UM_security_target_lite_eMRTD_BAC

User manual

ST-Doc eMRTD BAC on STeID JC Open OS v1.0 - Security Target Lite

Common Criteria
for IT security evaluation

1 Purpose

This document presents the Security Target of ST-Doc eMRTD BAC on STeID JC Open OS v1.0.

2 Scope

This document is public.

3 Reference documents

Table 1: List of reference CC documents

Reference	Document
[CC_P1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 5. April 2017
[CC_P2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1 Revision 5. April 2017
[CC_P3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. Version 3.1. Revision 5. April 2017.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1. Revision 5. April 2017. CCMB-2017-04-004.
[AIS31/20]	Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31, A proposal for Functionality classes for random number generators Version 2.0 vom 18.09.2011, Bundesamt für Sicherheit in der Informationstechnik (BSI)
[AIS36]	Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 36, Version 2 vom 12.11.2007, Bundesamt für Sicherheit in der Informationstechnik (BSI)
[SOGIS-COMP]	Composite product evaluation for Smart Cards and similar devices, version 1.5.1, May 2018
[CERT_ST31N600]	ST31N600 A03, ANSSI - CC - 2022/21 - R02
[CERT_ STeID_JCOS]	SteID JC Open OS v1.0, v1.3.2, NSCIB-CC-2400079-01

Table 2: List of reference Protection Profiles and Technical Guidelines

Reference	Document
[PP-0055]	CC Protection Profile – Machine Readable Travel Document with “ICAO Application", Basic Access Control – Version 1.10, 25 March 2009
[PP-0056]	CC Protection Profile – Machine Readable Travel Document with “ICAO Application", Extended Access Control with PACE – Version 1.3.2, 5 December 2012
[ICAO_9303]	ICAO Doc 9303, Machine Readable Travel Documents – Part 1 Machine Readable Passports – Eighth Edition, 2021
[ICAO_TR]	TECHNICAL REPORT – Supplemental Access Control for Machine Readable Travel Documents – Version 1.1 – April 15, 2014
[TR-03110-1]	Technical Guideline TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20. March 2012
[TR-03110-2]	Technical Guideline TR-03110-2: Advanced Security Mechanisms for Machine Readable Travel Documents Part 2, Version 2.10, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-03-20
[TR-03110-3]	Technical Guideline TR-03110-3: Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 – Common Specifications, Version 2.11, 12. July 2013
[TR-03111]	Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 1.11, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009-04-17

Table 3: List of reference Specifications

Reference	Document
[SP800-67]	NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, revised January 2012, National Institute of Standards and Technology
[FIPS_PUB_197]	Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), U.S. Department of Commerce/National Institute of Standards and Technology, November 26, 2001
[FIPS186]	Federal Information Processing Standards Publication FIPS PUB 186-3, Digital Signature Standard (DSS), 2009-06
[FIPS_180-2]	FIPS Publication 180-2: SECURE HASH STANDARD, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1
[SP800-38B]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005.
[SP800-38A]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, Special Publication 800-38A 2001 Edition
[SP800-90A]	National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators Special Publication 800-90A Rev.1 April 2014
[SP800-22]	National Institute of Standards and Technology, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications Special Publication 800-22 Rev.1a April 2010

[ISO7816]	ISO 7816-4, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, ISO/IEC, IS 2013
[ISO7810]	ISO/IEC 7810:2003, Identification cards -- Physical characteristics, ISO, 2010-05-03
[ISO 10116]	ISO/IEC 10116, Information technology - Security Techniques -- Modes of operation of an n-bit block cipher, ISO, 2006.
[ISO_9797-1]	ISO/IEC 9797-1:1999: Information technology - Security techniques – Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher
[ISO_9796-2]	ISO/IEC 9796-2:2010 Information technology — Security techniques Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms
[ISO_18013]	ISO/IEC 18013-2 – Information technology – Personal identification – ISO-compliant driving Licence Part 2: Machine-readable technologies – First Edition, 2008
[ISO_18013]	ISO/IEC 18013-3 – Information technology – Personal identification – ISO-compliant driving Licence Part 3: Access control, authentication and integrity validation – Second Edition, 2017

Table 4: List of reference STMicroelectronics documents

Reference	Document
[ST_SteidJCOS]	STMicroelectronics, STeID JC Open OS v1.0 Security Target, Version H, 2025-10-24
[AGD_PRE]	STMicroelectronics, ST-Doc ICAO on STeID JC Open OS - Preparative User Guidance for EMRTDApplet, Rev. 2, January 2026
[AGD_OPE]	STMicroelectronics, ST-Doc ICAO on STeID JC Open OS - Operational User Guidance for EMRTDApplet, Rev. 2, January 2026
[AGD_OPE_STeID]	STeID JC Open OS v1.0 – Operational guidance document (AGD_OPE), Rev. 3

4 Abbreviations

Table 5: List of abbreviations

Term	Definition
ATR	Answer To Reset
ATS	Answer To Select
AUTH	External Authentication
BIS	Basic Inspection System
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
DF	Dedicated File
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
EF	Elementary File
Enc	Encryption
ENC	Content Data Encryption
GIS	General Inspection System
HW	Hardware
ICCSN	Integrated Circuit Card Serial Number.
ID	Identifier

Term	Definition
IT	Information Technology
MF	Master File
MRTD	Machine Readable Travel Document
MRZ	Machine readable zone
n.a.	Not applicable
NIST	National Institute of Standards and Technology
OSP	Organizational security policy
PKI	Public Key Infrastructure
PP	Protection Profile
PT	Personalization Terminal
PTRNG	Physical True Random Number Generator
PUK	PIN Unlock Key
RNG	Random Number Generator
SAR	Security Assurance Requirement
SEMA	Simple Electromagnetic Analysis
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SIG	Content Data Signature
Sign	Signature
SPA	Simple Power Analysis
ST	Security Target
TOE	Target Of Evaluation
TRNG	True Random Number Generator
TSF	TOE Security Functionality

5 Glossary

Term	Description
Active Authentication	Security mechanism defined in [ICAO_9303] option by which means the travel document's chip proves and the inspection system verifies the identity and authenticity of the travel document's chip as part of a genuine travel document issued by a known State or Organization.
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the travel document's chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm the travel document and its data elements on the travel document's chip were created by the issuing State or Organization.
Basic Access Control (BAC)	Security mechanism defined in [ICAO_9303] by which means the travel document's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys.
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the travel document's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical travel document.
Biographical data (biodata)	The personalized details of the travel document's holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a travel document. [ICAO_9303]

Term	Description
Biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) digital portrait and (ii) optional biometric reference data. Counterfeit an unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAO_9303]
Country Signing CA Certificate (CCSCA)	Self-signed certificate of the Country Signing Certification Authority Public Key (KPuCSCA) issued by Country Signing Certification Authority and stored in the inspection system.
Document Basic Access Keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the travel document's chip and the inspection system [ICAO_9303]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Basic Access Key Derivation Algorithm	The [ICAO_9303] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
Document Security Object (SOD)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the travel document's chip. It may carry the Document Signer Certificate (CDS) [ICAO_9303]
Eavesdropper	A threat agent with Enhanced-Basic attack potential reading the communication between the travel document's chip and the inspection system to gain the data on the travel document's chip.
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; see [ICAO_9303] (there "Machine Readable Travel Document").
Travel document (electronic)	The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.
Travel document Holder	The rightful holder of the travel document for whom the issuing State or Organization personalized the travel document.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO_9303]
Extended Access Control	Security mechanism identified in [ICAO_9303] by which means the travel document's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Private Key and to get write and read access to the logical travel document and TSF data.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [ICAO_9303]

Term	Description
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 travel documents. [ICAO_9303]
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [ICAO_9303]
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [ICAO_9303]
Initialization	Process of writing Initialization Data to the TOE.
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as travel document's material (IC identification data).
Inspection	The act of an organization examining a travel document presented to it by the travel document's presenter and verifying its authenticity [ICAO_9303]
Inspection system (IS)	Technical system used to examine the travel document presented by the document holder, to verify its authenticity and to verify the holder as travel document holder
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit.
Integrity	Ability to confirm the travel document and its data elements on the travel document's chip have not been altered from that created by the issuing State or Organization
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	Country issuing travel documents [ICAO_9303]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO_9303]. The capacity expansion technology used is the travel document's chip.
Logical travel document	Data of the travel document's holder stored according to the Logical Data Structure as specified by ICAO [ICAO_9303] on the integrated circuit.
Machine readable travel document (MRTD)	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [ICAO_9303]

Term	Description
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [ICAO_9303]
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO_9303]
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes - the file structure implementing the LDS [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, EF.DG 16, EF.COM and EF.SOD) and - the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by, [ICAO_TR], 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	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Personalization	The process by which the portrait, signature and biographical data are applied to the document. This may also include the optional biometric data collected during the "Enrolment" (cf. TOE life cycle, Phase 3, Step 6).
Personalization Agent	The agent acting on the behalf of the issuing State or Organization to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or 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.

Term	Description
Physical travel document	Physical part of the travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) biographical data, data of the machine-readable zone, photographic image and other data.
Pre-Personalization	Process of writing Pre-Personalization Data to the TOE including the creation of the MRTD Application (see TOE life cycle)
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 Active Authentication Key Pair and the Personalization Agent Key Pair.
Pre-personalized MRTD's chip	MRTD's chip equipped with a unique identifier and a unique asymmetric Active Authentication Key Pair of the chip
Primary Inspection System (PIS)	An inspection system that contains a terminal for the contactless communication with the MRTD's chip and does not implement the terminals part of the Basic Access Control Mechanism.
Random identifier	Random identifier used to establish a communication to the TOE in Phase 3 and 4 preventing the unique identification of the MRTD and thus participates in the prevention of traceability.
Receiving State	The Country to which the Traveler is applying for entry. [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. [ICAO_9303]
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.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE ([CC_P1]).
Unpersonalized travel document	The MRTD that contains the MRTD Chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalization Agent from the Manufacturer.
User data	Data created by and for the user, that does not affect the operation of the TSF ([CC_P1]).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template.
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

6 Introduction

The ST-Doc v1.0 is a Java Card Applet that implements the Machine Readable Travel Document (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO) and supports the Basic Access Control (BAC), the Chip Authentication (CA) and the Active Authentication (AA), as described in the 'ICAO Doc 9303' [ICAO_9303].

The applet is integrated with the CC certified STMicroelectronics Java Card™ operating system 'STeID JC Open OS v1.0' [ST_SteidJCOS], designed on the CC certified STMicroelectronics ST31N600 Security Integrated Circuit [CERT_ST31N600][CERT_ST31N600].

The TOE certification depends on the certification of the platform 'STeID JC Open OS v1.0' [ST_SteidJCOS][CERT_ STeID_JCOS].

The product is a contact/contactless chip that can be personalized as

- electronic travel document according to [ICAO_9303],
- ISO Driving Licence electronic document according to [ISO_18013], or
- Digital Identity electronic document.

The product supports user authentication by PACE PIN/PUK when it is personalized as Digital Identity electronic document.

This document is the Security Target for the Common Criteria evaluation of the ST-Doc eMRTD BAC on STeID JC Open OS v1.0. It provides information about the Target of Evaluation (TOE), that is the item subject of the Common Criteria evaluation. The TOE is evaluated in composition with the STMicroelectronics Java Card Platform STeID JC Open OS.

6.1 ST Reference

Title:	ST-Doc eMRTD BAC on STeID JC Open OS v1.0 Security Target Lite
Developer:	STMicroelectronics, Z.I. Marcianise Sud, 81025, Marcianise (CE), ITALY
Version:	Rev. C
Date:	January, 2026

6.2 TOE Reference

TOE name:	ST-Doc eMRTD BAC
TOE version:	1.0
com.st.steid.bsi version:	1.4
com.st.steid.emrtd version:	1.6

The ST-Doc eMRTD BAC is made of two Java Card packages: the com.st.steid.bsi library package and the com.st.steid.emrtd package containing the EMRTDApplet class that implements the MRTD application.

The TOE version 1.0 contains the com.st.steid.bsi and the com.st.steid.emrtd packages with version defined above. The TOE version can be verified using the GET_DATA command. In fact, the concatenation of the two versions is returned by that command, according to the instructions in section "TOE identification" of the Preparative User Guidance for EMRTDApplet of this TOE [AGD_PRE].

6.3 Platform Reference

STeID JC Open OS v1.0 on ST31N600 Security Integrated Circuit

OS Identification: 00000900

OS Version: 00010302

CC certificate [CERT_ STeID_JCOS]

OS Identification and OS Version can be verified using the GET_DATA command according to the instructions in the section "TOE identification" of the Preparative User Guidance of this TOE [AGD_PRE].

