUDIT DATA STORAGE	43

	Reference	D1390182	Release	1.2p
			(Printed copy not controlled: verify the version before using)	
	Classification Level	Public	Pages	68

8.1.1.	<i>Description</i>	43
8.1.2.	<i>Extended Components</i>	43
8.2.	EXTENDED FAMILY FCS_RND – GENERATION OF RANDOM NUMBERS	43
8.2.1.	<i>Description</i>	43
8.2.2.	<i>Extended Components</i>	43
8.3.	EXTENDED FAMILY FMT_LIM – LIMITED CAPABILITIES AND AVAILABILITY	44
8.3.1.	<i>Description</i>	44
8.3.2.	<i>Extended Components</i>	44
8.4.	EXTENDED FAMILY FPT_EMS – TOE EMANATION	45
8.4.1.	<i>Description</i>	45
8.4.2.	<i>Extended Components</i>	45
9.	SECURITY REQUIREMENTS	46
9.1.	SECURITY FUNCTIONAL REQUIREMENTS	46
9.1.1.	<i>Class FAU Security Audit</i>	46
9.1.2.	<i>Class FCS Cryptographic Support</i>	46
9.1.3.	<i>Class FIA Identification and authentication</i>	47
9.1.4.	<i>Class FDP User data protection</i>	49
9.1.5.	<i>Class FMT Security management</i>	50
9.1.6.	<i>Class FPT Protection of the security functions</i>	51
9.2.	SECURITY ASSURANCE REQUIREMENTS	52
9.3.	SECURITY REQUIREMENTS RATIONALE	52
9.3.1.	<i>TOE security objectives coverage – Mapping table</i>	52
9.3.2.	<i>TOE security objectives coverage – Rationale</i>	54
9.3.3.	<i>SFR dependency rationale</i>	55
9.3.4.	<i>SAR – Evaluation Assurance Level Rationale</i>	57
9.3.5.	<i>SAR – Dependency rationale</i>	57
9.4.	COMPOSITION TASKS – SFR PART	58
10.	TOE SUMMARY SPECIFICATION	66
10.1.	SEALYS eTRAVEL SCOSTA-CL EMBEDDED SOFTWARE	66
10.2.	P60D081 INTEGRATED CIRCUIT	67
10.3.	TSS MAPPING TABLE	67



	Reference	D1390182	Release	1.2p <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level	Public	Pages	68

TABLE OF FIGURES

FIGURE 1: TOE LOGICAL BOUNDARIES..... 16
 FIGURE 2: TOE LIFE CYCLE 18

TABLE OF TABLES

TABLE 1: PRODUCT AND TOE ACTORS..... 19
 TABLE 2: INVOLVED SITES UP TO THE TOE DELIVERY POINT 19
 TABLE 3: THREATS, OSPs AND ASSUMPTIONS COVERAGE BY SECURITY OBJECTIVES – MAPPING TABLE 35
 TABLE 4: TOE SECURITY OBJECTIVES COVERAGE BY SECURITY FUNCTIONAL REQUIREMENTS – MAPPING TABLE 53

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68


1. Reference documents


1.1. EXTERNAL REFERENCES [ER]

[ISO14443]	Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Books 1 to 4
[ISO 9797]	ISO/IEC 9797-1: 2011 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher
[AIS20/AIS31]	BSI, Application Notes and Interpretation of the Scheme (AIS) 20/31 – Functionality classes for random number generators, Version 2 (18.09.2011), English translation.
[SP800-67]	NIST Recommendation for the Triple Data Encryption Algorithm(TDEA) Block Cipher 2012
[FIPS180-4]	FIPS PUB 180-4 : Secure Hash Standard
[BIO]	9303 Part 9 – ICAO Machine Readable Travel Document Seventh edition 2015
[ICAO-9303]	9303 Part 10 and Part 11 – ICAO Machine Readable Travel Document Seventh edition 2015
[ICAO]	INTERNATIONAL CIVIL AVIATION ORGANIZATION FACILITATION (FAL) DIVISION, twelfth session (Cairo, Egypt, 22 March – 1 April 2004)
[PKI]	MRTD Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, International Civil Aviation Organization, Version 1.1, October 01 2004
[SS]	9303 Part 2 – ICAO Machine Readable Travel Document Seventh edition 2015
[SCOSTA-CL]	Specifications for the Smart-Card Operating System with Contact-less Interface, Version 1.2, July 6 th 2007, Government of India
[CC-1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012.
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.
[CEM]	Common Methodology for Information Technology Security Evaluation Methodology CCMB-2012-09-004, version 3.1 rev 4, September 2012
[PP-MRTD-BAC]	Common Criteria Protection Profile - Machine Readable Travel Document with ICAO Application, Basic Access Control Bundesamt für Sicherheit in der Informationstechnik BSI-PP-0055, version 1.10, 25th March 2009
[PP/0084]	Security IC Platform Protection Profile with Augmentation Packages, version 1.0, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0084-2014
[CR-IC]	Certification Report BSI-DSZ-CC-0955-V2 11 October 2016
[ST_IC]	NXP Secure Smart Card Controller P6021y VB - Security Target Lite Rev. 1.51, 19 July 2016

1.2. INTERNAL REFERENCES [IR]

[AGD]	TOE guidance documentation
[PRE]	D1417012_PRE_ScostaCL_V4_BAC.doc
[OPE]	D1417014_OPE_ScostaCL_V4_BAC.doc


	Reference D1390182	Release 1.2p <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level Public	Pages 68

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68


2. Acronyms and glossary

Acrr.	Term	Definition
AA	Active Authentication	Security mechanism defined in [PKI] option by which means the MTRD's chip proves and the inspection system verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known State of organization.
	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
BAC	Basic Access Control	Security mechanism defined in [PKI] by which means the MTRD's chip proves and the inspection system protects their communication by means of secure messaging with Basic Access Keys (see there).
BIS	Basic Inspection System	An inspection system which implements the terminal part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys drawn from printed MRZ data for reading the logical MRTD.
	Biographical data (biodata)	The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [SS]
	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. [SS]
CSCA	Country Signing Certification Authority	Self-signed certificate of the Country Signing CA Public Key (K _{PuCSCA}) issued by CSCA stored in the inspection system.
CPLCD	Card Production Life Cycle Data	The TOE identification is provided by the Card Production Life Cycle Data (CPLCD) of the TOE, located in OTP and in EEPROM. These data are available by executing a dedicated command.
CVCA	Country Verifying Certification Authority	The Country Verifying Certification Authority enforces the privacy policy of the issuing Country 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.
DV	Document Verifier	The Document Verifier enforces the privacy policy of the receiving Country with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The DV manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the Issuing State or Organization in form of the Document Verifier Certificates.
	Document Basic Access Keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key K _{ENC}) and message authentication (key K _{MAC}) of data transmitted between the MRTD's chip and the inspection system [PKI]. 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.
DSO	Document Security Object	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). [PKI]
	Eavesdropper	A threat agent with moderate 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. [BIO]
EAC	Extended Access Control	Security mechanism identified in [PKI] 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 Authentication Private Key and to get write and read access to the logical MRTD and TSF data.
EIS	Extended Inspection System	The EIS in addition to the General Inspection System (GIS) (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.
	Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [SS]
GIS	General Inspection System	The GIS is a Basic Inspection System (BIS) which implements additionally the Chip Authentication Mechanism.
	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. [BIO]
	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.
	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. [SS]
	Improperly Documented Person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [BIO]
	Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
	Inspection	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [BIO]
IS	Inspection system	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder.
IC	Integrated circuit	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68


	Integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization.
	Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO-9303].
	Issuing State	The Country issuing the MRTD. [ICAO-9303]
LDS	Logical Data Structure	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO-9303]. The capacity expansion technology used is the MRTD's chip.
	Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure (LDS) as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder (1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), (2) the digitized portraits (EF.DG2), (3) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and (4) the other data according to LDS (EF.DG5 to EF.DG16).
	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).
MRTD	Machine readable travel document	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [ICAO-9303]
MRV	Machine readable visa	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. [ICAO-9303]
MRZ	Machine Readable Zone	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [ICAO-9303]
	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. [SS]
	MRTD administrator	The Issuing State or Organization which is allowed to perform administrative commands (update data of the MRTD application, invalidation of the application) in the phase 4 Operational Use.
	MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes: <ul style="list-style-type: none"> - the file structure implementing the LDS [ICAO-9303], - the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG14 and EF.DG16), - the TSF Data including the definition of the authentication data but without 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.

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

	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 ICAOT, [ICAO], p. 14. Programed according to the Logical Data Structure as specified by ICAOT, [ICAO], p. 14.
	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	<ul style="list-style-type: none"> - verification of the digital signature of the Document Security Object - comparison 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. [SS]
	Personalization Agent	The agent acting on the behalf of the issuing State or organisation 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, FIA_UAU.5 and FIA_UAU.6.
	Physical travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to): <ul style="list-style-type: none"> - biographical data, - data of the machine-readable zone, - photographic image and - other data.
	Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalization Agent Key Pair.
	Pre –personalized MRTD's chip	MRTD's chip equipped with pre-personalization data.
PIS	Primary Inspection System	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.

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

	Receiving State	The Country to which the MRTD holder is applying for entry. [ICAO-9303]
	reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
	secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [SS]
	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.
	TD1	Size 1 machine readable official travel document (TD-1): A card with nominal dimensions guided by those specified for the ID-1 type card (ISO/IEC 7810) (excluding thickness). In the case of a plastic card which carries any optional, additional data storage technology, the reading of which requires it to be inserted into a slot reader (i.e. magnetic stripe, optical memory or integrated circuit with contacts), the TD-1 conforms to the precise dimensions and tighter tolerances specified in ISO/IEC 7810.
	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. [BIO]
	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 [CC-1].
	Unpersonalized MRTD	MRTD material prepared to produce a personalized MRTD containing an initialized and pre-personalized MRTD's chip.
	User data	Data created by and for the user, that does not affect the operation of the TSF [CC-1].
	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. [BIO]
	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.

