TOSHIBA
Leading Innovation >>>

TOSMART-P080
Security Target

May 13, 2011

Version 01.00.03
Public ST Version 01.00.00

TOSHIBA CORPORATION

Software Design Group
Smart Card Systems Department
Komukai Operations

Table of contents

1. Introduction

This document is the security target for the Toshiba ePassport TOSMART-P080 contactless smartcard product.
This Security Target is provided in accordance with "Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model" [CC_1]

This ST claims conformance with the version 3.1 (Revision 2) Protection Profile - Machine Readable Travel Document with ICAO Application and Basic Access Control [PP-0055], and with version 3.1 (Revision 2) Protection Profile - Machine Readable Travel Document with „ICAO Application", Extended Access Control [PP-0056]. Furthermore this ST refers to the version 2.1 Protection Profile with the official requirements document of the Japanese government [PP-ePassport]. Parts of [PP-0056] are copied literally in this ST and if not stated otherwise clearly marked in light grey. Where the contents of [PP-0055] differ from [PP-0056], the words are marked in italic light grey.

1.1. Common Criteria requirements

This document addresses the following requirements of the Common Criteria:

- ASE: Security Target Evaluation

1.2. Definitions and abbreviations

This document uses the following abbreviations:

AA	Active Authentication
APDU	Application Data Unit
BAC	Basic Access Control
CAP	Chip Authentication Protocol
CC	Common Criteria
EAC	Extended Access Control
IC	Integrated Circuit
MRTD	Machine Readable Travel Document
NVM	Non Volatile Memory (=EEPROM)
OSP	Organizational Security Policy
PA	Passive Authentication
TAP	Terminal Authentication Protocol
TOE	Target of Evaluation

TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface

2. ST introduction

This chapter presents the ST reference, a TOE reference, a TOE overview and a TOE description.

2.1. ST and TOE identification

Title:	TOSMART-P080 Security Target
Version:	Version 01.00.03
Date of issue:	13 May 2011
TOE identification:	TOSMART-P080
TOE version:	Version 01.06.04 + NVM Ver.01.00.01
Produced by:	TOSHIBA CORPORATION Social Infrastructure Systems Company

2.2. TOE overview

The TOE is a composite security IC, consisting of the hardware T6ND1, a Toshiba Integrated Circuit with Crypto Library which is used as the evaluated underlying platform and the Machine Readable Travel Document (OS and application) software, which is built on this hardware platform.

The T6ND1 is a secure single chip microcontroller with a RF type communication interface compliant to ISO-14443 type B. It consists of a central processing unit (CPU), memory elements (ROM, RAM, NV memory), and circuitry for the RF external interface that have been integrated with consideration given to tamper resistance. The software that is incorporated in the memory element is capable of providing security functions for the Machine Readable Travel Document (MRTD). The T6ND1 provide secure cryptographic services - triple DES, RSA, ECDSA signature verification, EC-Diffie-Hellman key exchange and Diffie-Hellman.
The MRTD consists of a secure operating system and application on top of the T6ND1. The operating system contains the embedded software functions used by the MRTD application.

The MRTD application provides

I. Basic Access Control
II. Active Authentication
III. Extended Access Control [TG_ASM_MRTD]

and facilitates Passive Authentication.

In the personalization phase, the TOE provides four mechanisms for authentication of the personalization agent. These are

I. Authentication using the Mutual Authenticate command
II. Basic Access Control
III. Terminal Authentication
IV. Authentication

When personalizing the TOE as an EAC passport, only the Terminal Authentication protocol shall be used for authentication of the personalization agent.

The TOE consists of the security functions: Memory access control, Sensitive data with CRC checksum, encrypted key data on NVM.

The memory access control provides functionality to protect the memory against illegal access during response data transmitting and sensitive data transporting. It uses the HW memory firewall function and it protects the TOE against fault injection attacks.

The Sensitive data with CRC checksum function provides the data integrity.
The encrypted key data on NVM is one of the file management functions and useful to store the data confidentiality.