6.4 TOE Overview

The TOE is the STMicroelectronics ST-Doc eMRTD BAC, integrated with the STMicroelectronics Java Card™ operating system STeID JC Open OS v1.0, designed on the STMicroelectronics ST31N600 Security Integrated Circuit. The TOE is evaluated according to the composition approach.

The TOE is a contact/contactless chip personalized as electronic travel document according to [ICAO_9303].

The TOE is based on the Machine Readable Travel Document (MRTD) and comply with the requirements and recommendations of the International Civil Aviation Organization (ICAO) and implement the advanced security methods Basic Access Control (BAC) and the Active Authentication (AA) as described in the ‘ICAO Doc 9303’ [ICAO_9303].

The TOE protects the user data and the TSF data needed to execute the access protocols and to verify the integrity and authenticity of user data.

6.4.1 TOE Description

The TOE is a composite product comprising hardware, software and documentation.

The physical scope is defined as follows:

- Certified platform: the STMicroelectronics Java Card™ Operating System STeID JC Open OS v1.0 on the STMicroelectronics ST31N600 Secure Integrated Circuit [ST_SteidJCOS]
- Software: the STMicroelectronics TOE Java Card applet EMRTDApplet implementing the Machine Readable Travel Document (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO) programmed according to the Logical Data Structure (LDS) and implementing the advanced security methods Basic Access Control (BAC) and the Active Authentication (AA) as described in the ‘ICAO Doc 9303’ [ICAO_9303]
- Documentation:
  - ST-Doc ICAO on STeID JC Open OS - Preparative User Guidance for EMRTDApplet [AGD_PRE]
  - ST-Doc ICAO on STeID JC Open OS - Operational User Guidance for EMRTDApplet [AGD_OPE]

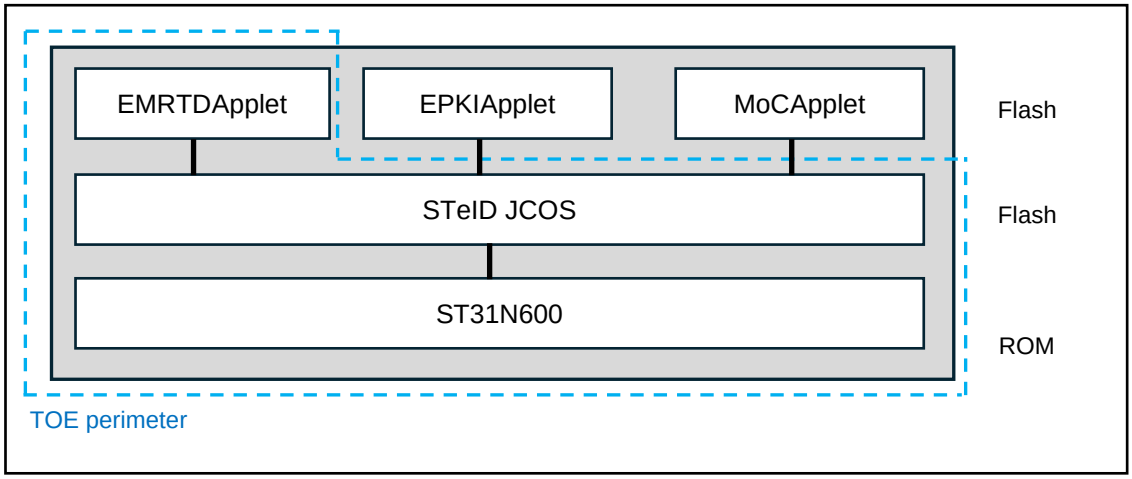
The platform guidance, as described in the ST of the platform [ST_SteidJCOS], is also included.

The first two components of the TOE (hardware and software) are delivered by trusted couriers at the end of the lifecycle Phase 2 “TOE Manufacturing” Step 3 “Embedded software loading” in wafer or micromodule D70, D76, CB6 format to Document manufacturer (see chap. 6.4.3).

The last component of the TOE (documentation) is delivered at the end of the lifecycle Phase 2 Step 3 “Embedded software loading” in printed copy by trusted couriers or in enciphered pdf format by e-mail to Document Personalization Agent (see chap. 6.4.3).

The Figure 1 shows the composition of the TOE parts, including their location in the memory areas of the TOE. The TOE is a Java Card Flash memory-based product.

Figure 1 - TOE architecture



Important note: The product is an open Java Card implementation including pre-loaded packages of EMRTDApplet, EPKIApplet, and MoCApplet. The EPKIApplet and the MoCApplet are out of the scope of the TOE. The EMRTDApplet is default selected after product reset. The pre-loaded applets are installed and initialized in Phase 2 “TOE Manufacturing” Step 3 “Embedded software loading” of TOE life cycle (see chap. 6.4.3). Upgrading of the applets and loading of further applets post-issuing is possible.

The STeID JC Open OS Operating System and the EMRTDApplet Java Card applet are loaded in the non-volatile memory (NVM) of the IC during the manufacturing phase.

The EMRTDApplet uses the IC RAM and NVM for storage of operational and permanent data, to provide security functionality.

During the “TOE Operational Use” life cycle phase (Phase 4) the EMRTDApplet interacts with other external entities.

This ST is based on the ST of the underlying STeID JC Open OS platform [ST_SteidJCOS].

6.4.2 TOE usage and security features for operational use

A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents the document to the inspection system to prove his or her identity. The document in context of this ST contains:

- 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), and
- data elements on the TOE according to LDS for contactless machine reading. The authentication of the traveler is based on

i. the possession of a valid document personalized for a holder with the claimed identity as given on the biographical data page, and

ii. optional biometrics using the reference data stored in the MRTD.

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

For this ST the MRTD is viewed as unit of:

- **the physical MRTD** as travel document in form of paper, plastic and chip (TOE). It presents visual readable data including (but not limited to) personal data of the document holder:
  i. the biographical data on the biographical data page of the MRTD
  ii. the printed data in the Machine-Readable Zone (MRZ)
  iii. the printed portrait
- **the logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [ICAO_9303] as specified by ICAO on the contact based or contactless integrated circuit. It presents contact based / contactless readable data including (but not limited to) personal data of the document holder:
  i. the digital Machine-Readable Zone Data (digital MRZ data, EF.DG1)
  ii. the digitized portraits (EF.DG2)
  iii. the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[1]
  iv. the other data according to LDS (EF.DG5 to EF.DG16)
  v. the Document security object (SOD)

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and the MRTD's chip (TOE) 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 TOE) and organizational security measures (e.g. control of materials, personalization procedures) [ICAO_9303]. These security measures include the binding of the MRTD's chip (TOE) 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 TOE.

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical electronic document, Active Authentication of the electronic document's chip, Extended Access Control to and the Data Encryption of sensitive biometrics as optional security measure in the [ICAO_9303], and Password Authenticated Connection Establishment [ICAO_TR]. The Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment.

The TOE protects the integrity of logical MRTD by write-only-once access control and by physical means, and the confidentiality of logical MRTD by the Basic Access Control Mechanism.

[1] These biometric reference data are optional according to [ICAO_9303]. It is assumed that the issuing State or Organization uses this option and protects these data by means of EAC

The Basic Access Control is a security feature supported by the TOE. The inspection system:

- reads optically the MRTD,
- authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the inspection system TOE provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [ICAO_9303] normative appendix 5.

Note: For what concern the Basic Access Control Mechanism and according to the assurance level EAL 4 and augmentations stated in the Protection Profile MRTD with BAC [PP-0055] this mechanism shall be evaluated considering only enhanced basic attack potential (i.e. AVA_VAN.3)

The TOE implements the Active Authentication as defined in [ICAO_9303]. Keys for Active Authentication can be loaded into the TOE. These operations take place at personalization time.

6.4.3 Life Cycle

The life cycle of the TOE is described in the Protection Profile MRTD with BAC [PP-0055] and it is split in seven steps, grouped in four phases:

- Phase 1: “TOE Development” (steps 1 and 2)
- Phase 2: “TOE Manufacturing” (steps 3, 4, and 5)
- Phase 3: “TOE Personalization” (step 6)
- Phase 4: “TOE Operational Use” (step 7)

In the beneath discussion, the following entities and roles are identified:

- *Document Embedded Software Developer:* STMicroelectronics srl, Marcianise (CE), Italy
- *IC Developer:* STMicroelectronics SAS, Rousset, France
- *IC Manufacturer:* STMicroelectronics srl, Marcianise (CE), Italy
- *Document Manufacturer:* National accredited document manufacturing center
- *Document Personalization Agent:* Public administration or national accredited personalization center enabled to issue personalized documents

6.4.3.1 Phase 1 “TOE Development”

The TOE development includes the design of the IC and the development of the embedded software. The embedded software includes IC dedicated software, embedded cryptographic library, operating system, and applications.

The “TOE Development” is split into Step 1 and Step 2.

Phase 1 Step 1 “IC design and dedicated software development”

- Design of the IC, performed by the *IC Developer*
- Development of the IC dedicated software and embedded cryptographic library, performed by the *IC Developer*

Phase 1 Step 2 "OS and applications development"

- Development of the operating system, performed by the *Document Embedded Software Developer*
- Development of the applications, performed by the *Document Embedded Software Developer*. The binaries are always verified with the off-card verifier during their building and saved on a repository where they cannot be altered. Later the binaries are loaded on the TOE that verifies their integrity.
- Development of the guidance documentation, performed by the *Document Embedded Software Developer*

The embedded software is delivered to the *IC Manufacturer*.

6.4.3.2 Phase 2 "TOE Manufacturing"

The "TOE manufacturing" is split into Step 3, Step 4, and Step 5.

Phase 2 Step 3 "Embedded software loading"

The *IC manufacturer* makes the IC, loads the embedded software on the IC programmable memory, and delivers the IC and the guidance documentation to the *Document manufacturer*.

The TOE Delivery occurs at the end of this Phase 2 Step 3 "Embedded software loading", from the *IC manufacturer* to the *Document manufacturer*.

Phase 2 Step 4 "Document manufacturing"

The *Document manufacturer* makes the document by combining the IC with the hardware for the contactless interface.

Phase 2 Step 5 "Document initialization"

The *Document manufacturer* creates the EMRTD application (application installation) or updates it (application upgrade) and loads third-parties' packages, if any (post-issuing).

6.4.3.3 Phase 3 "TOE Personalization" (Step 6)

The *Document Personalization Agent* personalizes the TOE with:

- the survey of the document holder's biographical data,
- the enrolment of the document 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 document,
- the writing of the TOE User Data and TSF Data into the logical document. This step is performed by the Personalization Agent and includes but is not limited to creation of:
    i. the digital MRZ data (EF.DG1),
    ii. the digitized portrait (EF.DG2) and
    iii. the Document security object
- Configuration of the TSF if necessary.
- The signing of the Document security object by the Document Signer [ICAO_9303] finalizes the personalization of the genuine MRTD for the MRTD holder.

- The personalized document (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

The TSF data (data created by and for the TOE, that might affect the operation of the TOE) comprise (but are not limited to) the Personalization Agent Authentication Key(s) and the Basic Authentication Control Key

6.4.3.4 Phase 4 “TOE Operational Use” (Step 7)

The TOE is used by the document holder and the inspection systems. The user data can be read according to the security policy of the issuing State or Organization and can be used according to the security policy of the issuing State but they can never be modified.

Application note: The authorized Personalization Agents might be allowed to add (not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 “TOE Operational Use”. This will imply an update of the Document Security Object including the re-signing by the Document Signer.

Application note: The Phase 1 (steps 1 and 2) and Phase 2 Step 3 are part of the TOE evaluation. The TOE delivery is after Phase 2 Step 3 “Embedded software loading”. Phase 2 Step 4 “Document manufacturing” is of minor security relevance and so is not part of the CC evaluation under ALC. The issuing State or Organization is responsible for this production step.

6.4.4 Non-TOE hardware/software/firmware required by the TOE

The antenna, the EPKIApplet Java Card applet, and the MoCApplet Java Card applet are not in the scope of the TOE.

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. 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 not inevitable for the secure operation of the TOE.

7 Conformance claim

7.1 CC Conformance Claim

This Security Target claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model [CC_P1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components [CC_P2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements [CC_P3]

The ST claims conformance to CC Part 2 extended and CC Part 3 conformant.

For the evaluation the following methodology is used:

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology [CEM]

7.2 PP Claim

This Security Target claims strict conformance to:

- Protection Profile Machine Readable Travel Document with “ICAO Application", Basic Access Control [PP-0055]

7.3 Package Claim

This Security Target claims conformance to the assurance package EAL 4 augmented with ALC_DVS.2, as defined in [CC_P3].

7.4 Conformance Claim Rationale

This Security Target claims strict conformance to the Protection Profile MRTD with BAC [PP-0055].