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

3. Security Target introduction

3.1. SECURITY TARGET IDENTIFICATION


Title: Sealys eTravel SCOSTA-CL V4 on NXP P60D081 – Security Target Lite
Version: 1.2p
Author: Gemalto
Reference: D1390182
Publication date: 11/04/2017

3.2. TOE IDENTIFICATION

Product name: Sealys eTravel SCOSTA-CL V4 MPH176
Product reference: T1036621 Release A.2
TOE name: Sealys eTravel SCOSTA-CL V4
TOE version: MPH176
TOE documentation: Guidance [AGD]
TOE hardware part: NXP P60D081 security controller
Developer: Gemalto

The certified product can be identified on the field through the execution of a dedicated GET DATA command (DO tag DF7Eh), allowing to retrieve the Card Production Life Cycle (CPLC) data located in ROM:

CPLC field	Length	Value	Meaning
Card Manufacturer	2	4790h	
IC Type	2	6B64h	
OS Identifier	2	B28Ah	
OS version	2	0401h	
OS date	2	6299h	
OS Type	1	AAh	
IC Serial Number	8	xx..xxh	Unique identification written by the IC Manufacturer

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68


3.3. TOE OVERVIEW

The product Sealys eTravel SCOSTA-CL V4 MPH176 is an electronic passport application embedded in a NXP P60D081 contactless IC. It enforces the requirements of the International Civil Aviation Organization (ICAO) and implements the Logical data Structure (LDS) and Basic Access Control (BAC) as specified in the [ICAO-9303] document. As such it enables the worldwide secure verification of passport holder identity by border inspection systems.

The product is also conformant to the [SCOSTA-CL] specifications, as required by the Government of India. It is a native product which embeds one single application (Sealys eTravel SCOSTA-CL V4). The underlying platform is totally closed, meaning that it is not possible to load any additional application.

For the present evaluation, the Target of Evaluation (TOE) is the Sealys eTravel SCOSTA-CL V4 application, including the underlying platform software and hardware supporting its execution. The TOE boundaries encompass:

- **The Sealys eTravel SCOSTA-CL V4 application** implemented according to the ICAO standard, with LDS and BAC as specified to the [ICAO-9303] document, and to the [SCOSTA-CL] specifications
- **The underlying platform (operating system)**
- **The NXP P60D081 Integrated Circuit**
P60D081 is the commercial name of a specific chip of the family P6021y VB [ST_IC]
- **The guidance documentation [AGD]**

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

4. TOE Description

4.1. TOE INTENDED USAGE

A State or Organization issues Machine Readable Travel Documents (MRTD) to be used by legitimate holders for international travel. Each MRTD is personalized with the following identity information:

- Visual (eye readable) biographical data and portrait of the holder
- A separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ)
- Data elements in the MRTD chip according to the Logical Data Structure (LDS) defined in [ICAO-9303] for contactless machine reading.


Hence, the MRTD can be viewed as either:

- **The physical MRTD as a travel document in form of paper, plastic and chip.**
It presents visual readable data including (but not limited to) personal data of the MRTD holder
 - (1) The biographical data on the biographical data page of the passport book,
 - (2) The printed data in the Machine Readable Zone (MRZ) and
 - (3) The printed portrait.
- **The logical MRTD as data of the MRTD holder stored in the contactless IC according to the Logical Data Structure [ICAO-9303].**
It presents contactless readable data including (but not limited to) personal data of the MRTD holder
 - (1) The digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
 - (2) The digitized portraits (EF.DG2),
 - (3) The biometric reference data of fingers (EF.DG3) or iris images (EF.DG4) or both,
 - (4) The other data according to LDS (EF.DG5 to EF.DG16) and
 - (5) The Document security object.

Through a secure enrolment and issuance process, the issuing State or Organization ensures the authenticity of the data of genuine MRTDs. Security features are also implemented in the MRTD itself to maintain the authenticity and integrity of the MRTD and the personalized data:

- The MRTD as the passport book and the MRTD's chip is uniquely identified by the Document Number.
- The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational (e.g. control of materials, personalization procedures) [ICAO-9303]. These security measures include the binding of the MRTD's chip to the passport book.
- The logical MRTD is protected in authenticity and integrity by a digital signature created by the document signer acting for the issuing State or Organization and the security features of the MRTD's chip.

The traveller presents its MRTD to the border inspection system to prove his or her identity. The receiving State trusts genuine MRTDs as it is able to verify their authenticity by means of the security mechanisms mentioned here above.

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

The [ICAO-9303] document defines the baseline security method “Passive Authentication” as well as the following optional security methods:

- “Basic Access Control” to the logical MRTD,
- “Active Authentication” of the MRTD’s chip,
- “Extended Access Control” to the logical MRTD,
- “Data Encryption” of sensitive biometrics.

The “Passive Authentication” and the “Data Encryption” mechanisms are performed completely and independently of the TOE by the TOE environment.

This security target addresses the protection of the logical MRTD (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the “Basic Access Control” mechanism. This security target does not address the “Active Authentication” and the “Extended Access Control” as optional security mechanisms.

The “Basic Access Control” is a security feature which is mandatory supported by the TOE. The inspection system (i) reads optically the MRTD, (ii) authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the inspection system the MRTD’s chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [ICAO-9303], normative appendix 5.

4.2. TOE BOUNDARIES


The Target of Evaluation (TOE) is the MRTD’s contactless IC programmed according to the Logical Data Structure defined in [ICAO-9303] and providing the Basic Access Control (BAC) according to the ICAO document [PKI].

The TOE boundaries encompass:

- The circuitry of the MRTD’s chip (the integrated circuit)
- The IC Dedicated Software comprised of IC Dedicated Test Software and IC Dedicated Support Software
- The IC Embedded Software (operating system and MRTD application)
- The associated guidance documentation [AGD].

Figure 1 illustrates the TOE boundaries within the high level logical representation of the product.

Note: the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete MRTD, nevertheless these parts are outside of the IC and are therefore not in the scope of the present evaluation.

	Reference	D1390182	Release	1.2p <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level	Public	Pages	68

TOE boundary

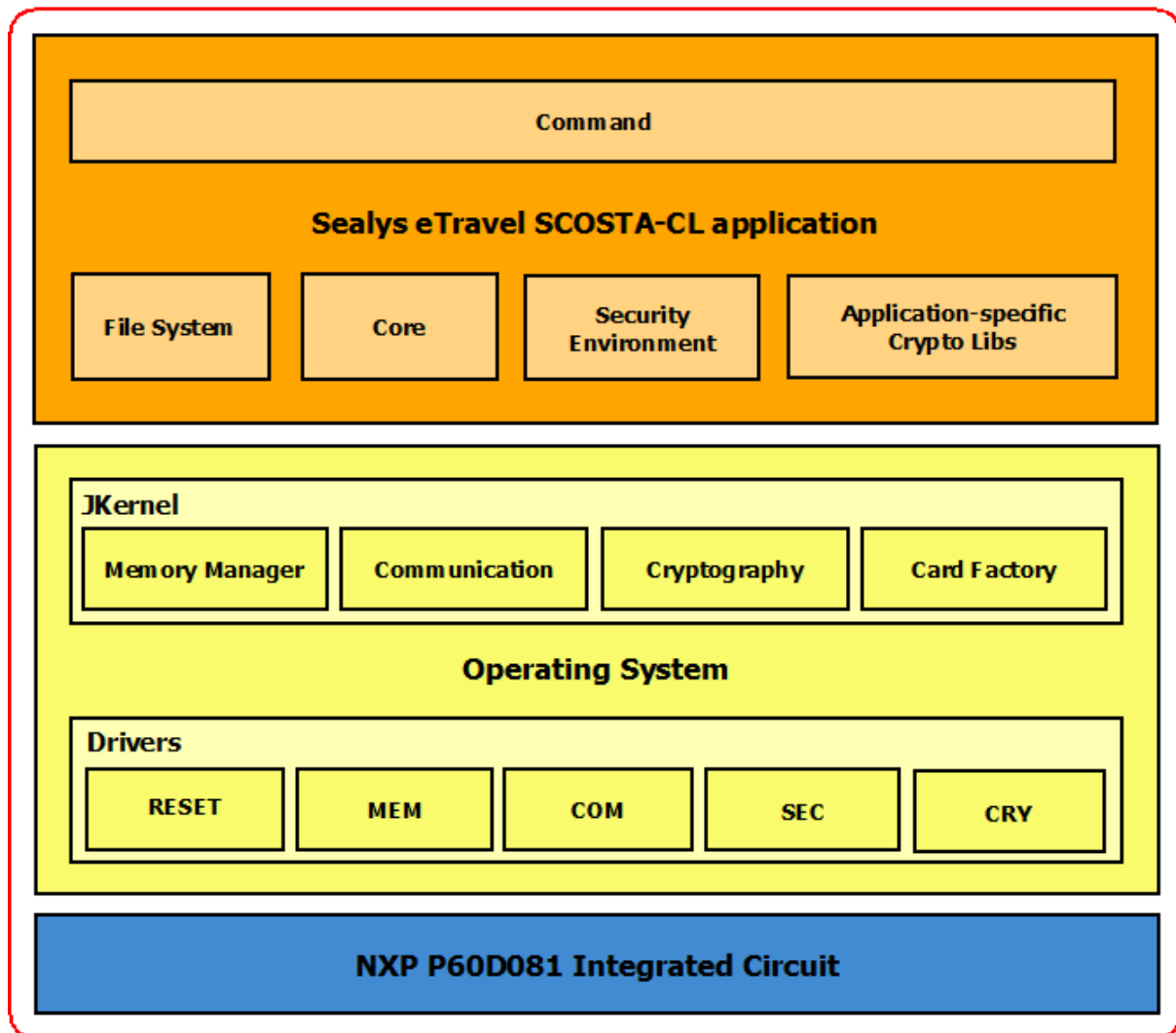


Figure 1: TOE logical boundaries


4.3. TOE LIFE-CYCLE

The TOE life cycle can be decomposed into 4 phases:

Phase 1 “Development”:

The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

The Embedded Software 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.

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

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

Phase 2 “Manufacturing”:

In a first step the TOE integrated circuit is produced containing the MRTD’s chip Dedicated Software and the parts of the MRTD’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 MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.

The MRTD manufacturer has the following tasks:

- Initialization: adding the parts of the IC Embedded Software (NVM ES) to the EEPROM,
- Pre-personalization: creation of the MRTD application and loading of Pre-personalization Data,
- Inlay manufacturing: packing the IC with hardware for the contactless interface.

Note: the following task is not part of the TOE manufacturing:

- Book manufacturing: manufacturing the passport book.