Other security features of the TOE are:

- The sensitive flag is verified by CRC
- The special comparison time-constant function
- The double processing (for the sensitive process)
- Write the data with atomic transaction for the sensitive process
- The Software random wait
- Checking the ROM CRC
- The Self-diagnose for HW (Coprocessor, HW-DES, RNG) before using it
- Clear or randomize the temporary data after cryptogram process
- Protection of integrity by write only once access control

And there are security features of the HW below, these are direct copy from [HW-ST].

Detection for:

- trap latch (light sensor)
- power supply glitch
- clock frequency, out of the range
- internal/rectified supply and current, out of the range
- temperature, out of the range
- signal line error

- illegal access to the memories
- illegal configuration on test mode
- undefined instruction to CPU or co-processor
- access to vacant addresses
- active shield error

Countermeasures for physical probing to the TSF:

- bus scrambling
- memory address scrambling
- memory ciphering
- active shield

For cryptographic functions, the TOE provides only cryptographic operational mechanisms. Key management shall be performed by "the security IC Embedded software" (an application program on the TOE).

The TOE is designed for use as MRTD. The issuing State or Organization has issued the MRTD to the holder to be used for international travel. The intended environment is at inspection systems where the holder presents the MRTD to prove his or her identity. Therefore limited control can be applied to the MRTD and the card operational environment.

The TOE does not require non-TOE hardware, software or firmware to operate. However, it is noted that the TOE needs proper set up public key infrastructure to operate. The issuing and receiving States and Organizations are responsible for setting up this infrastructure.

2.3. TOE description

In this ST is the MRTD is viewed as unit of:

The **physical MRTD** is a travel document in the form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder:

(1) The biographical data on the biographical data page of the passport book

(2) The printed data in the machine readable zone (MRZ) and

(3) The printed portrait.

The **logical MRTD** is the data of the MRTD holder stored according to the logical data structure [ICAO_9303] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder:

(1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1)
(2) the digitised portraits (EF.DG2)
(3) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both
(4) the other data according to LDS (EF.DG5 to EF.DG16) and
(5) the document security object.

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

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [ICAO_9303]. These security measures include the binding of the MRTDS chip in the passport book.

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

2.3.1. Physical scope of the TOE

In this ST the physical TOE is considered to be the IC with embedded software without the antenna. The following figure describes the physical scope of the IC and software of the TOE:

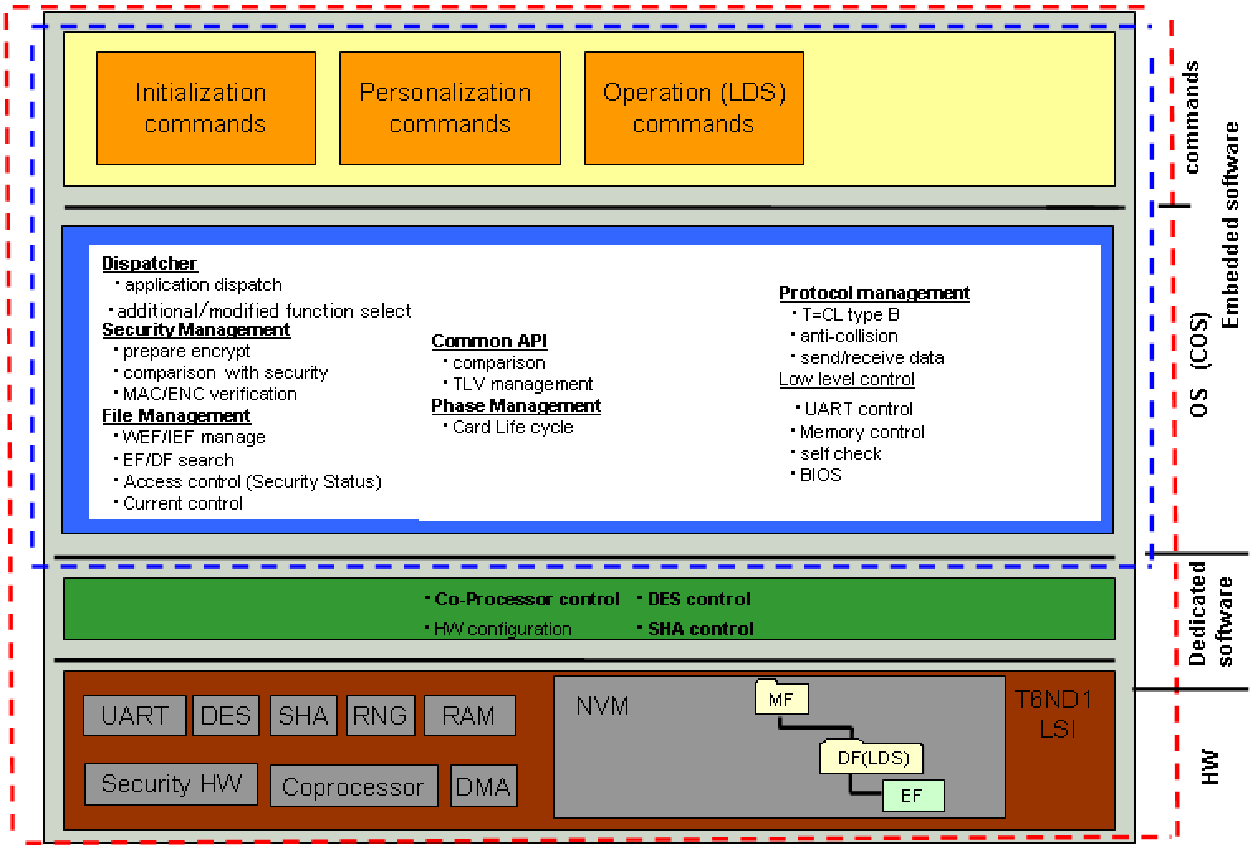

Figure 1 TOE scope (marked by red dashed line) and part additional to hardware (marked by blue dashed line)

The MRTD (OS and ePassport application) consists of a binary package that is implemented in the User ROM of the T6ND1. It can be divided in two layers, namely the OS providing a number of services to the other layer the application with commands.

The T6ND1 provides the computing platform and cryptographic support by means of co-processors and crypto library for the ePassport (OS and application) dedicated software. The T6ND1 Security Target describes the features as detectors, sensors and circuitry to protect the TOE of this hardware platform. These also apply to the composite TOE.

The antenna and capacitors for the RF interface are not part of the T6ND1 hardware. Paragraph 34 of the PP [PP-0056] states the following with respect to these items:
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.

2.3.2. TOE Delivery

Delivery item type	Identifier	Version	Medium	Notes
Hardware	T6ND1	#5.0	Sheet	
Software	MRTD＋OS	Ver.01.06.04 With NVM Ver.01.00.01	ROM and NV memory of hardware (user area)	
Guidance (for personalization agent)	Guidance Document for Personalization agent	MC-SJ0046-06	Document / pdf	
	Preparative guidance	MC-SJ0045-02	Document / pdf	
	Application Specification	MC-SM0914-05	Document / pdf	
	Personalization Manual	MC-SJ0047-05	Document / pdf	
	AA Personalization Manual	MC-SJ0048-05	Document / pdf	
	Authentication Manual using asymmetric command	MC-SJ0049-05	Document / pdf	
	Authentication Manual using MUTUAL AUTHENTICATE command	MC-SJ0050-05	Document / pdf	CFG_MuAuth
	Authentication Manual using BAC	MC-SJ0051-05	Document / pdf	CFG-BAC
	Authentication Manual using TA	MC-SJ0100-02	Document / pdf	CFG-TA
	Personalization Specification	MC-SM0812-04	Document / pdf	

	Procedural Request of Security Products Delivery and Receipt	MB-ICCARD-W471	Document / pdf

The column 'Notes' in the table above presents a configuration name for the used personalization agent authentication method in the respective document. When the TOE is delivered to the personalization agent, it is initialized by Toshiba to be used with a specific authentication method; by assigning a configuration name it can be ensured that the correct personalization guidance document is delivered.

2.3.3. Logical scope of the TOE

2.3.3.1. Description of the MRTD functionality

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Active Authentication of the MRTD's chip, Extended Access Control to and the Data Encryption of *additional* sensitive biometrics as optional security measure in the ICAO DOC 9303 [ICAO_9303]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently of the TOE by the TOE environment.