All the contents of Protection Profile MRTD with BAC [PP-0055] have been added to this Security Target. In addition, the following items have been added to specify the Active Authentication functions:

- the Security Objective “OT.Active_Auth_MRTD_Proof”,
- the Security Objectives for the Operational Environment “**OE.Active_Auth_Sign**” and “**OE.Active_Auth_Verif**”,
- the Organizational Security Policies “**P.Active_Auth**”, and
- the Security Functional Requirement “**FCS_COP.1/AA**” (Cryptographic operation – Active Authentication).

The operations done for the SFRs taken from the Protection Profile MRTD with BAC [PP-0055] are clearly indicated.

The **Security Assurance Requirements** statement for the TOE in this Security Target includes all the requirements for the TOE from the Protection Profile MRTD with BAC [PP-0055].

8 Security problem definition

8.1 Assets

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

8.1.1 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]. This data is user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG 16 contain personal data of the MRTD holder. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

For interoperability reasons the 'ICAO Doc 9303' [ICAO_9303] requires that Basic Inspection Systems may have access to logical MRTD data:

- 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.

Although the BAC mechanism cannot resist attacks with high attack potential (see the Protection Profile MRTD with BAC [PP-0055]) the TOE supporting BAC and AA is in certified mode because the assurance level of AVA_VAN has been lowered to AVA_VAN.3.

The TOE prevents read access to sensitive User Data

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

A sensitive asset is the following more general one.

8.1.2 Authenticity of the MRTD's chip

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

This Security Target includes the following primary assets:

- user data stored in the TOE

8.2 Subjects and external entities

This ST considers the following subjects:

8.2.1 Manufacturer

Generic term for the IC manufacturer, producing the integrated circuit, and the MRTD manufacturer, integrating the IC with the electronic document. The Manufacturer is the default user of the TOE during the "TOE Manufacturing" life cycle phase (Phase 2). The TOE does not distinguish between the IC manufacturer and MRTD manufacturer using this role Manufacturer.

8.2.2 Personalization Agent

The agent acting on behalf of the issuing State or Organization to personalise the MRTD for the holder by some or all of the following activities:

i. establishing the identity of the holder for the biographic data in the MRTD
ii. enrolling the biometric reference data of the holder e.g. the portrait, the encoded finger image(s) and/or the encoded iris image(s)
iii. writing a subset of these data on the physical MRTD (optical personalisation) and storing them in the MRTD (electronic personalisation) for the MRTD holder as defined in [ICAO_9303]
iv. writing the document details data
v. writing the initial TSF data
vi. signing the Document Security Object defined in [ICAO_9303]

The role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the MRTD Issuer.

8.2.3 MRTD holder

The person for whom the MRTD Issuer has personalised the MRTD.

8.2.4 Traveler

A person presenting the MRTD to a terminal and claiming the identity of the MRTD holder.

The MRTD presenter can also be an attacker.

8.2.5 Terminal

Any technical system communicating with the TOE either through the contact interface or through the contactless interface.

The role 'Terminal' is the default role for any terminal being recognised by the TOE as not being BAC authenticated ('Terminal' is used by the MRTD presenter).

8.2.6 Inspection system (IS)

Technical system used to examine the MRTD presented by the document holder, to verify its authenticity and to verify the holder 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.

Application note: This ST does not distinguish between the BIS, GIS and EIS because the Extended Access Control is outside the scope.

8.2.7 Attacker

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

Additionally, to the previously definition an attacker is refined as follows:

A threat agent trying to:

i. identify and trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the printed MRZ data)

ii. read or manipulate the logical MRTD without authorization

iii. to forge a genuine MRTD

Additionally, to the definition from PACE PP [7], chap 3.1 the definition of an attacker is refined as followed: A threat agent trying

iv. (i) to manipulate the logical MRTD without authorization,

v. (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4),

vi. (iii) to forge a genuine MRTD, or

vii. (iv) to trace a MRTD.

Application note: An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged MRTD. Therefore, the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.

8.3 Assumptions

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

8.3.1 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).

8.3.2 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.

8.3.3 A.Pers_Agent (Personalization of the MRTD's chip)

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

8.3.4 A.Insp_Sys (Inspection Systems for global interoperability)

The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO_9303]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

Application note: According to [ICAO_9303] the support of the Passive Authentication mechanism is mandatory whereas the Basic Access Control is optional. This ST does not address Primary Inspection Systems therefore the BAC is mandatory.

8.3.5 A.BAC-Keys (Cryptographic quality of Basic Access Control Keys)

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the [ICAO_9303], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

Application note: When assessing the MRZ data resp. the BAC keys entropy potential dependencies between these data (especially single items of the MRZ) have to be considered and taken into account. E.g. there might be a direct dependency between the Document Number when chosen consecutively and the issuing date.

8.4 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.

8.4.1 T.Chip_ID (Identification of MRTD's chip)

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

8.4.2 T.Skimming (Skimming the logical MRTD)

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

8.4.3 T.Eavesdropping (Eavesdropping to the communication between TOE and inspection system)

- **Adverse action**: An attacker is listening to an existing communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know these data in advance.
- **Threat agent**: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance
- **Asset**: confidentiality of logical MRTD data

8.4.4 T.Forgery (Forgery of data on MRTD's chip)

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

8.4.5 T.Abuse-Func (Abuse of Functionality)

- **Adverse action**: An attacker may use functions of the TOE which shall not be used in the phase "Operational Use" in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data. This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder.
- **Threat agent**: having enhanced basic attack potential, being in possession of a legitimate MRTD
- **Asset**: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

8.4.6 T.Information_Leakage (Information Leakage from MRTD's chip)

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

8.4.7 T.Phys-Tamper (Physical Tampering)

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

8.4.8 T.Malfunction (Malfunction due to Environmental Stress)

- **Adverse action**: An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software. This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.
- **Threat agent**: having enhanced basic attack potential, being in possession of a legitimate MRTD
- **Asset**: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

8.5 Organizational 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_P1]).

8.5.1 P.Manufact (Manufacturing of the MRTD's chip)

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

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

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

8.5.3 P.Personal_Data (Personal data protection policy)

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4)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 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.

8.5.4 P.Active_Auth (Active Authentication)

The TOE implements the Active Authentication according to [ICAO_9303]

9 Security objectives

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

9.1 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.

9.1.1 OT.AC_Pers (Access Control for Personalization of logical MRTD)

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [ICAO_9303] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG 3 to EF.DG16 are added.

Application note: The OT.AC_Pers implies that (1) the data of the LDS groups written during personalization for MRTD holder (at least EF.DG1 and EF.DG2) cannot be changed by write access after personalization, (2) 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.

9.1.2 OT.Data_Int (Integrity of personal data)

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

9.1.3 OT.Data_Conf (Confidentiality of personal data)

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

Application note: The traveler 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_Confidentiality 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. Thus, the read access must be prevented even in case of a successful BAC Authentication.

9.1.4 OT.Identification (Identification and Authentication of the TOE)

The TOE must provide means to store IC Identification and Pre-Personalization Data in its nonvolatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 “Manufacturing” and Phase 3 “Personalization of the MRTD”. The storage of the Pre-Personalization data includes writing of the Personalization Agent Key(s). 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.

The following TOE security objectives address the protection provided by the MRTD’s chip independent of the TOE environment.

9.1.5 OT.Prot_Abuse-Func (Protection against Abuse of Functionality)

After delivery of the TOE to the MRTD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to (i) disclose critical User Data, (ii) manipulate critical User Data of the IC Embedded Software, (iii) manipulate Soft-coded IC Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE. Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

9.1.6 OT.Prot_Inf_Leak (Protection against Information Leakage)

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

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

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.

9.1.7 OT.Prot_Phys-Tamper (Protection against Physical Tampering)

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

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or

- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data)

with a prior

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

9.1.8 OT.Prot_Malfunction (Protection against Malfunctions)

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

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.

9.1.9 OT.Active_Auth_MRTD_Proof (Proof of MRTD's chip authenticity by Active Authentication)

The TOE shall support the Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in 'ICAO Doc 9303' [ICAO_9303].

9.2 Security Objectives for the Operational Environment

9.2.1 Issuing State or Organization

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

9.2.1.1 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.

9.2.1.2 OE.MRTD_Delivery (Protection of the MRTD delivery)

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

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

- origin and shipment details,
- reception, reception acknowledgement,
- location material/information.

Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non-conformance to this process. Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.

9.2.1.3 OE.Personalization (Personalization of logical MRTD)

The issuing State or Organization must ensure that the Personalization Agents acting on behalf of the issuing State or Organization (i) establish the correct identity of the holder and create biographical data for the MRTD, (ii) enroll the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and (iii) personalize the MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

9.2.1.4 OE.Pass_Auth_Sign (Authentication of logical MRTD by Signature)

The issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity. The issuing State or Organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [ICAO_9303].

9.2.1.5 OE.BAC-Keys (Cryptographic quality of Basic Access Control Keys)

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the ‘ICAO 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.

9.2.1.6 OE.Active_Auth_Sign (Active Authentication of logical MRTD by Signature)

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

9.2.2 Receiving State or Organization

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

9.2.2.1 OE.Exam_MRTD (Examination of the physical MRTD)

The inspection system must examine the MRTD presented by the MRTD presenter to verify its authenticity by means of physical security measures and to detect any manipulation of the physical part of the MRTD. 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.

9.2.2.2 OE.Passive_Auth_Verif (Verification by Passive Authentication)

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

9.2.2.3 OE.Prot_Logical_MRTD (Protection of data from the logical MRTD)

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

9.2.2.4 OE.Active_Auth_Verif (Verification by Active Authentication)

The inspection systems to check the MRTD authenticity may use the active authentication verification, this is a stronger mechanism to guarantee the authenticity of the MRTD.

9.3 Security Objective Rationale

The following table provides an overview for security objectives coverage.

Table 6: Security Objectives Rationale

	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	OT.Active_Auth_MRTD	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.BAC-Keys	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD	OE.Active_Auth_Sign	OE.Active_Auth_Verif
T.Chip_ID				x										x					
T.Skimming			x											x					
T.Eavesdropping			x																
T.Forgery	x	x					x						x		x	x			
T.Abuse-Func					x							x							
T.Information_Leakage						x													
T.Phys-Tamper							x												
T.Malfunction								x											
P.Manufact				x															
P.Personalization	x			x								x							
P.Personal_Data		x	x																
P.Active_Auth									x									x	x
A.MRTD_Manufact										x									
A.MRTD_Delivery											x								
A.Pers_Agent												x							
A.Insp_Sys															x		x		
A.BAC-Keys														x					

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

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

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

transmission. The security objective **OT.Data_Confidentality** “Confidentiality of personal data” describes the protection of the confidentiality.

The OSP **P.Active_Auth “**Active Authentication” addresses the active authentication protocol as described in [ICAO_9303]. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to **OE.Active_Auth_Sign** “Active Authentication of logical MRTD by Signature” and verified by the inspection system according to **OE.Active_Auth_Verif** “Verification by Active Authentication”. This is possible only because genuine TOE enforce Active Authentication as specified in **OT.Active_Auth_Proof**.

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

The threat **T.Skimming** “Skimming digital MRZ data or the digital portrait” and **T.Eavesdropping “**Eavesdropping to the communication between TOE and inspection system” address the reading of the logical MRTD trough the contactless interface or listening the communication between the MRTD’s chip and a terminal. This threat is countered by the security objective **OT.Data_Conf** “Confidentiality of personal data” through Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys**

The threat **T.Forgery** “Forgery of data on MRTD’s chip” addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD“ requires the TOE to limit the write access for the logical MRTD to the trustworthy Personalization Agent (cf. OE.Personalization). The TOE will protect the integrity of the stored logical MRTD according 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”.

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

The threats **T.Information_Leakage** “Information Leakage from MRTD’s chip”, **T.Phys-Tamper** “Physical Tampering” and **T.Malfunction** “Malfunction due to Environmental Stress” are 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 objectives **OT.Prot_Inf_Leak** “Protection against Information Leakage”, **OT.Prot_Phys-Tamper** “Protection against Physical Tampering” and **OT.Prot_Malfunction** “Protection against Malfunctions”.

OT.Active_Auth_MRTD_Proof “Proof of MRTD’s chip authenticity by Active Authentication” using an authentication key pair to be generated by the issuing State or Organization. The

Public Active Authentication Key has to be written into EF.DG15 The TOE environment will also detect partly forged logical MRTD data by means of digital signature which will be created according to **OE.Active_Auth_Sign** “Active Authentication of logical MRTD by Signature” and verified by the inspection system according to **OE.Active_Auth_Verif** “Verification by Active Authentication”.

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

The assumption **A.MRTD_Delivery** “MRTD delivery during step 4 to 6” is covered by the security objective for the TOE environment **OE.MRTD_ Delivery** “Protection of the MRTD delivery” that requires to use security procedures during delivery steps of the MRTD.