The pre-personalized MRTD together with the IC Identifier is securely delivered from the MRTD manufacturer to the Personalization Agent. The MRTD manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

Phase 3 “Personalization of the MRTD”:

The personalization of the MRTD includes:

- the survey of the MRTD holder biographical data,
- the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
- the printing of the visual readable data onto the physical MRTD,
- the writing of the TOE User Data and TSF Data into the logical MRTD,
- configuration of the TSF if necessary.


The step “writing the TOE User Data” is performed by the Personalization Agent and includes but is not limited to the creation of:

- the digital MRZ data (EF.DG1),
- the digitized portrait (EF.DG2),
- the Document security object (SOD).

The signing of the Document security object by the Document signer [PKI] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

Phase 4 “Operational Use”

The TOE is used as MRTD’s chip by the traveler and the inspection systems in the “Operational Use” phase. The user data can be read according to the security policy of the Issuing State or Organization and used according to the security policy of the Issuing State but they can never be modified.

	Reference	D1390182	Release	1.2p <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level	Public	Pages	68

Application note: In this ST, the role of the Personalization Agents is strictly limited to the phase 3 (Personalization). In the phase 4 (Operational Use), the modification of the data groups of the MRTD application is forbidden.

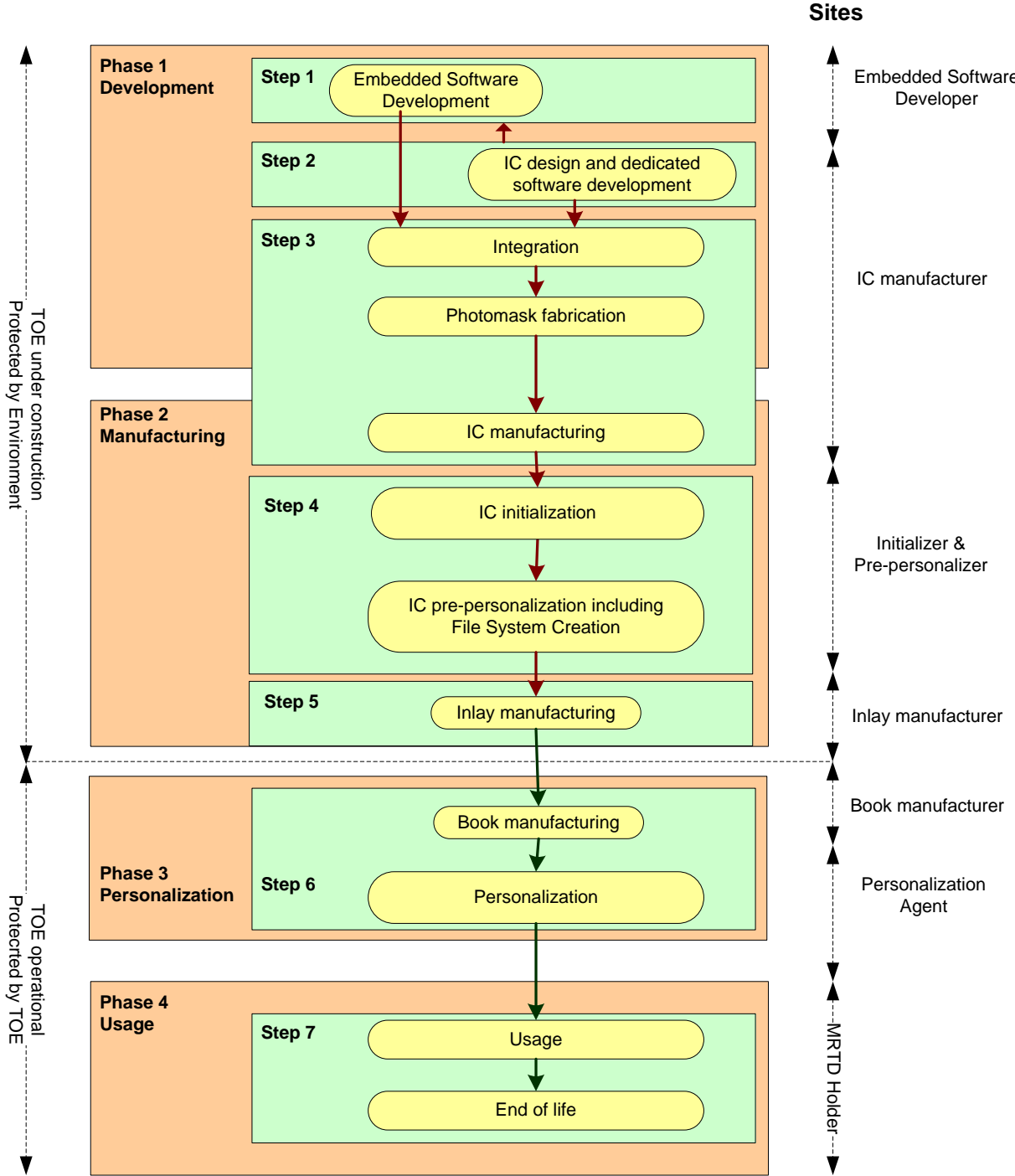



Figure 2: TOE life cycle

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

At the end of phase 2, the TOE is entirely built and protects itself through the security mechanisms implemented in the Embedded Software and the underlying IC. Consequently, the TOE delivery point - which determines the boundary between the ALC and AGD Common Criteria assurance classes - is put at the end of phase 2 (end of step 5), as illustrated in figure 2.


4.4. TOE ACTORS AND SITES

Actor	Identification
Integrated Circuit (IC) Developer	NXP
Embedded Software Developer	Gemalto
Integrated Circuit (IC) Manufacturer	NXP
Initializer	Gemalto
Pre-personalizer	Gemalto
Inlay manufacturer	Gemalto
Book manufacturer	The entity agent who is acting on the behalf of the issuing State or Organization and manufactures the passport booklet that embeds the inlay.
Personalization Agent	The agent who is acting on the behalf of the issuing State or Organization and personalizes the MRTD for the holder by activities establishing the identity of the holder with biographic data.
MRTD Holder	The legitimate holder of the MRTD for whom the issuing State or Organization personalizes the MRTD.

Table 1: Product and TOE actors

Actors	Site
Integrated Circuit (IC) Developer	Described in the IC certificate [CR-IC]
Embedded Software Developer	Gemalto Singapore (for OS and Application) Gemalto Meudon, France (for Crypto libraries)
Integrated Circuit (IC) Manufacturer	Described in the IC certificate [CR-IC]
Initializer & Pre-personalizer	Gemalto Gemenos, France Gemalto Singapore Gemalto Tczew, Poland
Inlay manufacturer	Gemalto Tczew, Poland

Table 2: Involved sites up to the TOE delivery point

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

5. Conformance claims

Common criteria Version: This ST conforms to CC Version 3.1 [CC-1] [CC-2] [CC-3]

Conformance to CC part 2 and 3:

- This ST is CC part 2 extended with the FAU_SAS.1, FCS_RND.1, FMT_LIM.1, FMT_LIM.2 and FPT_EMS.1 families. All the other SFRs have been drawn from the catalogue of requirements in CC part 2 [CC-2].
- This ST is CC part 3 conformant. It means that all SARs in that ST are based only upon assurance components in CC part 3 [CC-3].

Assurance package conformance: EAL4 augmented (EAL4+)

This ST conforms to the assurance package EAL4 augmented by ALC_DVS.2.

Evaluation type


This is a composite evaluation, which relies on the P60D081 chip certificate and evaluation results.

P60D081 chip certificate:

- Certification done under the BSI scheme
- Certification report BSI-DSZ-CC-0955-V2-2016
- Security Target [ST_IC] strictly conformant to IC Protection Profile [PP/0084]
- Common criteria version: 3.1
- Assurance level: EAL5+ (ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2 augmentations)

Protection Profile (PP) conformance claim:

This Security Target claims strict conformance to the [PP-MRTD-BAC] protection profile.

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

6. Security problem definition

6.1. ASSETS

The assets to be protected by the TOE include the User Data on the MRTD's chip.

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 [ICAO-9303]. 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.DG16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG14) 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.

Due to interoperability reasons as the 'ICAO Doc 9303' [ICAO-9303] the TOE described in this protection profile specifies only the BAC mechanisms with resistance against enhanced basic attack potential granting access to

- Logical MRTD standard User Data (i.e. Personal Data) of the MRTD holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16),
- Chip Authentication Public Key in EF.DG14,
- Active Authentication Public Key in EF.DG15,
- Document Security Object (SOD) in EF.SOD,
- Common data in EF.COM.

The TOE prevents read access to sensitive User Data:

- Sensitive biometric reference data (EF.DG3, EF.DG4).

Authenticity of the MRTD's chip

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

6.2. USERS / SUBJECTS


This protection profile considers the following subjects:

Manufacturer

Generic term for the IC Manufacturer producing integrated circuit and the MRTD Manufacturer completing the IC to the MRTD's chip. 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 MRTD Manufacturer using this role Manufacturer.

Personalization Agent

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

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

Terminal

A terminal is any technical system communicating with the TOE 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 traveller and verifying its authenticity and (ii) verifying the traveller 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.

MRTD Holder

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

Traveller

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

Attacker

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

6.3. THREATS

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.


The TOE in collaboration with its IT environment shall avert the threats as specified below.

T.Chip_ID Identification of MRTD's chip

Adverse action: An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface. Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance. Asset: Anonymity of user.

T.Skimming Skimming the logical MRTD

Adverse action: An attacker imitates an inspection system trying to establish a communication to read the logical MRTD or parts of it via the contactless communication channel of the TOE. Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance. Asset: confidentiality of logical MRTD data.

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

T.Eavesdropping Eavesdropping to the communication between TOE and inspection system

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

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

T.Forgery Forgery of data on MRTD's chip


Adverse action: An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data. This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveller. 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 traveller 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.Abuse-Func Abuse of Functionality

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

Adverse action: An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis). Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD. Asset: confidentiality of logical MRTD and TSF data

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

T.Phys-Tamper Physical Tampering

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

T.Malfunction Malfunction due to Environmental Stress

Adverse action: An attacker may cause a malfunction the MRTD'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 MRTD outside the normal operating conditions, exploiting errors in the MRTD's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation. Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD. Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

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.Phys-Tamper) assuming a detailed knowledge about TOE's internals.

6.4. ORGANISATIONAL SECURITY POLICIES


The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CC part 1, §3.2).