This security target addresses the protection of the logical MRTD

(i) in integrity by write-only-once access control and by physical means, and

(ii) in confidentiality by the Basic Access Control Mechanism and the Extended Access Control Mechanism.

This Security Target addresses the Chip Authentication described in [TG_ASM_MRTD] as an alternative to the optional Active Authentication stated in [ICAO_9303]

The TOE implements Basic Access Control. *The inspection system*

(i) reads optically the MTRD

(ii) Authenticates itself as an inspection system by means of Document Basic Access Keys.

After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [ICAO_9303], normative appendix 5.

The TOE implements Chip Authentication as defined in [TG_ASM_MRTD]. The Chip Authentication prevents data traces described in [ICAO_9303], normative appendix 7, A7.3.3

The Chip Authentication is provided by the following steps:

(i) the inspection system communicates by means of secure messaging established by Basic Access Control.

(ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object

(iii) the inspection system generates a ephemeral key pair

(iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellmann Primitive and

(v) The inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys).

The Chip Authentication requires collaboration of the TOE and the TOE environment.

The TOE also optionally implements Active Authentication (described in [ICAO_9303]). By means of a challenge-response protocol between the inspection system and the TOE, is ensured that the chip has not been cloned. For this purpose the TOE contains its own Active Authentication RSA key pair. A hash representation of Data Group 15 Public key is stored in the Document Security Object (SOD) and therefore authenticated by the issuer's digital signature. The corresponding Private Key is kept in the TOE's secure memory and never disclosed.

The Security Target requires the TOE to implement the Extended Access Control as defined in [TG_ASM_MRTD]. The Extended Access Control consists of two parts

(i) Chip Authentication protocol and

(ii) Terminal Authentication protocol

The Chip Authentication protocol (i) authenticates the MRTD's chip to the inspection system and (ii) establishes secure messaging which is used by Terminal Authentication to protect the confidentiality and integrity, integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication can only be performed if the Chip Authentication has been successfully executed.

The Terminal Authentication Protocol consists of:

(i) the authentication of the inspection system as entity authorized by the receiving

State or Organization through the issuing State, and

(ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems.

The issuing State or Organization authorizes the receiving state by means of certification the authentication public keys of Document Verifiers who create Inspection System certificates.

The following functionality is provided by the software building upon what was already provided by the underlying hardware platform.

In addition to the T6ND1 hardware platform and crypto library, the TOE-Software implements a file system and the functionality as described in. section 2.3.3.1, furthermore it implements functionality that protects the data in files and uses the data stored in files.

The TOE Software satisfies the following requirements of the underlying certified hardware platform T6ND1 and crypto library:

- Destruction of the cryptographic keys after usage (FCS_CKM.4)
- Implementation of the T6ND1 user guidance with respect to:
  - Enabling the hardware countermeasures
  - Anti-perturbation countermeasures

2.3.4. Life cycle Boundaries of the TOE

Following [PP-0055] and [PP-0056] the TOE life cycle is described in terms of the four life cycle phases: Phase 1 “Development”, Phase 2 “Manufacturing”, Phase 3 “Personalization of the MRTD” and Phase 4 “Operational Use”.

The TOE delivery occurs after phase 2 (or before phase 3), as an inlay and sheeted product transport key locked. The TOE is in its evaluated configuration after the card lifecycle state has been set to “Operation”, i.e. after phase 3 (or before phase 4).

As the antenna and inlay/sheeting are not considered security sensitive, these production steps are not included in the life-cycle scope and ALC assurance class. Different routes can be used for the inlay (include antenna) and sheeting production steps. These production steps take place either at Toshiba premises or at a different company outside

Toshiba premises.

Procedural measures and technical measures are in place to prevent undetected modification or masquerading of the TOE in these production steps.

3. Conformance claim and rationale

3.1. Conformance claim

This Security Target claims conformance to the Common Criteria version 3.1 Revision 3 July 2009. Furthermore it claims to be CC Part 2 extended and CC Part 3 conformant. The extended Security Functional Requirements are defined in [PP-0055], Chapter 4, and in [PP-0056], Chapter 4.