The assumption **A.Pers_Agent** “Personalization of the MRTD’s chip” is covered by the security objective for the TOE environment **OE.Personalization** “Personalization of logical MRTD” including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data.

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

The assumption **A.BAC-Keys** “Cryptographic quality of Basic Access Control 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.

10 Extended components definition

This Security Target uses components defined as extensions in [CC_P2]. All these extended components are drawn from the Protection Profile MRTD with BAC [PP-0055]. The extended components FAU_SAS, FCS_RND, FMT_LIM and FPT_EMSEC are defined below.

10.1 Family FAU_SAS (Audit Data Storage)

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

The family FAU_SAS (Audit data storage) is specified as follows.

Family behavior	This family defines functional requirements for the storage of audit data.

Component leveling

FAU_SAS Audit Data Storage	1

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

FAU_SAS.1 Audit storage

Hierarchical to:	No other components.
Dependencies:	No dependencies.
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.

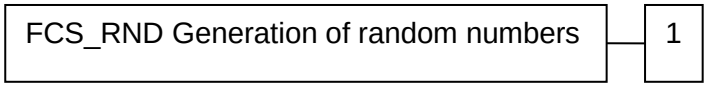
10.2 Family FCS_RND (Generation of random numbers)

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.

The family “Generation of random numbers (FCS_RND)” is specified as follows.

FCS_RND	Generation of random numbers
Family behavior:	This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

Component leveling:



FCS_RND.1	Generation of random numbers requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.
Management:	FCS_RND.1 There are no management activities foreseen.
Audit:	FCS_RND.1 There are no actions defined to be auditable.

10.2.1 FCS_RND.1 Quality metric for random numbers

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet [assignment*: a defined quality metric*].

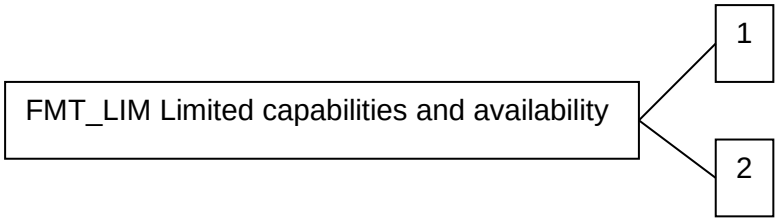
10.3 Family FMT_LIM (Limited capabilities and availability)

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.

The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

FMT_LIM	Limited capabilities and availability
Family behavior:	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.

Component leveling:



FMT_LIM.1	Limited capabilities require that the TSF is built to provide only the capabilities (perform action, gather information) which are 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:	FMT_LIM.1, FMT_LIM.2 There are no management activities foreseen.
Audit:	FMT_LIM.1, FMT_LIM.2 There are no actions defined to be auditable.

To define the IT security functional requirements of the TOE a sensitive family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family 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.

The TOE Functional Requirement "Limited capabilities (FMT_LIM.1)" is specified as follows.

10.3.1 FMT_LIM.1 (Limited capabilities)

Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability.
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*].

10.3.2 FMT_LIM.2 (Limited availability)

Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: *Limited capability and availability policy*].

Application Note: The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that

1. the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced,

or conversely,

2. the TSF is designed with test and support functionality that is removed from, or disabled in, the product prior to the Operational Use Phase.

The combination of both requirements shall enforce the policy.

10.4 Family FPT_EMSEC (TOE Emanation)

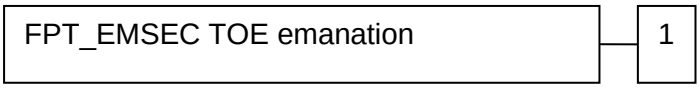
The sensitive family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena 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_P2].

The family "TOE Emanation (FPT_EMSEC)" is specified as follows.

FMT_LEMSEC TOE Emanation

Family behavior: This family defines requirements to mitigate intelligible emanations.

Component leveling:



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: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

10.4.1 FPT_EMSEC.1 (TOE Emanation)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMSEC.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_EMSEC.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].

11 Security requirements

This section of the ST defines the detailed security requirements that shall be satisfied by the TOE. The statement of **TOE security requirements** shall define the *functional* and *assurance* security requirements that the TOE needs to satisfy to meet the security objectives for the TOE.

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and iteration are defined in section 8.1 of Part 1 of the Common Criteria [CC_P1]. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and removed are ~~crossed out~~.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted as underlined text. Selections made by the ST author appear *slanted and underlined*.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as underlined text. Assignments made by the ST author appear *slanted and underlined*.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

This part defines the detailed security requirements that are satisfied by the TOE. These requirements comprise functional components from [CC_P2], Extended components as defined in Chapter 10, and the assurance components as defined for the Evaluation Assurance Level EAL 4 from [CC_P3] augmented by ALC_DVS.2

The definition of the subjects "Manufacturer", "Personalization Agent", "Basic Inspection System" and "Terminal" used in the following chapter is given in section 8. Note, that all these subjects are acting for homonymous external entities. The operations "write", "read", "modify", and "disable read access" are used in accordance with the general linguistic usage. The operations "transmit", "receive" and "authenticate" are originally taken from [CC_P2].

Security attributes

The following table defines the security attributes of this ST.

Table 7: Security attributes

Security attribute	Values	Meaning
Terminal authentication status	None (any terminal)	Default role (i.e. without authorization after start-up)
	Personalization Agent	Terminal is authenticated as Personalization Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2
	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

11.1 Security Functional Requirements (SFRs)

The following table summarizes all TOE security functional requirements of this ST. They are described in the following sections.

Table 8: SFR Overview

Class FAU: Security Audit	
FAU_SAS.1	Audit Storage
Class FCS: Cryptographic Support	
FCS_CKM.1	Cryptographic key generation - Generation of Document Basic Access Keys by the TOE
FCS_CKM.4	Cryptographic key destruction - MRTD
FCS_COP.1/SHA	Cryptographic operation - Hash for Key Derivation
FCS_COP.1/ENC	Cryptographic operation – Encryption / Decryption Triple DES
FCS_COP.1/AUTH	Cryptographic operation – Authentication
FCS_COP.1/MAC	Cryptographic operation – Retail MAC
FCS_COP.1/AA	Cryptographic operation – Active Authentication
FCS_RND.1	Random number generation
Class FIA: Identification and Authentication	
FIA_UID.1	Timing of identification
FIA_UAU.1	Timing of authentication
FIA_UAU.4	Single-use authentication mechanism – Single-use authentication of the Terminal by the TOE
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.6	Re-authenticating of Terminal by the TOE
FIA_AFL.1	Authentication failure handling
Class FDP: User Data Protection	
FDP_ACC.1	Subset access control – Basic Access Control
FDP_ACF.1	Basic Security attribute based access control - Basic Access Control
FDP_UCT.1	Basic data exchange confidentiality - MRTD
FDP_UIT.1	Data exchange integrity - MRTD
Class FMT: Security Management	
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FMT_MTD.1/INI_ENA	Management of TSF data – Writing of initialization data and personalization data
FMT_MTD.1/INI_DIS	Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data
FMT_MTD.1/KEY_WRITE	Management of TSF data – Key Write
FMT_MTD.1/KEY_READ	Management of TSF data – Key Read
Class FPT: Protection of the TSF	
FPT_EMSEC.1	TOE emanation
FPT_FLS.1	Failure with preservation of secure state
FPT_TST.1	TSF testing
FPT_PHP.3	Resistance to physical attack

11.2 SFRs: Class FAU (Security Audit)

11.2.1 Family FAU_SAS (Audit Data Storage)

The TOE shall meet the following requirements for the storage of audit data.

11.2.1.1 FAU_SAS.1 (Audit storage)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide the Manufacturer[2] with the capability to store the Identification and Pre-Personalization Data[3] in the audit records.

Application note: The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_ENA in sec. 11.6.4.1 and FMT_MTD.1/INI_DIS in sec. 11.6.4.2).

11.3 SFRs: Class FCS (Cryptographic Support)

11.3.1 Family FCS_CKM (Cryptographic key generation)

The TOE shall meet the following requirements for the generation of cryptographic keys. The iterations are caused by different cryptographic key generation algorithms to be implemented and key to be generated by the TOE.

11.3.1.1 FCS_CKM.1 (Generation of Document Basic Access Keys by the TOE)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
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[4] and specified cryptographic key sizes 112 bit[5] that meet the following: [ICAO 9303], normative appendix 5[6].

Application note: The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [ICAO_9303], normative appendix A5.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure

2 [assignment: *authorized users*]
3 [assignment: *list of audit information*]
4 [assignment: *cryptographic key generation algorithm*]
5 [assignment: *cryptographic key sizes*]
6 [assignment: *list of standards*]

messaging by the algorithm in [ICAO_9303], Normative appendix A5.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.

11.3.1.2 FCS_CKM.4 (Cryptographic key destruction – MRTD)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *physical deletion by overwriting the memory data with zeros*[7] that meets the following: *none*[8].

Application Note: The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging.

11.3.2 Family FCS_COP (Cryptographic operation)

The TOE shall meet the following requirements for the cryptographic operations. The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

11.3.2.1 FCS_COP.1/SHA (Cryptographic operation – Hash for Key Derivation)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/SHA	The TSF shall perform hashing[9] in accordance with a specified cryptographic algorithm: *SHA-1, SHA-224, SHA-256, SHA-384, SHA-512*[10] and cryptographic key sizes none[11] that meet the following: *[FIPS_180-2]*[12].

Application Note: This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive of the Basic Access Control Authentication Mechanism (see also FIA_UAU.4) according to [ICAO_9303].

11.3.2.2 FCS_COP.1/ENC (Cryptographic operation – Encryption / Decryption Triple DES)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.

[7] [assignment: *list of cryptographic operations*]
[8] [assignment: *list of standards*]
[9] [assignment: *list of cryptographic operations*]
[10] [assignment: *cryptographic algorithm*]
[11] [assignment: *cryptographic key sizes*]
[12] [assignment: *list of* standards]

Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ENC	The TSF shall perform secure messaging (BAC) – encryption and decryption[13] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[14] and cryptographic key sizes 112 bit[15] that meet the following: [SP800-67] and [ICAO_9303] normative appendix 5, A5.3[16].

Application note: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

11.3.2.3 FCS_COP.1/AUTH (Cryptographic operation – Authentication)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AUTH	The TSF shall perform symmetric authentication – encryption and decryption[17] in accordance with a specified cryptographic algorithm *AES*[18] and cryptographic key sizes: *128 bits*[19] that meet the following: *[FIPS_PUB_197]*[20].

Application note: This SFR requires the TOE to implement the cryptographic primitive for authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism (cf. FIA_UAU.4).

11.3.2.4 FCS_COP.1/MAC (Cryptographic operation – Retail MAC)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

[13] [assignment: *list of cryptographic operations*]
[14] [assignment: *cryptographic algorithm*]
[15] [assignment: *cryptographic key sizes*]
[16] [assignment: *list of* standards]
[17] [assignment: *list of cryptographic operations*]
[18] [assignment: *cryptographic algorithm*]
[19] [assignment: *cryptographic key sizes*]
[20] [assignment: *list of standards*]

FCS_COP.1.1/MAC The TSF shall perform secure messaging – message authentication code[21] in accordance with a specified cryptographic algorithm Retail MAC[22] and cryptographic key sizes 112 bit[23] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)[24].

Application note: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

11.3.2.5 FCS_COP.1/AA (Cryptographic operation – Active Authentication)

Defined in: This ST

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FMT_MTD.1/KEY_WRITE

Justification: The Active Authentication cryptographic key is only imported in the TOE, therefore FCS_CKM.1 makes no sense in this case. The key is imported by the personalization agent according to the SFR FMT_MTD.1/KEY_WRITE

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/AA The TSF shall perform Table 9 column 1[25] in accordance with a specified cryptographic algorithm Table 9 column 2[26] and cryptographic key sizes Table 9 column 3[27] that meet the following standards Table 9 column 4[28].

Table 9: Cryptographic algorithms and keys of SFR "FCS_COP.1/AA"

List of cryptographic operations	Cryptographic algorithm	Cryptographic key sizes in bits	List of standards
Digital signature creation	RSA CRT	1024, 2048, 3072, 4096	[ISO_9796-2]
Digital signature creation	ECDSA	192, 224, 256, 320, 384, 512, 521	[TR-03111]

11.3.3 Family FCS_RND (Generation of random numbers)

The TOE shall meet the following requirements for the generation of random numbers.

11.3.3.1 FCS_RND.1 (Quality metric for random numbers)

Defined in: Protection Profile MRTD with BAC [PP-0055]

[21] [assignment: *list of cryptographic operations*]
[22] [assignment: *cryptographic algorithm*]
[23] [assignment: *cryptographic key sizes*]
[24] [assignment: *list of* standards]
[25] [assignment: *list of cryptographic operations*]
[26] [assignment: *cryptographic algorithm*]
[27] [assignment: *cryptographic key sizes*]
[28] [assignment: *list of standards*]

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet *DRG.3 capabilities defined in [AIS31/20] standard*[29].