P.Manufact Manufacturing of the MRTD's chip

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

P.Personalization Personalization of the MRTD by issuing State or Organization only

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

	Reference D1390182	Release 1.2p (Printed copy not controlled: verify the version before using)
	Classification Level Public	Pages 68

P.Personal_Data Personal data protection policy

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4)3 and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [ICAO-9303].

Application Note: the organizational security policy P.Personal_Data is drawn from the ICAO 'ICAO Doc 9303' [ICAO-9303]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

6.5. SECURE USAGE ASSUMPTIONS

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

A.MRTD_Manufact MRTD manufacturing on steps 4 to 6

It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRTD and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

A.MRTD_Delivery MRTD delivery during steps 4 to 6

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


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

A.Pers_Agent Personalization of the MRTD's chip

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

A.Insp_Sys Inspection Systems for global interoperability

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

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68


A.BAC-Keys Cryptographic quality of Basic Access Control Keys

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


6.6. COMPOSITION TASKS – SECURITY PROBLEM DEFINITION PART

6.6.1. Statement of Compatibility – Threats part


The following table (see next page) lists the relevant threats of the security target [ST_IC], and provides the link to the threats on the composite-product, showing that there is no contradiction between the two.

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

IC relevant threat label	IC relevant threat title	IC relevant threat content	Link to the composite-product threats
T.Leak-Inherent	Inherent Information Leakage	An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential user data as part of the assets. No direct contact with the Security IC internals is required here. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements.	T.Information_Leakage
T.Phys-Probing	Physical Probing	An attacker may perform physical probing of the TOE in order (i) to disclose user data while stored in protected memory areas, (ii) to disclose/reconstruct the user data while processed or (iii) to disclose other critical information about the operation of the TOE to enable attacks disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software.	T.Phys-Tamper
T.Malfunction	Malfunction due to Environmental Stress	An attacker may cause a malfunction of TSF or of the Security IC Embedded Software by applying environmental stress in order to (i) modify security services of the TOE or (ii) modify functions of the Security IC Embedded Software (iii) deactivate or affect security mechanisms of the TOE to enable attacks disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software. This may be achieved by operating the Security IC outside the normal operating conditions.	T.Malfunction
T.Phys-Manipulation	Physical Manipulation	An attacker may physically modify the Security IC in order to (i) modify user data of the Composite TOE, (ii) modify the Security IC Embedded Software (iii) modify or deactivate security services of the TOE, or (iv) modify security mechanisms of the TOE to enable attacks disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software.	T.Phys-Tamper
T.Leak-Forced	Forced Information Leakage	An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential user data of the Composite TOE as part of the assets even if the information leakage is not inherent but caused by the attacker.	T.Information_Leakage
T.Abuse-Func	Abuse of	An attacker may use functions of the TOE which may not be used after TOE Delivery in	T.Abuse-Func

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

IC relevant threat label	IC relevant threat title	IC relevant threat content	Link to the composite-product threats
	Functionality	<p>order to</p> <ul style="list-style-type: none"> (i) disclose or manipulate User Data of the Composite TOE, (ii) manipulate (explore, bypass, deactivate or change) security services of the TOE or (iii) manipulate (explore, bypass, deactivate or change) functions of the Security IC Embedded Software or (iv) enable an attack disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software. 	
T.RND	Deficiency of Random Numbers	An attacker may predict or obtain information about random numbers generated by the TOE security service for instance because of a lack of entropy of the random numbers provided.	T.Skimming
T.Unauthorised-Access	Unauthorised Memory or Hardware Access	<p>An attacker may try to read, modify or execute code or data stored in restricted memory areas. And or an attacker may try to access or operate hardware resources that are restricted by executing code that accidentally or deliberately accesses these restricted hardware resources.</p> <p>Any code or data executed in Boot Mode, Firmware Mode, System Mode or User Mode may accidentally or deliberately access User Data or code of another application stored on the TOE. Or any code or data executed in Boot Mode, Firmware Mode, System Mode or User Mode may accidentally or deliberately access hardware resources that are restricted or reserved for other CPU modes.</p> <p>Access restrictions for the memories and hardware resources accessible by the Security IC Embedded Software must be defined and implemented by the security policy of the Security IC Embedded Software based on the specific application context.</p>	This threat is only relevant for products that host several applications. Therefore it is not applicable to the present composite TOE which corresponds to a native and closed product featuring a single application.

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68


6.6.2. Statement of compatibility – OSPs part

The following table lists the relevant OSPs of the security target [ST_IC], and provides the link to the OSPs related to the composite-product, showing that there is no contradiction between the two.


IC OSP label	IC OSP content	Link to the composite product
P.Process-TOE	Identification during TOE Development and Production: an accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.	P.Manufact
P.Crypto-Service	Cryptographic services of the TOE: The TOE provides secure hardware based cryptographic services for the IC Embedded Software. <ul style="list-style-type: none"> - Triple-DES encryption and decryption - AES encryption and decryption 	The 3DES hardware functionality is used by the composite TOE. The AES hardware functionality is not used by the composite TOE.
P.Add-Components-Plain	Additional Specific Security Components: The P6021P VB shall provide the following additional security functionality to the Security IC Embedded Software: <ul style="list-style-type: none"> - Integrity support of data stored in EEPROM - Hardware Post Delivery Configuration: reconfiguration of customer selectable options - PUF functionality 	Checksum for EEP data not available but other integrity checks are available. PDC & PUF are not used by the TOE.

6.6.3. Statement of compatibility – Assumptions part

The following table (see next page) lists the relevant assumptions of the security target [ST_IC], and provides the link to the assumptions related to the composite-product, showing that there is no contradiction between the two.

	Reference D1390182	Release 1.2p (Printed copy not controlled: verify the version before using)
	Classification Level Public	Pages 68

IC assumption label	IC assumption title	IC assumption content	IrPA	CfPA	SgPA	Link to the composite product
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalization	It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use). This means that the Phases after TOE Delivery are assumed to be protected appropriately.		X	X	<ul style="list-style-type: none"> During phases 1 & 2: CfPA Fulfilled by the ALC composite-SARs During phases 3 & 4: SgPA A.MRTD_Manufact, A.MRTD_Delivery
A.Resp-Appl	Treatment of user data of the Composite TOE	All user data of the Composite TOE are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant user data of the Composite TOE (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.		X		OT.Prot_Inf_Leak OT.Data_Conf OT.Data_Int
A.Check-Init-Plain	Check of initialization data by the Security IC Embedded Software	The Security IC Embedded Software must provide a function to check initialization data. The initialization data is defined by the customer and injected by the TOE Manufacturer into the non-volatile memory to provide the possibility for TOE identification and for traceability.		X		There are ways to read back the card serial number and pre-perso information

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

7. Security objectives

7.1. SECURITY OBJECTIVES FOR THE TOE

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

OT.AC_Pers Access Control for Personalization of logical MRTD

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [ICAO-9303] and the TSF data can be written by authorized Personalisation 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 personalisation. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

Application Note: the OT.AC_Pers implies that

- The data of the LDS groups written during personalisation for MRTD holder (at least EF.DG1 and EF.DG2) cannot be changed using write access after personalisation.
- The Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly. The support for adding data in the "Operational Use" phase is optional.


OT.Data_Int Integrity of personal data

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

OT.Data_Conf Confidentiality of personal data

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

Application Note: the traveller grants the authorization for reading the personal data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 to the inspection system by presenting the MRTD. The MRTD's chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys. The security objective OT.Data_Conf requires the TOE to ensure the strength of the security function Basic Access Control Authentication. The Document Basic Access Keys are derived from the MRZ data defined by the TOE environment and are loaded into the TOE by the Personalization Agent. Therefore the sufficient quality of these keys has to result from the MRZ data's entropy. Any attack based on decision of the 'ICAO Doc 9303' [ICAO-9303] that the inspection system derives Document Basic Access is ensured by OE.BAC-Keys. Note that the authorization for reading the biometric data in EF.DG3 and EF.DG4 is only granted after successful Enhanced Access Control not covered by this protection profile. Thus the read access must be prevented even in case of a successful BAC Authentication.

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

OT.Identification Identification and Authentication of the TOE

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

Application Note: the TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 'Manufacturing' and for traceability and/or to secure shipment of the TOE from Phase 2 'Manufacturing' into the Phase 3 'Personalization of the MRTD'. The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing. In the Phase 4 'Operational Use' the TOE is identified by the Document Number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or MRTD identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent.

OT.Prot_Abuse-Func Protection against Abuse of Functionality

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

OT.Prot_Inf_Leak Protection against Information Leakage

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


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

Application Note: this objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.

OT.Prot_Phys-Tamper Protection against Physical Tampering

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

- Measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- Measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)
- Manipulation of the hardware and its security features, as well as
- Controlled manipulation of memory contents (User Data, TSF Data) with a prior
- Reverse-engineering to understand the design and its properties and functions.

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

OT.Prot_Malfunction Protection against Malfunctions

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation have not been proven or tested. This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature.

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 objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE's internals.

7.2. SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

OE.MRTD_Manufact Protection of the MRTD Manufacturing

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.

OE.MRTD_Delivery Protection of the MRTD delivery

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


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

The issuing State or Organization must ensure that the Personalization Agents acting on behalf of the issuing State or Organization (i) establish the correct identity of the holder and create biographical data for the MRTD, (ii) enrol 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.

	Reference D1390182	Release 1.2p (Printed copy not controlled: verify the version before using)
	Classification Level Public	Pages 68

OE.Pass_Auth_Sign Authentication of logical MRTD by Signature

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

OE.BAC-Keys Cryptographic quality of Basic Access Control Keys

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

OE.Exam_MRTD Examination of the MRTD passport book

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

OE.Passive_Auth_Verif Verification by Passive Authentication

The border control officer of the receiving State uses the inspection system to verify the traveller 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 Protection of data from the logical MRTD


The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD being under Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems).