This Security Target claims conformance to Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application", Basic Access Control, [PP-0055] CC version 3.1.

This Security Target claims conformance to Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application", Extended Access Control, [PP-0056] CC version 3.1.

This Security Target is conforming to assurance package EAL4, augmented with ALC_DVS.2, AVA_VAN.5, and ASE_TSS.2. As there are known weaknesses in the quality (i.e. entropy) of the BAC keys generated by the environment, only enhanced basic attack potential (i.e. AVA_VAN.3) is considered for the Basic Access Control Mechanism of [PP-0055].

This Security Target also refers to the T6ND1 security target [HW_ST], which is compliant to the IC platform protection profile [PP-0035].

3.2. Conformance claim rationale

The PP-TOE of [PP-0055] is a MRTD ePassport with the Basic Access Control Mechanism. The PP-TOE of [PP-0056] is a MRTD ePassport with the Extended Access Control Mechanism, and requiring [PP-0055] for the BAC mechanism. The composite TOE is a MRTD ePassport providing the BAC and EAC mechanisms and active authentication.

.

Both PP's [PP-0055] and [PP-0056] require strict compliance, and their claims are combined in this Security Target, following Application Note 1 of [PP-0056]:

Application Note1: It is assumed that there are separate Security Targets for BAC and EAC. Note, that the claim for conformance to the BAC-PP [25] does not require the conformance claim to the EAC-PP. Nevertheless claiming conformance of this (EAC-)PP requires that the TOE meets a (separate) ST conforming to the BAC-PP [25]. Moreover, if possible with respect to the applied national scheme there might be one ST and with it one evaluation process merging the claims for [25] and this PP at hand.

In addition to [PP-0055] and [PP-0056] security objectives for both the TOE and the environment are defined in this Security Target for the implementation of the Active Authentication protocol. This protocol is used in life-cycle phase 4 and complements the Basic and Extended Access Control mechanisms. The additional security objectives do not conflict with the security objectives defined in the two PP's.

4. Security problem definition

This chapter presents the threats, organisational security policies and assumptions for the TOE.

The Assets, Assumptions, Threats and Organisational Security Policies are completely taken from the MRTD Basic Access Control Protection Profile [PP-0055] and the MRTD Extended Access Control Protection Profile [PP-0056].

4.1. Definition of subjects, objects and operations

To facilitate easy definition of threats, OSPs, assumptions, security objectives and security requirements, we first define the subjects to be used in the ST.

4.1.1. Subjects

The subjects in the following table are a literal copy for the ease of the user from the PP MRTD BAC [PP-0055] and PP MRTD EAC [PP-0056].

Table 4-1 Subjects; a literal copy of the MRTD Basic and Extended Access control PP's

Identification	Description
Manufacturer	The generic term for the IC Manufacturer producing the integrated circuit and the MRTD manufacturer completing the IC to the MRTD's chip. The manufacturer is the default user of the TOE during the Phase 2 Manufacturing. The TOE does not distinguish between the users IC manufacturer and the MRTD manufacturer using this role Manufacturer.
Personalization Agent	The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities: (i) establishing the identity of the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder, i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s), (iii) Writing these data on the physical and logical MRTD for the holder as defined in global, international and national interoperability, (iv) Writing the initial TSF data (v) Signing the Document Security Object defined in [ICAO_9303]
Country Verification Certification Authority	The Country verifying certification authority (CVCA) enforces the privacy policy of the issuing Country or Organization with respect to the protection of sensitive biometric reference data stored in the MRTD. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the

	public key of the CVCA are distributed in form of Country Verifying CA Link-certificates
Document Verifier	The Document Verifier (DV) enforces the privacy policy of the receiving Country with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations in form of the Document Verifier Certificates.
Terminal	A terminal is any technical system communicating with the TOE through the contactless interface
Inspection System	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder. 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 of the logical MRTD under the Basic Access Control by optical reading the MRTD or other parts of the passport book providing this information. The General Inspection System (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism. The Extended Inspection System (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.
MRTD Holder	The rightful holder of the MRTD for whom the issuing state or Organization personalized the MRTD.
Traveller	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
Attacker	*[PP-0055] definition:* A threat agent trying (i) to manipulate the logical MRTD without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4) or (iii) to forge a genuine MRTD. *[PP-0056] definition:* A threat agent trying