Application note: The TOE implements a deterministic random number generator. When initialized with a random seed using a PTRNG of class PTG.2 as random source, the internal state of the RNG has at least 100 bits of min-entropy. The TOE's RNG is initialized with a random seed at each TOE startup/reset/power-up. It generates output, for which 2^{34} strings of bit length 128 are mutually different with probability greater than $1-2^{-16}$. The TOE's RNG provides forward secrecy. It provides backward secrecy even if the current internal state is known. Statistical test suites cannot practically distinguish the TOE's RNG sequences from output sequences of an ideal RNG. The TOE's RNG pass test procedure A and the NIST statistical test suite [SP800-22].

Application note: This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

11.4 SFRs: Class FIA (Identification and Authentication)

Class defined in Common Criteria Par 2 [CC_P2].

The unambiguous identification of authorised users and the correct association of security attributes with users and subjects is critical to the enforcement of the intended security policies.

Other classes of requirements (e.g. User Data Protection, Security Audit) are dependent upon correct identification and authentication of users in order to be effective.

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

Table 10: Overview on the authentication mechanisms

Name	SFR for the TOE	Algorithms and key sizes according to [ICAO_9303], normative appendix 5, and [TR-03110-1]
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	AES with 128-bit keys (cf. FCS_COP.1/AUTH)
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)

11.4.1 Family FIA_UID (User identification)

The TOE shall meet the following requirements for the identification of the user.

11.4.1.1 FIA_UID.1 (Timing of identification)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	No dependencies.

[29] [assignment: *a defined quality metric*]

FIA_UID.1.1 The TSF shall allow

1. to read the Initialization Data in Phase 2 “Manufacturing”,
2. to read the random identifier in Phase 3 “Personalization of the MRTD”,
3. to read the random identifier in Phase 4 “Operational Use”[30] 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.

Application note: The IC manufacturer and the MRTD manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the Phase 2 “TOE Manufacturing”. The audit records can be written only in the Phase 2 Manufacturing of the TOE. At this time the Manufacturer is the only user role available for the TOE. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 “Personalization of the MRTD”. The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. The Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System.

Application note: In the “TOE Operational Use” phase the MRTD must not allow anybody to read the ICCSN, the MRTD identifier or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note that the terminal and the MRTD’s chip use a (randomly chosen) identifier for the communication channel to allow the terminal to communicate with more than one RFID. If this identifier is randomly selected it will not violate the OT.Identification. If this identifier is fixed the ST writer should consider the possibility to misuse this identifier to perform attacks addressed by T.Chip_ID.

11.4.2 Family FIA_UAU (User authentication)

11.4.2.1 FIA_UAU.1 (Timing of authentication)

Defined in: Protection Profile MRTD with BAC [PP-0055]

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1 The TSF shall allow

1. to read the Initialization Data in Phase 2 “Manufacturing”,
2. to read the random identifier in Phase 3 “Personalization of the MRTD”,
3. to read the random identifier in Phase 4 “Operational Use”[31]

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.

Application note: The Basic Inspection System and the Personalization Agent authenticate themselves.

[30] [assignment: *list of TSF-mediated actions*]
[31] [assignment: *list of TSF-mediated actions*]

11.4.2.2 FIA_UAU.4 (Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE)

Defined in: Protection Profile MRTD with BAC [PP-0055]

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. Basic Access Control Authentication Mechanism,
2. Authentication Mechanism based on *AES*[32].

Application note: The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalisation Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

Application note: The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [ICAO_9303]. In the first step the terminal authenticates itself to the MRTD's chip and the MRTD's chip authenticates to the terminal in the second step. In this second step the MRTD's chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD's chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore, the TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfill the security objective OT.Identification and to prevent T.Chip_ID.

11.4.2.3 FIA_UAU.5 (Multiple authentication mechanisms)

Defined in: Protection Profile MRTD with BAC [PP-0055]

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

1. Basic Access Control Authentication Mechanism
2. Symmetric Authentication Mechanism based on *AES*[33]

to support user authentication.

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

1. 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*[34],
2. 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[35].

Application note: The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The

[32] [assignment: *identified authentication mechanism(*s)]
[33] [assignment: *list of multiple authentication mechanisms*]
[34] [selection*: the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key, [assignment other]*]
[35] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System may use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

11.4.2.4 FIA_UAU.6 (Re-authenticating – Re-authenticating of Terminal by the TOE)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	No dependencies.
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[36].

Application note: The Basic Access Control Mechanism specified in [ICAO_9303] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user.

Application note: Note that in case the TOE should also fulfill the Protection Profile MRTD EAC with PACE [PP-0056], the BAC communication might be followed by a Chip Authentication mechanism establishing a new secure messaging that is distinct from the BAC based communication. In this case the condition in FIA_UAU.6 above should not contradict to the option that commands are sent to the TOE that are no longer meeting the BAC communication but are protected by a more secure communication channel established after a more advanced authentication process.

11.4.3 Family FIA_AFL (Authentication failures)

The TOE shall meet the following requirements for authentication failures.

11.4.3.1 FIA_AFL.1 (Authentication failure handling)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when a positive integer equal to 1 [37] of unsuccessful authentication attempts occur related to the Personalization Agent authentication and the Basic Inspection System authentication[38].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met[39], the TSF shall wait for an administrator configurable time

[36] [assignment: *list of conditions under which re-authentication is required*]
[37] [assignment: *range of acceptable value*]
[38] [assignment: *list of authentication event*]
[39] [assignment: *met or surpassed*]

between the receiving the terminal challenge and sending the TSF response during the BAC authentication attempts[40].

Application note: In this ST the open operations in the SFR FIA_AFL.1.1 and FIA_AFL.1.2 have been assigned to ensure the strength of authentication function as terminal part of the Basic Access Control Authentication Protocol to resist enhanced basic attack potential.

11.5 SFRs: Class FDP (User Data Protection)

11.5.1 Family FDP_ACC (Access control policy)

The TOE shall meet the following requirements for the access control policy.

11.5.1.1 FDP_ACC.1 (Subset access control – Basic Access control)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the Basic Access Control SFP[41] 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[42].

11.5.2 Family FDP_ACF (Access control functions)

The TOE shall meet the following requirements for the access control functions.

11.5.2.1 FDP_ACF.1 (Basic Security attribute based access control – Basic Access Control)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1	The TSF shall enforce the Basic Access Control SFP[43] to objects based on the following:

1. Subjects:
   a. Personalization Agent,
   b. Basic Inspection System,
   c. Terminal,
2. Objects:
   a. data EF.DG1 to EF.DG16 of the logical MRTD,
   b. data in EF.COM,
   c. data in EF.SOD,
3. Security attributes
   a. authentication status of terminals[44].

[40] [assignment: *list of actions*]
[41] [assignment: *access control SFP*]
[42] [assignment: *list of subjects*, *objects, and operations among subjects and objects covered by the SFP*]
[43] [assignment: *access control SFP*]
[44] [assignment: *list of subjects and objects controlled under the indicated SFP, and. for each, the SFP relevant security attributes*, *or named groups of SFP-relevant security attributes*]

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

1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,
2. 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[45].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[46].

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

1. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.
2. Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD.
3. The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4[47].

Application note: The inspection system needs special authentication and authorization for read access to EF.DG3 and EF.DG4 are not defined in this ST.

11.5.3 Family FDP_UCT (Inter-TSF user data confidentiality transfer protection)

The TOE shall meet the following requirements for the Inter-TSF user data confidentiality transfer protection.

11.5.3.1 FDP_UCT.1 (Basic data exchange confidentiality - MRTD)

Defined in: Protection Profile MRTD with BAC [PP-0055]

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1 The TSF shall enforce the Basic Access Control SFP[48] to be able to transmit and receive[49] user data in a manner protected from unauthorized disclosure.

11.5.4 Family FDP_UIT (Inter-TSF user data integrity transfer protection)

The TOE shall meet the following requirements for the Inter-TSF user data integrity transfer protection.

[45] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[46] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
[47] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[48] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[49] [selection: *transmit, receive*]

11.5.4.1 FDP_UIT.1 (Data exchange integrity - MRTD)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
FDP_UIT.1.1	The TSF shall enforce the Basic Access Control SFP[50] to be able to transmit and receive[51] user data in a manner protected from modification, deletion, insertion and replay[52] errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[53] has occurred.

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.

11.6 SFRs: Class FMT (Security Management)

Application note: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

11.6.1 Family FMT_SMF (Specification of Management Functions)

The TOE shall meet the following requirements for the management functions.

Management functions provide TSFI that allow administrators to define the parameters that control the operation of security related aspects of the TOE, such as data protection attributes, TOE protection attributes, audit attributes, and identification and authentication attributes. Management functions also include those functions performed by an operator to ensure continued operation of the TOE, such as backup and recovery.

11.6.1.1 FMT_SMF.1 (Specification of Management Functions)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	No Dependencies
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: 1. Initialization, 2. Pre-personalization, 3. Personalization54.

[50] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[51] [selection: *transmit, receive*]
[52] [selection: *modification, deletion, insertion, replay*]
[53] [selection: *modification, deletion, insertion, replay*]
[54] [assignment: *list of management functions to be provided by the TSF*]

11.6.2 Family FMT_SMR (Security management roles)

The TOE shall meet the following requirements for controlling the assignment of different roles to users.

11.6.2.1 FMT_SMR.1 (Security roles)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FMT_SMR.1.1	The TSF shall maintain the roles 1. Manufacturer, 2. Personalization Agent, 3. Basic Inspection System55.
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Application note: The following SFRs 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.

11.6.3 Family FMT_LIM (Limited capabilities and availability)

The TOE shall meet the following requirements for the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

11.6.3.1 FMT_LIM.1 (Limited capabilities)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability.
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 1. User Data to be disclosed or manipulated 2. TSF data to be disclosed or manipulated 3. software to be reconstructed and 4. substantial information about construction of TSF to be gathered which may enable other attacks

11.6.3.2 FMT_LIM.2 (Limited availability)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities.

[55] [assignment: *the authorized identified roles*]

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

Application note: The formulation of "Deploying Test Features …" in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless, the combination of FMT_LIM.1 and FMT_LIM.2 is introduced provide an optional approach to enforce the same policy. Note that the term "software" in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

Application note: The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

11.6.4 Family FMT_MTD (Management of TSF data)

The TOE shall meet the following requirements for the management of TSF data. The iterations address different management functions and different TSF data.

11.6.4.1 FMT_MTD.1/INI_ENA (Management of TSF data – Writing of Initialization Data and Pre-personalization Data)

Defined in: Protection Profile MRTD with BAC [PP-0055]

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to write[56] the Initialization Data and Pre-personalization Data[57] to the TOE Manufacturer[58].

Application note: The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Key.

11.6.4.2 FMT_MTD.1/INI_DIS (Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data)

Defined in: Protection Profile MRTD with BAC [PP-0055]

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

[56] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]
[57] [assignment: *list of TSF data*]
[58] [assignment: *the authorized identified roles*]

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to disable read access for users to[59] the Initialization Data[60] to the Personalization Agent[61].

Application note: According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 “TOE Manufacturing” but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Prepersonalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 “personalization” but is not needed and may be misused in the Phase 4 “Operational Use”. Therefore, the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

11.6.4.3 FMT_MTD.1/KEY_WRITE (Management of TSF data – Key Write)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles

FMT_MTD.1.1/ KEY_WRITE The TSF shall restrict the ability to write[62] the Document Basic Access Keys *and the Active Authentication key*[63] to the Personalization Agent[64].

Application note: This ST includes the Active Authentication Private Key to the list of TSF data defined in Protection Profile MRTD with BAC [PP-0055].

Application note: The verb “write” means here that the Active Authentication Private Key is generated securely outside the TOE and written into the TOE memory.

11.6.4.4 FMT_MTD.1/KEY_READ (Management of TSF data – Key Read)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to read[65] the Document Basic Access Keys the Personalization Agent Keys *and the Active Authentication key*[66] to none[67].

Application note: The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.

[59] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]
[60] [assignment: *list of TSF data*]
[61] [assignment: *the authorized identified roles*]
[62] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]
[63] [assignment: *list of TSF data*]
[64] [assignment: *the authorized identified roles*]
[65] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]
[66] [assignment: *list of TSF data*]
[67] [assignment: *the authorized identified roles*]

11.7 SFRs: Class FPT (Protection of the TSF)

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.

11.7.1 Family FPT_EMSEC (TOE Emanation)

The TOE shall meet the following requirements to mitigate intelligible emanations.