7.3. SECURITY OBJECTIVES RATIONALE

7.3.1. Threats, OSPs and Assumptions coverage – Mapping table

	T.Chip_ID	T.Skimming	T.Eavesdropping	T.Forgery	T.Abuse-Func	T.Information_Leakage	T.Phys-Tamper	T.Malfunction	P.Manufact	P.Personalization	P.Personal_Data	A.MRTD_Manufact	A.MRTD_Delivery	A.Pers_Agent	A.Insp_Sys	A.BAC-Keys
OT.AC_Pers				X						X						
OT.Data_Int				X							X					
OT.Data_Conf		X	X								X					
OT.Identification	X								X	X						
OT.Prot_Abuse-Func					X											
OT.Prot_Inf_Leak						X										
OT.Prot_Phys-Tamper				X			X									
OT.Prot_Malfunction								X								
OE.MRTD_Manufact												X				
OE.MRTD_Delivery													X			
OE.Personalization				X	X					X				X		
OE.Pass_Auth_Sign				X												
OE.BAC-Keys	X	X														X
OE.Exam_MRTD				X											X	
OE.Passive_Auth_Verif				X												
OE.Prot_Logical_MRTD															X	

Table 3: Threats, OSPs and assumptions coverage by security objectives – Mapping table

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

7.3.2. Threats coverage – Rationale

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

T.Skimming addresses the reading of the logical MRTD through the contactless interface or listening the communication between the MRTD's chip and a terminal. This threat is countered by the security objective OT.Data_Conf 'Confidentiality of personal data' through Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment OE.BAC-Keys.

T.Eavesdropping addresses the reading of the logical MRTD through the contactless interface or listening the communication between the MRTD's chip and a terminal. This threat is countered by the security objective OT.Data_Conf 'Confidentiality of personal data'.


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

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

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

T.Phys-Tamper is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is addressed by the directly related security objective OT.Prot_Phys-Tamper 'Protection against Physical Tampering'.

T.Malfunction is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is addressed by the directly related security objective OT.Prot_Malfunction 'Protection against Malfunctions'.

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

7.3.3. OSP coverage – Rationale

P.Manufact requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalization Data as being fulfilled by OT.Identification.

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

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

7.3.4. Assumptions coverage – Rationale

A.MRTD_Manufact is covered by the security objective for the TOE environment OE.MRTD_Manufact 'Protection of the MRTD Manufacturing' that requires to use security procedures during all manufacturing steps.

A.MRTD_Delivery is covered by the security objective for the TOE environment OE.MRTD_Delivery 'Protection of the MRTD delivery' that requires to use security procedures during delivery steps of the MRTD.


A.Pers_Agent is covered by the security objective for the TOE environment OE.Personalization 'Personalization of logical MRTD' including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data.

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


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

7.4. COMPOSITION TASKS – OBJECTIVES PART


7.4.1. Statement of compatibility – TOE Objectives part

	Reference	D1390182	Release	1.2p <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level	Public	Pages	68


The following table (see next page) lists the relevant TOE security objectives of the P60D081 IC, and provides the link to the composite-product TOE security objectives, showing that there is no contradiction between the two sets of objectives.

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

Label of the chip TOE security objective	Title of the chip TOE security objective	Content of the chip TOE security objective	Linked Composite-product TOE security objectives
O.Leak-Inherent	Protection against Inherent Information Leakage	<p>The TOE must provide protection against disclosure of confidential data stored and/or processed in the Security IC</p> <ul style="list-style-type: none"> - by measurement and analysis of the shape and amplitude of signals (for example on the power, clock, or I/O lines) and - by measurement and analysis of the time between events found by measuring signals (for instance on the power, clock, or I/O lines). <p>This objective pertains to measurements with subsequent complex signal processing whereas O.Phys-Probing is about direct measurements on elements on the chip surface.</p>	OT.Prot_Inf_Leak
O.Phys-Probing	Protection against Physical Probing	<p>The TOE must provide protection against disclosure/reconstruction of user data while stored in protected memory areas and processed or against the disclosure of other critical information about the operation of the TOE. This includes protection against:</p> <ul style="list-style-type: none"> - 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) <p>with a prior reverse-engineering to understand the design and its properties and functions.</p>	OT.Prot_Phys-Tamper
O.Malfunction	Protection against Malfunctions	<p>The TOE must ensure its correct operation.</p> <p>The TOE must indicate or prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent malfunctions. Examples of environmental conditions are voltage, clock frequency, temperature, or external energy fields.</p>	OT.Prot_Malfunction
O.Phys-Manipulation	Protection against Physical Manipulation	<p>The TOE must provide protection against manipulation of the TOE (including its software and TSF data), the Security IC Embedded Software and the user data of the Composite TOE. This includes protection against</p> <ul style="list-style-type: none"> - reverse-engineering (understanding the design and its properties and functions), - manipulation of the hardware and any data, as well as - undetected manipulation of memory contents. 	OT.Prot_Phys-Tamper
O.Leak-Forced	Protection against Forced	The Security IC must be protected against disclosure of confidential data processed in the Security IC (using	OT.Prot_Inf_Leak


	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

Label of the chip TOE security objective	Title of the chip TOE security objective	Content of the chip TOE security objective	Linked Composite-product TOE security objectives
	Information Leakage	<p>methods as described under O.Leak-Inherent) even if the information leakage is not inherent but caused by the attacker</p> <ul style="list-style-type: none"> - by forcing a malfunction (refer to "Protection against Malfunction due to Environmental Stress (O.Malfunction)" and/or - by a physical manipulation (refer to "Protection against Physical Manipulation (O.Phys-Manipulation)". <p>If this is not the case, signals which normally do not contain significant information about secrets could become an information channel for a leakage attack.</p>	
O.Abuse-Func	Protection against Abuse of Functionality	The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order to (i) disclose critical user data of the Composite TOE (ii) manipulate critical user data of the Composite TOE (iii) manipulate Security IC Embedded Software or (iv) bypass, deactivate, change or explore security features or security services of the TOE. Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.	OT.Prot_Abuse-Func
O.Identification	TOE Identification	The TOE must provide means to store Initialization Data and Pre-personalization Data in its non-volatile memory. The Initialization Data (or parts of them) are used for TOE identification.	OT.Identification
O.RND	Random Numbers	The TOE will ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have a sufficient entropy. The TOE will ensure that no information about the produced random numbers is available to an attacker since they might be used for instance to generate cryptographic keys.	OT.AC_Pers OT.Data_Int OT.Data_Conf
O.TDES	Cryptographic service Triple-DES	The TOE provides secure hardware based cryptographic services implementing the Triple-DES for encryption and decryption.	OT.AC_Pers OT.Data_Int OT.Data_Conf
O.AES	Cryptographic service AES	The TOE provides secure hardware based cryptographic services for the AES for encryption and decryption.	AES is not used by the Composite TOE
O.CUST_RECONF_PLAIN	Post Delivery Configuration of Hardware	The TOE shall provide the customer with the functionality to reconfigure parts of the TOE properties as specified for Hardware Post Delivery Configuration listed in Table 7.	PDC not used by the Composite TOE
O.EEPROM_INTEGRITY	Integrity support of data stored in EEPROM	The TOE shall provide a retrimming of the EEPROM to support the integrity of the data stored in the EEPROM.	Checksum not available for EEP data but other

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68


Label of the chip TOE security objective	Title of the chip TOE security objective	Content of the chip TOE security objective	Linked Composite-product TOE security objectives
			integrity checks supported
O.FM_FW	Firmware Mode Firewall	The TOE shall provide separation between the NXP Firmware (i.e. NXP firmware functionality as part of the Security IC Dedicated Support Software) as part of the Security IC Dedicated Support Software and the Security IC Embedded Software. The separation shall comprise software execution and data access.	OT.Prot_Abuse-Func
O.MEM_ACCESS	Area based Memory Access Control	Access by processor instructions to memory areas is controlled by the TOE. The TOE decides based on the CPU mode (Boot Mode, Test Mode, Firmware Mode, System Mode or User Mode) and the configuration of the Memory Management Unit if the requested type of access to the memory area addressed by the operands in the instruction is allowed.	OT.Prot_Abuse-Func
O.SFR_ACCESS	Special Function Register Access Control	The TOE shall provide access control to the Special Function Registers depending on the purpose of the Special Function Register or based on permissions associated to the memory area from which the CPU is currently executing code. The access control is used to restrict access to hardware components of the TOE. The possibility to define access permissions to specialized hardware components of the TOE shall be restricted to code running in System Mode.	OT.Prot_Abuse-Func
O.PUF	Sealing/Unsealing user data	The TOE shall provide a PUF functionality that supports sealing/unsealing of user data. Using this functionality, the user data can be sealed within the TOE and can be unsealed by the same TOE that the user data was sealed on. The PUF functionality comprises import/export of data, encryption/decryption of data and calculation of a MAC as a PUF authentication value. Note: The PUF functionality provided by the P6021P VB shall only be active if explicitly configured by the Security IC Embedded Software.	PUF not used by the Composite TOE

7.4.2. Statement of compatibility – ENV Objectives part

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

The following table lists the relevant ENV security objectives related to the P60D081 chip, and provides the link to the composite-product, showing that they have been taken into account and that no contradiction has been introduced.

IC ENV security objective label	IC ENV security objective title	IC ENV security objective content	Link to the composite-product
OE.Resp-Appl	Treatment of user data of the Composite TOE	Security relevant user data of the Composite TOE (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context. For example the Security IC Embedded Software will not disclose security relevant user data of the Composite TOE to unauthorized users or processes when communicating with a terminal.	Covered by TOE Security Objectives: OT.Data_Int, OT.Data_Conf
OE.Process-Sec-IC	Protection during composite product manufacturing	Security procedures shall be used after TOE Delivery up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use). This means that Phases after TOE Delivery up to the end of Phase 6 must be protected appropriately.	<ul style="list-style-type: none"> • During phases 1 & 2: covered by the ALC composite-SARs • During phases 3 & 4: covered by OE.MRTD_Manufact, OE.MRTD_Delivery
OE.Check-Init	Check of initialization data by the Security IC Embedded Software	To ensure the receipt of the correct TOE, the Security IC Embedded Software shall check a sufficient part of the pre-personalization data. This shall include at least the FabKey Data that is agreed between the customer and the TOE Manufacturer.	OT.AC_Pers, OT.Identification

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

8. Extended components definition

8.1. EXTENDED FAMILY FAU SAS – AUDIT DATA STORAGE

8.1.1. Description

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

8.1.2. Extended Components

FAU_SAS.1	Requires the TOE to provide the possibility to store audit data.
Management:	There are no management activities foreseen.
Audit:	There are no actions defined to be auditable.

FAU_SAS.1 Audit Data 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.

Hierarchical to: No other components.