11.7.1.1 FPT_EMSEC.1 (TOE Emanation)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	No Dependencies.
FPT_EMSEC.1.1	The TOE shall not emit *power variations, timing variations*[68] **during command execution** in excess of *non-useful information*[69] enabling access to Personalization Agent Key(s)[70] and *the Document Basic Access Keys and the Active Authentication key.*[71]
FPT_EMSEC.1.2	The TSF shall ensure any unauthorized users[72] are unable to use the following interface smart card circuit contacts **and contactless**[73] to gain access to Personalization Agent Key(s)[74] and *the Document Basic Access Keys and the Active Authentication key*[75].

Application note: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The MRTD’s chip has to provide a smart card contactless interface but may have also (not used by the terminal but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

The following security functional requirements address the protection against forced illicit information leakage including physical manipulation.

[68] [assignment: *types of emissions*]
[69] [assignment: *specified limits*]
[70] [assignment: *list of types of TSF data*]
[71] [assignment: *list of types of user data*]
[72] [assignment: *type of users*]
[73] [assignment: *type of connection*]
[74] [assignment: *list of types of TSF data*]
[75] [assignment: *list of types of user data*]

11.7.2 Family FPT_FLS (Fail secure)

The TOE shall meet the following requirements for ensuring that the TOE will always enforce its SFRs in the event of identified categories of failures in the TSF.

11.7.2.1 FPT_FLS.1 (Failure with preservation of secure state)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	No Dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1. Exposure to out-of-range operating conditions where therefore a malfunction could occur, 2. failure detected by TSF according to FPT_TST.1[76].

11.7.3 Family FPT_TST (TSF self test)

The TOE shall meet the following requirements for the self-testing of the TSF.

11.7.3.1 FPT_TST.1 (TSF testing)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	No Dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests *during initial start-up and before calling a security sensitive module*[77] to demonstrate the correct operation of the TSF[78].
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data[79].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

11.7.4 Family FPT_PHP (TSF physical protection)

The TOE shall meet the following requirements for protection from physical tampering and interference.

11.7.4.1 FPT_PHP.3 (Resistance to physical attack)

Defined in:	Protection Profile MRTD with BAC [PP-0055]
Hierarchical to:	No other components.
Dependencies:	No dependencies.

[76] [assignment: *list of types of failures in the TSF*]
[77] [selection: *during initial start-up*], [*assignment: conditions under which self test should occur*]
[78] [selection: *[assignment: parts of TSF], the TSF*]
[79] [selection: *[assignment: parts of TSF], TSF data*]

FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing[80] to the TSF[81] by responding automatically such that the SFRs are always enforced.

Application note: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, “automatic response” means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

11.8 Security Assurance Requirements (SARs)

The assurance requirements for the evaluation of the TOE, its development and operating environment are those taken from Evaluation Assurance Level 4 [CC_P3] augmented with the following component (EAL4+):

- ALC_DVS.2 (Sufficiency of security measures)

The following table lists the security assurance requirements of the TOE.

Table 11: Security Assurance Requirements - EAL4+

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures (augmentation)
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition

[80] [assignment: *physical tampering scenarios*]
[81] [assignment: *list of TSF devices/elements*]

	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

11.9 Security Requirements Rationale

11.9.1 Security Functional Requirements (SFRs) Rationale

The following table provides an overview for security functional requirements coverage.

Table 12: Coverage of Security Objectives for the TOE by SFR

Security Objectives / SFR	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func	OT.Active_Auth_MRTD_Proof
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_COP.1/AA									x
FCS_RND.1	x	x	x						
FIA_UID.1			x	x					
FIA_AFL.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						
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						x

SFR \ Security Objectives	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func	OT.Active_Auth_MRTD_Proof
FMT_MTD.1/KEY_READ	x	x	x						x
FPT_EMSEC.1	x				x				
FPT_FLS.1	x				x		x		
FPT_TST.1					x		x		
FPT_PHP.3	x				x	x			

11.9.2 Rationale for the Fulfilment of the Security Objectives for the TOE

In the following, a detailed justification as required to show the suitability and sufficiency of the security functional requirements to achieve the security objectives defined for the TOE is given.

11.9.2.1 OT.AC_Pers

The security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD” addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR FDP_ACC.1 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 Protection Profile MRTD EAC with PACE [PP-0056] 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_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

11.9.2.2 OT.Data_Int

The security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to protect the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the 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** "Integrity of personal data" requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data by means of the BAC mechanism. The SFR FIA_UAU.6, 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 with FMT_MTD.1/KEY_READ.

11.9.2.3 OT.Data_Confidentiality

The security objective **OT.Data_Confidentiality** "Confidentiality of personal data" requires the TOE to ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Confidentiality. In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The read access to the logical MRTD data is defined by the FDP_ACC.1 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 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 andFCS_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_Confidentiality nor the SFR FIA_UAU.5 requires the Personalization Agent to use the Basic Access Control Authentication Mechanism or secure messaging.

11.9.2.4 OT.Identification

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

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

11.9.2.5 OT.Prot_Abuse-Func

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

11.9.2.6 OT.Prot_Inf_Leak

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

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines, which is addressed by the SFR FPT_EMSEC.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.

11.9.2.7 OT.Prot_Phys-Tamper

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

11.9.2.8 OT.Prot_Malfunction

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

11.9.2.9 OT.Active_Auth_MRTD_Proof

The security objective **OT.Active_Auth_MRTD_Proof** “Proof of MRTD’s chip authenticity by Active Authentication” “is covered by the SFRs FCS_COP.1.1/AA_RSA, FCS_COP.1.1/AA_ECDSA, FMT_MTD.1/KEY_WRITE and FMT_MTD.1/KEY_READ.

11.9.3 SFR Dependency Rationale

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and

non-dissolved dependencies are appropriately explained. The table below shows the dependencies between the SFR of the TOE

Table 13: Dependencies between the SFRs

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]	Fulfilled by FCS_COP.1/ENC and FCS_COP.1/MAC
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by FCS_CKM.1
FCS_COP.1/SHA	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Justification 1 for non-satisfied dependencies
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by FCS_CKM.1
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/AUTH	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Justification 2 for non-satisfied dependencies
	FCS_CKM.4 Cryptographic key destruction	Justification 2 for non-satisfied dependencies
FCS_COP.1/MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by FCS_CKM.1
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4

SFR	Dependencies	Support of the Dependencies
FCS_COP.1/AA	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Justification 2 for non-satisfied dependencies
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	n.a.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a.
FIA_UAU.6	No dependencies	n.a.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control	Fulfilled by FDP_ACC.1
	FMT_MSA.3 Static attribute initialization	Justification 3 for non-satisfied dependencies
FDP_UCT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	Justification 4 for non-satisfied dependencies
	[FDP_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	Fulfilled by FDP_ACC.1
FDP_UIT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	Justification 4 for non-satisfied dependencies
	[FDP_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	Fulfilled by FDP_ACC.1
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FMT_LIM.1	FMT_LIM.2	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	Fulfilled by FMT_LIM.1
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions	Fulfilled by FMT_SMF.1

SFR	Dependencies	Support of the Dependencies
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FPT_EMSEC.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.

Justification for non-satisfied dependencies between the SFR for TOE:

No. 1: The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore, neither BAC key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.

No. 2: The SFR FCS_COP.1/AUTH and FCS_COP.1/AA uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT_MTD.1/INI_ENA) by the manufacturer. Thus, there is no need to generate or import a key during the addressed TOE lifecycle by 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.

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

No. 4: The SFR FDP_UCT.1 and FDP_UIT.1 require 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.

11.9.4 Security Assurance Requirements Rationale

The EAL 4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, through rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL 4 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.

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

The component ALC_DVS.2 augmented to EAL 4 has no dependencies to other security requirements.

The component ALC_DVS.2 has no dependencies.

11.9.5 Security Requirements – Mutual Support and Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form a mutually supportive and internally consistent whole.

The analysis of the TOE´s security requirements with regard to their mutual support and internal consistency demonstrates:

The dependency analysis in section 11.9.3 SFR Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-satisfied dependencies are appropriately explained.

The assurance class EAL 4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 11.9.4 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in sections 11.9.3 SFR Dependency Rationale and 11.9.4 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 11.9.4 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So, the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

12 TOE Security Functions (TSFs)

The TOE provides the following TOE security functionality, which comply to the Protection Profile MRTD with BAC [PP-0055]:

- Personalization Agent Authentication
- BAC
- Active Authentication
- Secure Messaging
- Access Control
- Cryptographic Support
- Data Protection

These Security Functions are implemented by the realisation of the Security Functional requirements, according to chap. 11. The details of the implementation of this TOE security functionality are provided in the following sections.

12.1 SF_AUTH – Personalization Agent Authentication

The TOE implements security mechanisms to authenticate external entities and assign roles and rights.

The authentication mechanism is based on challenge-response protocol according to [ICAO_9303] using the AES algorithm and key length of 128 bits, as selected for the SFRs FCS_COP.1/AUTH and FCS_RND.1.

The purpose of the TSF SF_AUTH is to authenticate the roles of “Personalization Agent” when the TOE is in the life cycle phase 3 “TOE Personalization” (FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FMT_SMF.1, FMT_SMR.1). After a successful authentication, the “Personalization Agent” takes control of the TOE, executes the steps and operations as described in the life cycle Phase 3 “TOE Personalization”, and initiates the Logical Data Structure (LDS).

The Personalization Agent Authentication Key(s) are pre-loaded in the TOE at the end of phase 2 “TOE Manufacturing”. After a successful authentication the “Personalization Agent” takes control of the TOE, executes the steps and operations as described in the life cycle phase 3 “TOE Personalization”, and initiates the Logical Data Structure (LDS) (FDP_ACC.1, FDP_ACF.1).

The Personalization Agent Authentication algorithm is detailed in the Preparative User Guidance of this TOE [AGD_PRE].

12.2 SF_BAC – Basic Access Control Authentication

The TOE implements the Basic Access Control (BAC) mechanism to protect the Logical Data Structure (LDS) according to SFRs FDP_ACC.1 and FDP_ACF.1.

The TOE implements the Basic Access Control (BAC) mechanism to establish secure messaging key to protect data during communication with Basic Inspection system (BIS) (FMT_SMR.1). The TOE implements the BAC according to [ICAO_9303]. The Basic Inspection System uses the Basic Access Control with the Document Basic Access Keys.

The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [ICAO_9303] and includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in

MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6)

The authentication mechanisms as part of BAC Mechanism include the key agreement (FCS_CKM.1) for the encryption (FCS_COP.1/ENC) and the message authentication (FCS_COP.1/MAC) key to be used for secure messaging (FDP_UCT.1, FDP_UIT.1)

After the user is authenticated as Basic Inspection System, the TOE allows the user to read the ICCSN, the MRTD identifier or any other unique identification (FIA_UID.1).

The TSF SF_BAC destroys the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging whenever they are no more needed (FCS_CKM.4).

The TSF SF_BAC detects when an unsuccessful authentication attempt occurs. In case of failed authentication attempts, the TSF enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack (FIA_AFL.1).

12.3 SF_AA – Active Authentication

The TOE implements the Active Authentication (AA) mechanism to proof the travel document chip authenticity according to [ICAO_9303].

The Active Authentication cryptographic algorithm, key length and standards are defined by SFR FCS_COP.1/AA.

The RSA algorithm is supported with RSA CRT key long 1024, 2048, 3072, and 4096 bits. The ECDSA algorithm is supported with EC key long 192, 224, 256, 320, 384, 512, and 521 bits. For both the algorithms, the following hashing algorithms are supported: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512.

The Active Authentication cryptographic key is imported in the TOE by the personalization agent according to the SFR FMT_MTD.1/KEY_WRITE

12.4 SF_SM – Secure Messaging

The TOE implements a trusted channel providing confidentiality and integrity of transferred data according to the FDP_UCT.1 and FDP_UIT.1 requirements. The trusted channel is using TripleDES cipher for encryption in CBC mode as selected and defined in the SFR FCS_COP.1/ENC and message authentication code generation in Retail-MAC mode as selected and defined in the SFR FCS_COP.1/MAC. The SFR SF_SM uses new fresh random (FCS_RND.1) at each set up of the trusted channel between TOE and Basic Inspection System (BIS).

12.5 SF_AC – Access Control

The TOE operates in accordance with the access policies according to FDP_ACC.1, FDP_ACF.1 and considers the management functions and user roles as defined in FMT_SMF.1 and FMT_SMR.1 respectively.

This TSF checks that for each operation initiated by a subject on data (EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical travel document) and keys (Personalization agent key, Document Basic Access Keys), the security attributes for that roles authorization are satisfied. The function covers the management, writing, update and read of stored keys and data as defined in FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_MTD.1/KEY_WRITE and FMT_MTD.1/KEY_READ.

The TSF SF_AC access control allows the user in the role “TOE Manufacturer” during the Phase 2 “TOE Manufacturing” to write the “Initialization Data”, which includes but are not limited to the “IC Identification data” as required by FAU_SAS.1, to write these data only once.

12.6 SF_CRY – Cryptographic Support

This Security Function is responsible for providing cryptographic support to all the other Security Functions including secure key generation and operations on data such as encrypt, decryption and MAC generation and random number generation:

- The TSF provides the secure generation of symmetric Key for secure messaging (FCS_CKM.1). The TSF produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [ICAO_9303], Normative appendix A5.1. The algorithm uses the random number generated by TSF as required by FCS_RND.1
- The TSF provides high quality Random Number Generator (FCS_RND.1) compliant with the [AIS31/20]. This generator is a deterministic RNG of level DRG.3 according to supporting enhanced backward and forward secrecy
- The TSF provides Hashing Cryptographic operation for key derivation (FCS_COP.1/SHA)
- The TSF provides TripleDES cipher for encryption/decryption in CBC mode and 112-bits cryptographic key (FCS_COP.1/ENC)
- The TSF provides AES cipher for encryption/decryption in CBC mode and 128-bits cryptographic key (FCS_COP.1/AUTH)
- The TSF provides message authentication based on Retail-MAC and 112-bits cryptographic key (FCS_COP.1/MAC)
- Secure destruction of cryptographic key secret or private material (FCS_CKM.4)

This TSF enforces protection of Key material during cryptographic functions processing and Key Generation, against state-of-the-art attacks, including IC power consumption analysis (FPT_EMSEC.1).

12.7 SF_PRO – Data Protection

This Security Function is responsible for protection of the TSF data, user data, and TSF functionality. The TSF SF_RPO Data Protection is composed of software implementations of test and security functions including:

- Performing self-tests of the TOE at each power-up including a set of tests to verify that the underlying cryptographic algorithms are operating correctly (FPT_TST.1)
- Initializing memory after reset
- Initializing memory of de-allocated data and secure destruction of cryptographic key, secrets and private material (FCS_CKM.4, FDP_RIP.1)
- Preserving the TOE lifecycle state integrity to ensure that the testing/debugging features used during development remain irreversibly deactivated for deployment in order to ensure User and TSF Data confidentiality (FMT_LIM.1, FMT_LIM.2).
- Protecting the integrity of all stored cryptographic keys before use and preventing use of corrupted data by stopping the operation involved and setting an error (FCS_CKM.4, FDP_RIP.1)
- Preventing electromagnetic and power emissions or associated information like timing behaviour, in order to preserve the confidentiality of stored keys or residual key material information (FPT_EMSEC.1)
- Preserving secure state after sensitive processing failure (RNG, power loss, memory or functional failure) or potential physical tampering or intrusion detection (FPT_FLS.1, FPT_PHP.3)

This TSF prevents re-activation of de-activated or disabled or terminated mechanisms: the code area and data area are protected (FMT_LIM.1, FMT_LIM.2).

12.8 SF_OSPlat – Java Platform and OS

This TSF is implemented at SW layer JCS and OS Kernel. Here the TSF is described as a single and cumulative security function representing the following sub-functions which services and characteristics are reported below in the description: **SECURE_MANAGEMENT, CRYPTO_KEY, CRYPTO_OP, TRANSACTION,** and **OBJECT_DELETION**. The TSF provides optimized services for data integrity, memory management, I/O functions, atomic data transaction, cryptographic support, test and management of HW peripheral of Integrated Circuit ST31N600 including crypto library NESLIB V.6.2.1.

The TSF provide and manages the following functionalities:

- Secure Management functionalities (SECURE_MANAGEMENT) such as:
  - Memory cleaning upon: allocation of class instances, arrays, and APDU buffer, and de-allocation of array object, any transient object, any reference to an object instance created during an aborted transaction.
  - Unobservability: operations on secret keys are not observable by other subjects by observation of variations in power consumption or timing analysis, (supporting fulfilment of, FPT_EMSEC.1).
  - Preservation of a secure state when the following types of failures occur: loss of power or card tearing, NVRAM memory wear-out, failed checksum verification on sensitive data (Supporting fulfilment of FPT_FLS.1).
  - Monitor events related to TOE security and to preserve a TOE secure state, auditable events are: card tearing, power failure, abnormal environmental operating conditions (frequency, voltage, and temperature), physical tampering and NVRAM consistency/integrity check failure (Supporting fulfilment of FPT_PHP.3).
  - Exception handling: This function addresses the TOE exception management. The reasons of these exceptions are: range of operating conditions, integrity errors, life cycle and TOE internal audit failure. Upon detection of exception and depending on exception severity the TOE may end the working session entering a state where the TOE becomes irresponsive or, in case of major severity, may change its life cycle state entering the “end of use” state.
  - Testing: This function ensures the tests of TOE functionalities. It includes the test of Integrated Circuit ST31N600 hardware components and its environmental operating conditions such as temperature, voltage and clock frequency. Depending on the typology and on the operation to be performed, the test is executed at power-up or before/after sensitive operation e.g. digital signature or cryptographic computation. Upon detection of an anomaly and depending on anomaly severity the TOE may end the working session entering a state becoming irresponsive or, in case of major severity, may change its life cycle state entering the “end of use” state (Supporting fulfilment, FPT_TST.1).
- Crypto Key management functionalities (CRYPTO_KEY) such as:
  - key generation
  - key destruction (supporting the fulfilment of SFRs: FCS_CKM.4)
  - Integrity and the unobservability of the keys.

- **Crypto Operation (CRYPTO_OP):** functionalities of encryption/decryption and signature creation/verification with the support of the following algorithms:
  - DES ECB and CBC
  - Triple DES ECB and CBC with 16, 24 bytes of key
  - AES ECB and CBC with 128, 256 bits of key
  - RSA CRT with key length 1024, 2048, 3072, and 4096 bits
  - ECC (ECDSA, ECKA) with key length up to 521 bits
  - Hashing (SHA-1, SHA-256, SHA-384, SHA-512)
  - Deterministic Random Number Generation

  Supporting the fulfilment of SFRs: FCS_CKM.1, FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/MAC, FCS_COP.1/AA, FCS_RND.1.
- **Data Transaction management (TRANSACTION):** functionalities concerning NVRAM changes in order to assure the coherence of the data if a failure or power interruption occurs during their update
- **Secure data deletion (OBJECT_DELETION):** de-allocation of memory resources of data no longer accessible. The security functionality also guarantees that the information content of unreachable data cannot be retrieved anymore (supporting the fulfilment of SFRs: FCS_CKM.4).

12.9 Coverage of the SFRs

The following table provides the coverage of the SFRs by the TSFs of the TOE.

Table 14: SFR vs TSF rationale

SFR \ TSF	SF_BAC – Basic Access Control	SF_AUTH – Perso Agent Auth	SF_AA Active Authentication	SF_SM – Secure Messaging	SF_AC – Access Control	SF_CRY – Cryptographic Support	SF_PRO – Data Protection	SF_OSPlat Java Platform and OS
FAU_SAS.1					x			
FCS_CKM.1	x					x		x
FCS_CKM.4	x					x		x
FCS_COP.1/SHA						x		x
FCS_COP.1/ENC	x					x		x
FCS_COP.1/AUTH						x		x
FCS_COP.1/MAC	x					x		x
FCS_COP.1/AA			x					x
FCS_RND.1						x		x
FIA_UID.1	x	x						
FIA_UAU.1	x	x						
FIA_UAU.4	x	x						
FIA_UAU.5	x	x						
FIA_UAU.6	x							
FIA_AFL.1	x	x			x			
FDP_ACC.1	x	x			x			
FDP_ACF.1	x	x			x			
FDP_UCT.1				x				
FDP_UIT.1				x				
FMT_SMF.1		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			
FMT_MTD.1/KEY_READ					x			
FPT_EMSEC.1						x	x	x
FPT_FLS.1							x	x
FPT_TST.1							x	x
FPT_PHP.3							x	x

13 Statement of compatibility

This is a Statement of Compatibility between this Security Target of the composite TOE and the Security Target of the underlying STeID JC Open OS platform [ST_SteidJCOS].

The following tables show the mapping between SARs, SFRs, and Objectives of the platform ST and this ST, demonstrating the compatibility between the two STs.

13.1 Security Assurance Requirements (SARs) mapping

The following table shows the mapping between the STeID JC Open OS platform SARs and this composite TOE SARs. The platform is certified EAL6 augmented with ALC_FLR.2. The composite TOE is certified EAL4 augmented with ALC_DVS.2. There is no conflict regarding the Security Assurance Requirements (SARs) because the composite TOE SARs represent a subset of the platform SARs.

Table 15: Platform SARs VS Composite TOE SARs

STeID JC Open OS platform SARs (EAL6 augmented with ALC_FLR.2)	Composite TOE SARs (EAL 4 augmented with ALC_DVS.2)
ADV_ARC.1	ADV_ARC.1
ADV_FSP.5	ADV_FSP.4
ADV_IMP.2	ADV_IMP.1
ADV.INT.3	-
ADV_SPM.1	-
ADV_TDS.5	ADV_TDS.3
AGD_OPE.1	AGD_OPE.1
AGD_PRE.1	AGD_PRE.1
ALC_CMC.5	ALC_CMC.4
ALC_CMS.5	ALC_CMS.4
ALC_DEL.1	ALC_DEL.1
ALC_DVS.2	ALC_DVS.2 (augmentation)
ALC_FLR.2 (augmentation)	-
ALC_LCD.1	ALC_LCD.1
ALC_TAT.3	ALC_TAT.1
ASE_CCL.1	ASE_CCL.1
ASE_ECD.1	ASE_ECD.1
ASE_INT.1	ASE_INT.1
ASE_OBJ.2	ASE_OBJ.2
ASE_REQ.2	ASE_REQ.2
ASE_SPD.1	ASE_SPD.1
ASE_TSS.1	ASE_TSS.1
ATE_COV.3	ATE_COV.2
ATE_DPT.3	ATE_DPT.1
ATE_FUN.2	ATE_FUN.1
ATE_IND.2	ATE_IND.2
AVA_VAN.5	AVA_VAN.3

13.2 Threats compatibility

The following table shows the compatibility between the STeID JC Open OS platform Threats and this composite TOE Threats.

Table 16: Compatibility between Platform and composite TOE Threats

STeID JC Open OS platform Threats	Rationale
T.CONFID-APPLI-DATA	The attacker executes an application to disclose data belonging to another application. Threat considered in the composite TOE.
T.CONFID-JCS-CODE	The attacker executes an application to disclose the Java Card System code. Threat covered by the platform evaluation.
T.CONFID-JCS-DATA	The attacker executes an application to disclose data belonging to the Java Card System. Threat covered by the platform evaluation.
T.INTEG-APPLI-CODE	The attacker executes an application to alter (part of) its own code or another application's code. Threat considered in the composite TOE.
T.INTEG-APPLI-CODE.LOAD	The attacker modifies (part of) its own or another application code when an application package is transmitted to the card for installation. Threat considered in the composite TOE.
T.INTEG-APPLI-DATA	The attacker executes an application to alter (part of) another application's data. Threat considered in the composite TOE.
T.INTEG-APPLI-DATA.LOAD	The attacker modifies (part of) the initialization data contained in an application package when the package is transmitted to the card for installation. The threat has been considered in the composite TOE.
T.INTEG-JCS-CODE	The attacker executes an application to alter (part of) the Java Card System code. Threat covered by the platform evaluation.
T.INTEG-JCS.DATA	The attacker executes an application to alter (part of) Java Card System or API data. Threat covered by the platform evaluation.
T.SID.1	An applet impersonates another application, or even the Java Card RE, in order to gain illegal access to some resources of the card or with respect to the end user or the terminal. Threat considered in the composite TOE.
T.SID.2	The attacker modifies the TOE's attribution of a privileged role (e.g. default applet and currently selected applet), which allows illegal impersonation of this role. Threat considered in the composite TOE.
T.EXE-CODE.1	An applet performs an unauthorized execution of a method. Threat considered in the composite TOE.
T.EXE-CODE.2	An applet performs an execution of a method fragment or arbitrary data. Threat considered in the composite TOE.
T.NATIVE	An applet executes a native method to bypass a TOE Security Function such as the firewall. Threat covered by the platform evaluation.