Dependencies: No dependencies.


8.2. EXTENDED FAMILY FCS RND – GENERATION OF RANDOM NUMBERS

8.2.1. Description

To define the IT security functional requirements of the TOE a sensitive family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND is not limited to generation of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

8.2.2. Extended Components

FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	There are no management activities foreseen.
Audit:	There are no actions defined to be auditable.

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

FCS_RND.1 Quality Metric for Random Numbers

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

Hierarchical to: No other components.

Dependencies: No dependencies.

8.3. EXTENDED FAMILY FMT LIM – LIMITED CAPABILITIES AND AVAILABILITY

8.3.1. Description

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

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

8.3.2. Extended Components


FMT_LIM.1	Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.
FMT_LIM.2	Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's lifecycle.
Management:	There are no management activities foreseen.
Audit:	There are no actions defined to be auditable.

FMT_LIM.1 Limited Capabilities

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

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

FMT_LIM.2 Limited Availability

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

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited Capabilities.

8.4. EXTENDED FAMILY FPT EMS – TOE EMANATION

8.4.1. Description

The sensitive family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2.

8.4.2. Extended Components

FPT_EMSEC.1 'TOE emanation' has two constituents:

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

Management: There are no management activities foreseen.

Audit: There are no actions defined to be auditable.


FPT_EMS.1 TOE Emanation

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

9. Security requirements

9.1. SECURITY FUNCTIONAL REQUIREMENTS

This section on security functional requirements for the TOE is divided into sub-section following the main security functionality.

Definition of security attributes:

Security attribute	Values	Meaning
Terminal authentication status	Non (any terminal)	Default role (i.e. without authorization after start-up)
	Basic Inspection System	Terminal is authenticated as Basic Inspection System after successful Authentication in accordance with the definition in rule 2 of FIA_UAU.5.2.
	Personalization Agent	Terminal is authenticated as Personalization Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2.

9.1.1. Class FAU Security Audit

FAU_SAS.1 Audit storage

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

9.1.2. Class FCS Cryptographic Support

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Document Basic Access Key Derivation Algorithm** and specified cryptographic key sizes **112 bits** that meet the following: **[ICAO-9303], normative appendix 5.**

FCS_CKM.4 Cryptographic key destruction


FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **zeroing the RAM zone storing the key** that meets the following: **None.**

FCS_COP.1/SHA Cryptographic operation

FCS_COP.1.1/SHA The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1** and cryptographic key sizes **none** that meet the following: **FIPS 180-4 [FIPS180-4].**

Application Note : Only use for BAC session keys derivation.

FCS_COP.1/ENC Cryptographic operation

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

FCS_COP.1.1/ENC The TSF shall perform **secure messaging (BAC) encryption and decryption** in accordance with a specified cryptographic algorithm **Triple-DES in CBC mode** and cryptographic key sizes **112 bits** that meet the following: **[SP800-67] and [ICAO-9303], normative appendix 5, A5.3.**

FCS_COP.1/AUTH Cryptographic operation

FCS_COP.1.1/AUTH The TSF shall perform **symmetric authentication (encryption and decryption)** in accordance with a specified cryptographic algorithm **Triple-DES** and cryptographic key sizes **112 bits** that meet the following: **[SP800-67]**

FCS_COP.1/MAC Cryptographic operation

FCS_COP.1.1/MAC The TSF shall perform **secure messaging - message authentication code** in accordance with a specified cryptographic algorithm **Retail MAC** and cryptographic key sizes **112 bits** that meet the following: **[ISO 9797] (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2).**

FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet **K3 class of [AIS20/AIS31] with seed entropy at least 112 bits and with strength of mechanism set to high.**

9.1.3. Class FIA Identification and authentication

Application note: The following table provides an overview on the authentication mechanisms used.


Name	SFR for the TOE	Algorithms and key sizes according to [ICAO-9303], normative appendix 5, and [TG-EAC]
Basic Access Control Authentication Mechanism	FIA_UAU.4 and FIA_UAU.6	Triple-DES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC)
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	Triple-DES with 112 bit keys (cf. FCS_COP.1/AUTH)

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow
to read the Initialization Data in Phase 2 "Manufacturing",
to read the random identifier in Phase 3 "Personalization of the MRTD",
to read the random identifier in Phase 4 "Operational Use"
on behalf of the user to be performed before the user is identified.

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

FIA_UAU.1 Timing of authentication

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

FIA_UAU.1.1 The TSF shall allow
to read the Initialization Data in Phase 2 "Manufacturing",
to read the random identifier in Phase 3 "Personalization of the MRTD",
to read the random identifier in Phase 4 "Operational Use"
on behalf of the user to be performed before the user is authenticated.

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

FIA_UAU.4 Single-use authentication mechanisms

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

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

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide

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

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the

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


FIA_UAU.6 Re-authenticating

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

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **an administrator configurable positive integer within 1 to 10** unsuccessful authentication attempts occur related to **Unsuccessful Basic Access Control authentication attempt.**

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **block the Document Basic Access Keys.**

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

9.1.4. Class FDP User data protection

Application note: FDP_UCT.1 and FDP_UIT.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

FDP_ACC.1 Subset access control

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

FDP_ACF.1 Security attribute based access control

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

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

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

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

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


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

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

FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1 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 Data exchange integrity

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

FDP_UIT.1.1 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 The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred.

9.1.5. Class FMT Security management

Application notes:

- The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.
- The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

FMT_SMF.1 Specification of Management Functions

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

- **Initialization,**
- **Pre-personalization,**
- **Personalization.**

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

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


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

FMT_LIM.1 Limited Capabilities

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced **Deploying Test Features after TOE Delivery does not allow**

- **User Data to be disclosed or manipulated**
- **TSF data to be disclosed or manipulated**
- **Software to be reconstructed and**
- **Substantial information about construction of TSF to be gathered which may enable other attacks.**

FMT_LIM.2 Limited Availability

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced **Deploying Test Features after TOE Delivery does not allow**

- **User Data to be disclosed or manipulated**
- **TSF data to be disclosed or manipulated**
- **Software to be reconstructed and**
- **Substantial information about construction of TSF to be gathered which may enable other attacks.**

FMT_MTD.1/INI_ENA Management of TSF data

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to **write the Initialization Data and Prepersonalization Data to Manufacturer.**

FMT_MTD.1/INI_DIS Management of TSF data

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to **disable read access for users to the Initialization Data to the Personalization Agent.**

FMT_MTD.1/KEY_WRITE Management of TSF data

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

FMT_MTD.1/KEY_READ Management of TSF data

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


9.1.6. Class FPT Protection of the security functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMSEC.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional requirements 'Failure with preservation of secure state (FPT_FLS.1)' and 'TSF testing (FPT_TST.1)' on the one hand and 'Resistance to physical attack (FPT_PHP.3)' on the other. The SFRs 'Limited capabilities (FMT_LIM.1)', 'Limited availability (FMT_LIM.2)' and 'Resistance to physical attack (FPT_PHP.3)' together with the SAR 'Security architecture description' (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **electromagnetic radiation, variation of timing or power consumption** in excess of **intelligible threshold** enabling access to **Personalization Agent Key(s)** and **confidential User Data.**

FPT_FLS.1 Failure with preservation of secure state

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

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

FPT_TST.1 TSF testing

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

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

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

FPT_PHP.3 Resistance to physical attack

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

9.2. SECURITY ASSURANCE REQUIREMENTS


The Evaluation Assurance Level is EAL4 augmented with ALC_DVS.2.

9.3. SECURITY REQUIREMENTS RATIONALE

9.3.1. TOE security objectives coverage – Mapping table

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FAU_SAS.1				X				
FCS_CKM.1	X	X	X					
FCS_CKM.4	X		X					
FCS_COP.1/SHA	X	X	X					
FCS_COP.1/ENC	X	X	X					
FCS_COP.1/AUTH	X	X						
FCS_COP.1/MAC	X	X	X					
FCS_RND.1	X	X	X					
FIA_UID.1			X	X				
FIA_UAU.1			X	X				
FIA_UAU.4	X	X	X					
FIA_UAU.5	X	X	X					
FIA_UAU.6	X	X	X					
FIA_AFL.1			X	X				
FDP_ACC.1	X	X	X					
FDP_ACF.1	X	X	X					
FDP_UCT.1	X	X	X					
FDP_UIT.1	X	X	X					
FMT_SMF.1	X	X	X					
FMT_SMR.1	X	X	X					
FMT_LIM.1					X			
FMT_LIM.2					X			
FMT_MTD.1/INI_ENA				X				
FMT_MTD.1/INI_DIS				X				
FMT_MTD.1/KEY_WRITE	X	X	X					
FMT_MTD.1/KEY_READ	X	X	X					
FPT_EMS.1	X					X		
FPT_FLS.1	X					X	X	
FPT_TST.1						X	X	
FPT_PHP.3	X					X	X	

Table 4: TOE Security Objectives coverage by Security Functional Requirements – Mapping table

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

9.3.2. TOE security objectives coverage – Rationale

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

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


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

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

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

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

OT.Data_Conf requires the TOE to ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. In case of failed authentication attempts FIA_AFL.1 blocks the Document Basic Access Key. The read access to the logical MRTD data is defined by the FDP_ACC.1 and FDP_ACF.1.2: the successful authenticated Personalization Agent is allowed to read the data of the logical MRTD (EF.DG1 to EF.DG16). The successful authenticated Basic Inspection System is allowed to read the data of the logical MRTD (EF.DG1, EF.DG2 and EF.DG5 to EF.DG16). The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

management functions (including Personalization for the key management for the Document Basic Access Keys).

The SFR FIA_UAU.4 prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5 enforces the TOE to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Moreover, the SFR FIA_UAU.6 requests secure messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism which includes the protection of the transmitted data in ENC_MAC_Mode by means of the cryptographic functions according to FCS_COP.1/ENC and FCS_COP.1/MAC (cf. the SFR FDP_UCT.1 and FDP_UIT.1). (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA and FCS_RND.1 establish the key management for the secure messaging keys. The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.

Note, neither the security objective OT.Data_Conf nor the SFR FIA_UAU.5 requires the Personalization Agent to use the Basic Access Control Authentication Mechanism or secure messaging.

OT.Identification addresses the storage of the IC Identification Data uniquely identifying the MRTD's chip in its non-volatile memory. This will be ensured by TSF according to SFR FAU_SAS.1.

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

OT.Prot_Abuse-Func is ensured by the SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other features which may not be used after TOE Delivery.


OT.Prot_Inf_Leak requires the TOE to protect confidential TSF data stored and/or processed in the MRTD's chip against disclosure

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines, which is addressed by the SFR FPT_EMS.1,
- by forcing a malfunction of the TOE, which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE, which is addressed by the SFR FPT_PHP.3

OT.Prot_Phys-Tamper is covered by the SFR FPT_PHP.3.

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


9.3.3. SFR dependency rationale

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

Security Functional Requirement	CC dependencies	Satisfied dependencies
FAU_SAS.1	No Dependencies	
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/ENC, FCS_COP.1/MAC
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1
FCS_COP.1/SHA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4 See rationale
FCS_COP.1/ENC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/AUTH	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	See rationale
FCS_COP.1/MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1, FCS_CKM.4
FCS_RND.1	No Dependencies	
FIA_UID.1	No Dependencies	
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FIA_UAU.4	No Dependencies	
FIA_UAU.5	No Dependencies	
FIA_UAU.6	No Dependencies	
FIA_AFL.1	(FIA_UAU.1)	FIA_UAU.1
FDP_ACC.1	(FDP_ACF.1)	FDP_ACF.1
FDP_ACF.1	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1 See rationale
FDP_UCT.1	(FDP_ACC.1 or FDP_IFC.1) and (FDP_ITC.1 or FDP_TRP.1)	FDP_ACC.1 See rationale
FDP_UIT.1	(FDP_ACC.1 or FDP_IFC.1) and (FDP_ITC.1 or FDP_TRP.1)	FDP_ACC.1 See rationale
FMT_SMF.1	No Dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1
FMT_LIM.1	No Dependencies	
FMT_LIM.2	No Dependencies	
FMT_MTD.1/INI_ENA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/INI_DIS	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/KEY_WRITE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FPT_EMS.1	No Dependencies	
FPT_FLS.1	No Dependencies	
FPT_TST.1	No Dependencies	
FPT_PHP.3	No Dependencies	

Rationale for the exclusion of dependencies:

- The dependency (FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) of FCS_COP.1/SHA is **unsupported**. The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.
- The dependency (FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) of FCS_COP.1/AUTH is **unsupported**. The SFR FCS_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT_MTD.1/INI_ENA) by the manufacturer. Thus there is neither the necessity to generate or import a key during the

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

addressed TOE lifecycle by the means of FCS_CKM.1 or FDP_ITC. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4, too.

- **The dependency FCS_CKM.4 of FCS_COP.1/AUTH is unsupported.** The SFR FCS_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT_MTD.1/INI_ENA) by the manufacturer. Thus there is neither the necessity to generate or import a key during the addressed TOE lifecycle by the means of FCS_CKM.1 or FDP_ITC. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4, too.
- **The dependency FMT_MSA.3 of FDP_ACF.1 is unsupported.** The access control TSF according to FDP_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.
- **The dependency (FTP_ITC.1 or FTP_TRP.1) of FDP_UCT.1 is unsupported.** The SFR FDP_UCT.1 requires the use secure messaging between the MRTD and the BIS. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.
- **The dependency (FTP_ITC.1 or FTP_TRP.1) of FDP_UIT.1 is unsupported.** The SFR FDP_UIT.1 requires the use secure messaging between the MRTD and the BIS. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

9.3.4. SAR – Evaluation Assurance Level Rationale


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

EAL 4 provides assurance by an analysis of the security functions, specifications, guidance, design of the TOE, and the implementation, to understand the security behavior. The analysis is supported by independent testing of the security functions and an independent vulnerability analysis demonstrating resistance to penetration attackers.

EAL4 also provides assurance through the use of development environment controls and configuration management including automation, and evidence of secure delivery procedures.

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.


9.3.5. SAR – Dependency rationale

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

Security Assurance Requirement	CC dependencies	Satisfied dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.4 ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3 ALC_TAT.1
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4 ALC_DVS.2 ALC_LCD.1
ALC_CMS.4	No dependencies	
ALC_DEL.1	No dependencies	
ALC_DVS.2	No dependencies	
ALC_LCD.1	No dependencies	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1 ASE_INT.1 ASE_REQ.2
ASE_ECD.1	No dependencies	
ASE_INT.1	No dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1 ASE_OBJ.2
ASE_SPD.1	No dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4 ASE_INT.1 ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4 ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1 ADV_TDS.3 ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4 AGD_OPE.1 AGD_PRE.1 ATE_COV.2 ATE_FUN.1
AVA_VAN.3	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1 ADV_FSP.4 ADV_IMP.1 ADV_TDS.3 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1


The table here-above shows that all SAR dependencies are met.

9.4. COMPOSITION TASKS – SFR PART


	Reference	D1390182	Release	1.2p <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level	Public	Pages	68

The following table (see next page) lists the SFRs that are declared in the security target [ST_IC], and separates them in relevant platform¹-SFRs (RP_SFR) and irrelevant platform-SFRs (IP_SFR). The table also provides the link between the relevant platform-SFRs and the composite product SFRs.


¹ Using the composition tasks terminology, the platform is the P60D081 chip.

	Reference	D1390182	Release	1.2p <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level	Public	Pages	68


Platform-SFR	Platform-SFR content	Platform-SFR additional information	RP_SFR	IP_SFR	Composite product SFRs
FRU_FLT.2	Limited fault tolerance: The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1).	None	X		FPT_FLS.1
FPT_FLS.1	Failure with preservation of secure state: The TSF shall preserve a secure state when the following types of failures occur: exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur.	None	X		FPT_FLS.1
FMT_LIM.1	The TSF shall be designed and implemented in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Limited capability and availability Policy (TEST).	Limited capability and availability Policy (TEST) Deploying Test Features after TOE Delivery does not allow user data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.	X		FMT_LIM.1
FMT_LIM.2	The TSF shall be designed and implemented in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: Limited capability and availability Policy (TEST).		X		FMT_LIM.2
FAU_SAS.1 / HW	The TSF shall provide the test process before TOE Delivery with the capability to store the Initialization Data, Pre-personalization Data or other data in the EEPROM.	None	X		FAU_SAS.1
FDP_SDC.1 / EEPROM	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the EEPROM.	None	X		FDP_ACC.1 FDP_ACF.1
FDP_SDC.1 / RAM	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the RAM.	None	X		FDP_ACC.1 FDP_ACF.1
FDP_SDI.2 /	The TSF shall monitor user data stored in containers controlled	Each EEPROM memory block is	X		FPT_FLS.1

	Reference D1390182	Release 1.2p (Printed copy not controlled: verify the version before using)
	Classification Level Public	Pages 68


Platform-SFR	Platform-SFR content	Platform-SFR additional information	RP_SFR	IP_SFR	Composite product SFRs
HW	by the TSF for integrity violations due to ageing on all objects, based on the following attributes: User data including code stored in the EEPROM. Upon detection of a data integrity error, the TSF shall adjust the EEPROM write operation.	considered as one container and the adjustment is done for one complete EEPROM memory block.			
FDP_SDI.2 / EEPROM	The TSF shall monitor user data stored in containers controlled by the TSF for modification, deletion, repetition or loss of data on all objects, based on the following attributes: parity bits of each byte in the EEPROM. Upon detection of a data integrity error, the TSF shall correct 1-bit attack detectors in the EEPROM automatically and trigger a security reset for more-than-one-bit attack detectors.	None	X		FDP_ACC.1 FDP_ACF.1
FDP_SDI.2 / RAM	The TSF shall monitor user data stored in containers controlled by the TSF for modification, deletion, repetition or loss of data on all objects, based on the following attributes: parity bits of each byte in the RAM. Upon detection of a data integrity error, the TSF shall trigger a security reset.	None	X		FDP_ACC.1 FDP_ACF.1
FDP_SDI.2 / ROM	The TSF shall monitor user data stored in containers controlled by the TSF for modification, deletion, repetition or loss of data on all objects, based on the following attributes: parity bits of each byte in the ROM. Upon detection of a data integrity error, the TSF shall trigger a security reset.	None	X		FDP_ACC.1 FDP_ACF.1
FPT_PHP.3	The TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced.	None	X		FPT_PHP.3
FDP_IFC.1	The TSF shall enforce the Data Processing Policy on all confidential data when they are processed or transferred by the TOE or by the Security IC Embedded Software.	Data Processing Policy User data of the Composite TOE	X		FDP_ACC.1, FDP_ACF.1 FDP_UCT.1

	Reference D1390182	Release 1.2p (Printed copy not controlled: verify the version before using)
	Classification Level Public	Pages 68


Platform-SFR	Platform-SFR content	Platform-SFR additional information	RP_SFR	IP_SFR	Composite product SFRs
		and TSF data shall not be accessible from the TOE except when the Security IC Embedded Software decides to communicate the user data of the Composite TOE via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Security IC Embedded Software.			FPT_EMS.1
FDP_ITT.1	The TSF shall enforce the Data Processing Policy to prevent the disclosure of user data when it is transmitted between physically-separated parts of the TOE.		X		FDP_ACC.1, FDP_ACF.1 FDP_UCT.1 FPT_EMS.1
FPT_ITT.1	The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE. The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as separated parts of the TOE.		X		FDP_ACC.1, FDP_ACF.1 FDP_UCT.1 FPT_EMS.1
FCS_RNG.1 / HW	The TSF shall provide a physical random number generator that implements: * A total failure test [...] The TSF shall provide octets of bits that meet [...]	None	X		FCS_RND.1
FCS_COP.1 / TDES	The TSF shall perform: encryption and decryption in accordance with a specified cryptographic algorithm: TDES in ECB mode and provide hardware support for CBC mode and cryptographic key sizes: 112 or 168 bits that meet the following NIST SP800-67, NIST SP800-38A.	None	X		FCS_COP.1/ENC FCS_COP.1/AUTH FCS_COP.1/MAC
FCS_CKM.4 / TDES	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting the internal stored key that meets the following: none	None	X		FCS_CKM.4
FCS_COP.1 / AES	The TSF shall perform decryption and encryption in accordance with a specified cryptographic algorithm: AES in ECB mode and provide hardware support for CBC mode and cryptographic key sizes 128, 192 or 256 bit that meet the following FIPS 197, NIST SP800-38A.	None		X	AES is not used by the Composite TOE
FCS_CKM.4 / AES	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting the internal stored key that meets the following: none	None		X	AES is not used by the Composite TOE
FCS_CKM.1 /	The TSF shall generate cryptographic keys in accordance with	None		X	PUF not supported by the