T.RESOURCES	An attacker prevents correct operation of the Java Card System through consumption of some resources of the card: RAM or NVRAM. Threat covered by the platform evaluation.
T.DELETION	The attacker deletes an applet or a package already in use on the card, or uses the deletion functions to pave the way for further attacks (putting the TOE in an insecure state). Threat covered by the platform evaluation.
T.INSTALL	The attacker fraudulently installs post-issuance of an applet on the card. This concerns either the installation of an unverified applet or an attempt to induce a malfunction in the TOE through the installation process). Threat covered by the platform evaluation.
T.OBJ-DELETION	The attacker keeps a reference to a garbage collected object in order to force the TOE to execute an unavailable method, to make it to crash, or to gain access to a memory containing data that is now being used by another application. Threat covered by the platform evaluation.
T.PHYSICAL	The attacker discloses or modifies the design of the TOE, its sensitive data or application code by physical (opposed to logical) tampering means. This threat includes IC failure analysis, electrical probing, unexpected tearing, and DPA. That also includes the modification of the runtime execution of Java Card System or SCP software through alteration of the intended execution order of (set of) instructions through physical tampering techniques. Threat covered by the platform evaluation.
T.LOADER_MISUSE	The attacker performs unauthorised use of the software loader functionality to upload a modified or malicious software version. Threat covered by the platform evaluation.

13.3 Assumptions compatibility

The following table shows the compatibility between the STeID JC Open OS platform Assumptions and this composite TOE Assumptions.

Table 17: Compatibility between Platform and composite TOE Assumptions

STeID JC Open OS platform Assumptions	Rationale
A.CAP_FILE	CAP files loaded post-issuance do not contain native methods. Assumption covered by ADV_IMP.1 of the composite TOE.
A.DELETION	Deletion of applets through the card manager is secure. Assumption not related to the composite TOE.
A.VERIFICATION	All the bytecodes are verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time. Assumption ensured by ALC_DVS.2 of the composite TOE.

13.4 Objectives compatibility

The following table shows the compatibility between the STeID JC Open OS platform Objectives and this composite TOE Objectives.

Table 18: Platform Objectives vs composite TOE Objectives

STeID Open JCOS Objectives	Rationale
O.SID	Objective covered by the platform evaluation
O.FIREWALL	Objective covered by the platform evaluation
O.GLOBAL_ARRAYS_CONFID	Objective covered by the platform evaluation
O.GLOBAL_ARRAYS_INTEG	Objective covered by the platform evaluation
O.NATIVE	Objective covered by the platform evaluation
O.OPERATE	Objective covered by the platform evaluation
O.REALLOCATION	Objective covered by the platform evaluation
O.RESOURCES	Objective covered by the platform evaluation
O.ALARM	Objective also covered by the composite TOE
O.CIPHER	Objective also covered by the composite TOE
O.RNG	Objective covered by platform evaluation
O.KEY-MNGT	Objective also covered by the composite TOE
O.PIN-MNGT	Objective also covered by the composite TOE
O.TRANSACTION	Objective covered by the platform evaluation
O.OBJ-DELETION	Objective covered by the platform evaluation
O.DELETION	Objective covered by the platform evaluation
O.LOAD	Objective covered by the platform evaluation
O.INSTALL	Objective covered by the platform evaluation
O.SENSITIVE_RESULTS_INTEG	Objective covered by the platform evaluation
O.CARD-MANAGEMENT	Objective covered by the platform evaluation
O.SCP.RECOVERY	Objective also covered by the composite TOE
O.SCP.SUPPORT	Objective also covered by the composite TOE
O.SCP.IC	Objective covered by the platform evaluation
OT.ACCESS_CONTROL	Objective covered by the platform evaluation

13.5 Security objectives for the environment (OEs) compatibility

The following table shows the compatibility between the STeID JC Open OS platform OEs and this composite TOE OEs.

Table 19: Platform OEs vs composite TOE OEs

STeID JC Open OS platform OEs	Rationale
OE.CAP_FILE	No applet loaded post-issuance shall contain native methods. This security objective is still relevant for the composite TOE and must be taken into account by the TOE user during the loading of additional applets.
OE.VERIFICATION	All the bytecodes shall be verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time. Additionally, the applet shall follow all the recommendations, if any, mandated in the platform guidance for maintaining the isolation property of the platform. This security objective is still relevant for the composite TOE and must be taken into account by the TOE user during the loading of additional applets.
OE.CODE-EVIDENCE	For application code loaded pre-issuance, evaluated technical measures implemented by the TOE or audited organizational measures must ensure that loaded application has not been changed since the code verifications required in OE.VERIFICATION. This security objective is still relevant for the composite TOE and must be taken into account by the TOE user during the loading of additional applets.
OE.KEY_PERSO	When the TOE life cycle is in manufacturing state, and before it is set to release state, all the default keys in the TOE are updated with final usage phase keys, FW authentication keys and the content loading keys. Objective covered by the platform evaluation.

13.6 Organizational security policies (OSPs) compatibility

The following table shows the compatibility between the STeID JC Open OS platform OSPs and this composite TOE OSPs.

STeID JC Open OS platform OSPs	Rationale
OSP.VERIFICATION	This policy shall ensure the consistency between the export files used in the verification and those used for installing the verified file. The policy must also ensure that no modification of the file is performed in between its verification and the signing by the verification authority. Policy covered by the platform evaluation

13.7 Compatibility between SFRs

The following table shows the compatibility between the STeID JC Open OS platform SFRs and this composite TOE SFRs. STeID JC Open OS platform SFRs are separated in the following groups as defined in [SOGIS-COMP]:

- IP_SFR: irrelevant Platform SFR not being used by the composite TOE
- RP_SFR-MECH: relevant Platform SFR being used by the composite TOE because its security properties providing protection attacks to the composite TOE
- RP_SFR-SERV: relevant Platform SFR being used by the composite TOE to implement a security service with associated TSFI

Table 20: Platform SFRs vs composite TOE SFRs

STeID JC Open OS platform SFRs	Rationale
FDP_ACC.2/FIREWALL	FIREWALL access control. RP_SFR-MECH
FDP_ACF.1/FIREWALL	FIREWALL access control. RP_SFR-MECH
FDP_IFC.1/JCVM	JCVM information flow control. RP_SFR-MECH
FDP_IFF.1/JCVM	JCVM information flow control. RP_SFR-MECH
FDP_RIP.1/OBJECTS	Any previous information content of a resource is made unavailable upon the allocation of the resource. RP_SFR-MECH
FMT_MSA.1/JCRE	FIREWALL access control. RP_SFR-MECH
FMT_MSA.1/JCVM	FIREWALL access control and JCVM information flow control. RP_SFR-MECH
FMT_MSA.2/FIREWALL_JCVM	FIREWALL access control and JCVM information flow control. RP_SFR-MECH
FMT_MSA.3/FIREWALL	FIREWALL access control. RP_SFR-MECH
FMT_MSA.3/JCVM	JCVM information flow control. RP_SFR-MECH
FMT_SMF.1/CM	Management Functions. RP_SFR-MECH
FMT_SMR.1/CM	Security roles. RP_SFR-MECH
FCS_CKM.1	Cryptographic key generation. RP_SFR-SERV
FCS_CKM.4	Cryptographic key destruction. RP_SFR-SERV
FCS_COP.1	Cryptographic operation. RP_SFR-SERV
FCS_RNG.1/IC	Random number generation. RP_SFR-SERV
FCS_RNG.1/DRBG	Random number generation. RP_SFR-SERV
FDP_RIP.1/ABORT	Subset residual information protection. RP_SFR-MECH
FDP_RIP.1/APDU	Subset residual information protection. RP_SFR-MECH
FDP_RIP.1/bArray	Subset residual information protection. RP_SFR-MECH
FDP_RIP.1/GlobalArray	Subset residual information protection. RP_SFR-MECH
FDP_RIP.1/KEYS	Subset residual information protection. RP_SFR-MECH
FDP_RIP.1/TRANSIENT	Subset residual information protection. RP_SFR-MECH
FDP_ROL.1/FIREWALL	Basic rollback. RP_SFR-MECH
FAU_ARP.1	Security alarms. RP_SFR-MECH
FDP_SDI.2/DATA	Stored data integrity monitoring and action. RP_SFR-MECH
FPR_UNO.1	Unobservability. RP_SFR-MECH
FPT_FLS.1	Failure with preservation of secure state. RP_SFR-MECH
FPT_TDC.1	Inter-TSF basic TSF data consistency. RP_SFR-MECH
FIA_ATD.1/AID	User attribute definition. RP_SFR-MECH
FIA_UID.2/AID	User identification before any action. RP_SFR-MECH
FIA_USB.1/AID	User-subject binding. RP_SFR-MECH
FMT_MTD.1/JCRE	Management of TSF data. RP_SFR-MECH
FMT_MTD.3/JCRE	Secure TSF data. RP_SFR-MECH
FDP_ITC.2/Installer	Import of user data with security attributes. RP_SFR-MECH
FMT_SMR.1/Installer	Security roles. RP_SFR-MECH
FPT_FLS.1/Installer	Failure with preservation of secure state. RP_SFR-MECH
FPT_RCV.3/Installer	Automated recovery without undue loss. RP_SFR-MECH

FDP_ACC.2/ADEL	Complete access control by Applet deletion manager. RP_SFR-MECH
FDP_ACF.1/ADEL	Security attribute based access control of the Applet deletion manager. RP_SFR-MECH
FDP_RIP.1/ADEL	Subset residual information protection by Applet deletion manager. RP_SFR-MECH
FMT_MSA.1/ADEL	Management of security attributes by Applet deletion manager. RP_SFR-MECH
FMT_MSA.3/ADEL	Static attribute initialisation by Applet deletion manager. RP_SFR-MECH
FMT_SMF.1/ADEL	Management Functions of the Applet deletion manager. RP_SFR-MECH
FMT_SMR.1/ADEL	Security roles of the Applet deletion manager. RP_SFR-MECH
FPT_FLS.1/ADEL	Failure with preservation of secure state by Applet deletion manager. RP_SFR-MECH
FDP_RIP.1/ODEL	Subset residual information protection of the object deletion. RP_SFR-MECH
FPT_FLS.1/ODEL	Failure with preservation of secure state of the object deletion. RP_SFR-MECH
FCO_NRO.2/CM	Enforced proof of origin of package loading. RP_SFR-MECH
FDP_IFC.2/CM	Complete information flow control of package loading. RP_SFR-MECH
FDP_IFF.1/CM	Simple security attributes of package loading. RP_SFR-MECH
FDP_UIT.1/CM	Data exchange integrity of package loading. RP_SFR-MECH
FIA_UID.1/CM	Timing of identification of package loading. RP_SFR-MECH
FMT_MSA.1/CM	Management of security attributes of package loading. RP_SFR-MECH
FMT_MSA.3/CM	Static attribute initialisation of package loading. RP_SFR-MECH
FMT_SMF.1/CM	Specification of Management Functions. RP_SFR-MECH
FMT_SMR.1/CM	Security roles. RP_SFR-MECH
FTP_ITC.1/CM	Inter-TSF trusted channel. RP_SFR-MECH
FDP_SDI.2/RESULT	Integrity_Sensitive_Result. RP_SFR-MECH
FPT_TST.1	TSF Testing. RP_SFR-MECH
FTP_ITC.1/Loader	Inter-TSF trusted channel of the flash loader. IP_SFR
FDP_UIT.1	Data exchange integrity of the flash loader. IP_SFR
FDP_ACC.1/Loader	Subset access control of the flash loader. IP_SFR
FDP_ACF.1/Loader	Security attribute based access control of the flash loader. IP_SFR

13.8 Conclusion

There are no contradictions between the ST of this composite TOE and the ST of the underlying STeID JC Open OS platform [ST_SteidJCOS].

14 Annex A – Crypto disclaimer

The following cryptographic algorithms are used by the TOE to enforce its security policy:

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits
Authentication	AES in CBC mode	[FIPS_PUB_197] (AES), [ISO 10116] (CBC)	128
	RSA in CRT	[ISO_9796-2]	1024, 2048, 3072, 4096
	ECDSA	[TR-03111]	192, 224, 256, 320, 384, 512, 521
Key Agreement	Session key established with BAC	[ICAO_9303]	112
Confidentiality	3DES in CBC mode	[SP800-67] and [ICAO_9303] normative appendix 5, A5.3	112
Integrity	Retail-MAC	[ISO_9797-1] (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)	112
Trusted Channel	Secure messaging in ENC_MAC mode and key established with BAC	[ICAO_9303]	112
RNG	True Random Generator (TRNG) class PTG.2 Deterministic Random Generator (DRBG) class RNG DRG.3	[AIS31/20]	N.A.
Hashing	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	[FIPS_180-2]	N.A.

15 Safety requirements

N/A

16 Environmental requirements

STMicroelectronics recommends viewing documents on the screen rather than printing to limit paper consumption.

17 Revision history

Date	Revision	Changes
October 22, 2025	A	Initial release
October 31, 2025	B	TOE physical scope includes platform guidance
December 22, 2025	C	Add CC certificate platform reference Updated the versions of the ST and AGD OPE of the platform

18 Contents

19 List of tables

20 List of figures