	Reference D1390182	Release 1.2p (Printed copy not controlled: verify the version before using)
	Classification Level Public	Pages 68


Platform-SFR	Platform-SFR content	Platform-SFR additional information	RP_SFR	IP_SFR	Composite product SFRs
PUF	a specified cryptographic key generation algorithm key derivation function based on PUF and specified cryptographic key sizes 128 bits that meet the following: [19]				composite TOE
FCS_CKM.4 / PUF	The TSF shall destroy cryptographic keys derived by PUF block in accordance with a specified cryptographic key destruction method flushing of key registers that meets the following: none	None		X	PUF not supported by the composite TOE
FCS_COP.1 / PUF_AES	The TSF shall perform decryption and encryption in accordance with a specified cryptographic algorithm AES in CBC mode and cryptographic key size 128 bits that meets the following: FIPS 197 [20], NIST SP800-38A [24].	None		X	PUF not supported by the composite TOE
FCS_COP.1 / PUF_MAC	The TSF shall perform CBC-MAC used for calculation of a PUF authentication in accordance with a specified cryptographic algorithm AES in CBC-MAC and cryptographic key size 128 bit that meet the following: FIPS 197 [20], NIST Special Publication 800-38A [24] and ISO/IEC 9797-1 (MAC algorithm 1) [26].	None		X	PUF not supported by the composite TOE
FDP_ACC.1 / MEM	The TSF shall enforce the Access Control Policy on all code running on the TOE, all memories and all memory operations.	None	X		FDP_ACC.1
FDP_ACF.1 / MEM	The TSF shall enforce the Access Control Policy to objects based on the following: all subjects and objects and the attributes CPU mode, the MMU Segment Table, the Special Function Registers to configure the MMU segmentation and the Special Function Registers related to system management. The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed [...] The TSF shall explicitly authorize access of subjects to objects based on the following additional rules [...] The TSF shall explicitly deny access of subjects to objects based on the following additional rules [...]	None	X		FDP_ACF.1
FMT_MSA.1 / MEM	The TSF shall enforce the Access Control Policy to restrict the ability to modify the security attributes Special Function Registers to configure the MMU segmentation to code executed in the System Mode.	None	X		FDP_ACC.1 FDP_ACF.1

	Reference D1390182	Release 1.2p (Printed copy not controlled: verify the version before using)
	Classification Level Public	Pages 68

Platform-SFR	Platform-SFR content	Platform-SFR additional information	RP_SFR	IP_SFR	Composite product SFRs
FMT_MSA.3 / MEM	The TSF shall enforce the Access Control Policy to provide restrictive default values for security attributes that are used to enforce the SFP. The TSF shall allow no subject to specify alternative initial values to override the default values when an object or information is created.	None	X		FDP_ACC.1 FDP_ACF.1
FDP_ACC.1 / SFR	The TSF shall enforce the Access Control Policy on all code running on the TOE, all Special Function Registers, and all Special Function Register operations.	None	X		FDP_ACC.1
FDP_ACF.1 / SFR	The TSF shall enforce the Access Control Policy to objects based on the following: all subjects and objects and the attributes CPU mode, the MMU Segment Table and the Special Function Registers MMU_FWCTRL and MMU_FWCTRLH. The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed [...] The TSF shall explicitly authorize access of subjects to objects based on the following additional rules [...] The TSF shall explicitly deny access of subjects to objects based on the following additional rules [...].	None	X		FDP_ACF.1
FMT_MSA.1 / SFR	The TSF shall enforce the Access Control Policy to restrict the ability to modify the security attributes defined in Special Function Registers to code executed in a CPU mode which has write access to the respective Special Function Registers.	None	X		FDP_ACC.1 FDP_ACF.1
FMT_MSA.3 / SFR	The TSF shall enforce the Access Control Policy to provide restrictive default values for security attributes that are used to enforce the SFP. The TSF shall allow no subject to specify alternative initial values to override the default values when an object or information is created.	None	X		FDP_ACC.1 FDP_ACF.1
FMT_SMF.1 / HW	The TSF shall be capable of performing the following management functions: Change of the CPU mode by calling a system call vector (SVEC) or firmware vector (FVEC) address, change of the CPU mode by invoking an exception or interrupt,	None	X		FDP_ACC.1 FDP_ACF.1

	Reference D1390182	Release 1.2p (Printed copy not controlled: verify the version before using)
	Classification Level Public	Pages 68

Platform-SFR	Platform-SFR content	Platform-SFR additional information	RP_SFR	IP_SFR	Composite product SFRs
	change of the CPU mode by finishing an exception/interrupt (with a RETI instruction), change of the CPU mode with a special LCALL/ACALL/ECALL address, change of the CPU mode by writing to the respective bits in the CPU_CSR Special Function Register and modification of the Special Function Registers containing security attributes, and modification of the MMU Segment Table, and temporary disabling and enabling of the security functionality EEPROM Size, CXRAM Size, AES coprocessor, Fame2 coprocessor and permanent disabling and enabling of the security functionality EEPROM Size, CXRAM Size, AES coprocessor, Fame2 coprocessor and permanent disabling and enabling of the security functionality MIFARE Software and MIFARE Software EEPROM size.				

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

10. TOE summary specification

The TOE being a composite product, the TOE Security Functionality is provided by both the Sealys eTravel SCOSTA-CL embedded software (including the OS layers JKernel and Drivers) and by the IC.

10.1. SEALYS eTRAVEL SCOSTA-CL EMBEDDED SOFTWARE

SF.REL Protection of data

The SF.REL security feature provides the protection of data on the TOE. It includes:

- Physical protection of the TOE as defined in
 - FPT_PHP.3 to protect the TOE against physical attacks
 - FPT_EMS.1 to implement measures to limit information contained in electromagnetic and current emissions
 - FPT_FLS.1 to preserve secure states
- The test mechanisms as defined in FPT_TST.1 to preserve secure states
- Protection against misuse of tests as defined in FMT_LIM.1 and FMT_LIM.2 to limit the capabilities and availability of the TSF after TOE delivery.

SF.AC Access control


The SF.AC security feature provides the access control of the TOE. It includes:

- the access control by the terminal as defined in FDP_ACC.1 and FDP_ACF.1 to enforce the access control mechanism
- the access control to specific data as defined in
 - FAU_SAS.1 to provide initialization data accessible for reading and writing action to the pre-personalizer and the personalizer
 - FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ to restrict the ability for reading/writing of Initialization Data, Prepersonalization Data, Document Basic Access Keys and Personalization Agent Keys to the Manufacturer and the Personalization Agent
- the role management as defined in FMT_SMR.1 to maintain the different roles according to the life cycle status
- the management functions linked to the different states of the TOE as defined in FMT_SMF.1 to maintain the different roles according to the life cycle status

SF.SYM_AUTH Symmetric authentication

The SF.SYM_AUTH security feature provides the symmetric authentication functions to the TOE. It includes the identification and authentication as defined in

- FIA_AFL.1 to detect unsuccessful authentication attempts with required consequences
- FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the MRTD's chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt
- FIA_UAU.4 to prevent reuse of authentication data to strengthen the authentication of the user

	Reference	D1390182	Release	1.2p (Printed copy not controlled: verify the version before using)
	Classification Level	Public	Pages	68

- FIA_UAU.5 to enforce the TOE to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys
- FIA_UAU.6 to request secure messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism

SF.SM Secure messaging

The SF.SM function provides the secure messaging of the TOE. It includes:

- The secure transfer of data through SM as defined in FDP_UCT.1 and FDP_UIT.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal
- The cryptographic mechanisms used for the authentication and the SM, as defined in
 - FCS_CKM.1, FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/MAC, FIA_AFL.1 and FCS_RND.1. Some cryptographic mechanisms are used for both authentication and secure messaging. For convenience, they are grouped in this function
 - The erasure of session keys as defined in FCS_CKM.4

10.2. P60D081 INTEGRATED CIRCUIT

The following IC security features and services also participate to the TOE protection:

- **SS.RNG**: Random Number Generator
- **SS.TDES**: Triple-DES coprocessor
- **SF.OPC**: Control of Operating Conditions
- **SF.PHY**: Protection against Physical Manipulation
- **SF.LOG**: Logical Protection
- **SF.COMP**: Protection of Mode Control
- **SF.MEM_ACC**: Memory Access Control
- **SF.SFR_ACC**: Special Function Register Access Control

These security features and services are described further in the [ST_IC] document.

10.3. TSS MAPPING TABLE

Security Functional Requirement	Coverage by TSS Security Function(s)
FAU_SAS.1	SF.AC
FCS_CKM.1	SF.SM
FCS_CKM.4	SF.SM
FCS_COP.1/SHA	SF.SM
FCS_COP.1/ENC	SF.SM
FCS_COP.1/AUTH	SF.SM
FCS_COP.1/MAC	SF.SM
FCS_RND.1	SF.SM



Reference **D1390182**

Release **1.2p**
(Printed copy not controlled: verify the version before using)

Classification Level **Public**

Pages **68**

Security Functional Requirement	Coverage by TSS Security Function(s)
FIA_UID.1	SF.SYM_AUTH
FIA_UAU.1	SF.SYM_AUTH
FIA_UAU.4	SF.SYM_AUTH
FIA_UAU.5	SF.SYM_AUTH
FIA_UAU.6	SF.SYM_AUTH
FIA_AFL.1	SF.SYM_AUTH, SF.SM
FDP_ACC.1	SF.AC
FDP_ACF.1	SF.AC
FDP_UCT.1	SF.SM
FDP_UIT.1	SF.SM
FMT_SMF.1	SF.AC
FMT_SMR.1	SF.AC
FMT_LIM.1	SF.REL
FMT_LIM.2	SF.REL
FMT_MTD.1/INI_ENA	SF.AC
FMT_MTD.1/INI_DIS	SF.AC
FMT_MTD.1/KEY_WRITE	SF.AC
FMT_MTD.1/KEY_READ	SF.AC
FPT_EMS.1	SF.REL
FPT_FLS.1	SF.REL
FPT_TST.1	SF.REL
FPT_PHP.3	SF.REL

END OF DOCUMENT