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

4.2. Assumptions about operational environment of TOE

Since this Security Target claims conformance to the MRTD BAC PP [PP-0055] and to the MRTD EAC PP [PP-0056], the assumptions defined in section 3.2 of these Protection Profiles are valid for this Security Target. The following table lists the assumptions of both Protection Profiles.

Table 4-2 Assumptions defined in the MRTD Basic Access Control Protection Profile and in the MRTD Extended Access Control Protection Profile

Assumptions	Titles
A.MRTD_Manufact	MRTD manufacturing on steps 4 to 6
A.MRTD_Delivery	MRTD delivery during steps 4 to 6
A.Pers_Agent	Personalization of the MRTD's chip
A.Insp_Sys	Inspection System for Global Interoperability
A.BAC_Keys	Cryptographic quality of Basic Access Control Keys
A.Signature_PKI	PKI for Passive Authentication
A.Auth_PKI	PKI for Inspection Systems

4.3. Description of Assets

Since this Security Target claims conformance to the MRTD Basic Access Control Protection Profile [PP-0055] and to the MRTD Extended Access Control Protection Profile [PP-0056], the assets defined in section 3.1 of these Protection Profiles are applied:

Logical MRTD Data ([PP-0055]):

- 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.

Logical MRTD sensitive User Data ([PP-0056]):

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

Authenticity of the MRTD's chip:

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

4.4. Threats

Since this Security Target claims conformance to the MRTD Basic Access Control Protection Profile [PP-0055] and to the MRTD Extended Access Control Protection Profile [PP-0056], the threats defined in section 3.3 of these Protection Profiles are valid for this Security Target. The following table lists the threats of the Protection Profile.

Table 4-3 Threats defined in the MRTD Basic Access Control Protection Profile and in the MRTD Extended Access Control Protection Profile

Treats	Titles
T.Chip_ID ([PP-0055] only)	Identification of MRTD's chip
T.Skimming ([PP-0055] only)	Skimming the logical MRTD
T.Eavesdropping ([PP-0055] only)	Eavesdropping to the communication between TOE and inspection system
T.Read_Sensitive_Data ([PP-0056] only)	Read the sensitive biometric reference data
T.Forgery	Forgery of data on the MRTD's chip
T.Counterfeit	MRTD's chip
T.Abuse_Func	Abuse of Functionality
T.Information_Leakage	Information leakage from MRTD's chip
T.Phys-Tamper	Physical Tampering
T.Malfunction	Malfunction of the environmental stress

4.5. Organizational Security Policies

Since this Security Target claims conformance to the MRTD Basic Access Control Protection Profile [PP-0055] and to the MRTD Extended Access Control Protection Profile [PP-0056], the Organisational Security Policies defined in section 3.4 of these Protection Profiles are valid for this Security Target. The following table lists the Organisational Security Policies of the Protection Profile.

Table 4-4 Organisational Security Policies defined in the MRTD Basic Access Control Protection Profile and in the MRTD Extended Access Control Protection Profile

OSP	Titles
P.BAC-PP ([PP-0056] only)	Fulfilment of the Basic Access Control Protection Profile
P.Sensitive_data ([PP-0056] only)	Privacy of sensitive biometric reference data
P.Manufact	Manufacturing of the MRTD's chip
P.Personalization	Personalization of the MRTD by issuing State or Organization only
P.Personal_data ([PP-0055] only)	Personal data protection policy

The additional Organisation Security Policies because of optional active authentication are:

P.Pers_Agent_Active_Authentication Personalization of the MRTD's chip including Active Authentication

The Personalization Agent ensures the correctness of *the Active Authentication Public Key (EF.DG15) if stored on the MRTD's chip.* The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by using the Personalization keys.

P.Insp_Sys_Active_Auth Inspection systems for global interoperability supporting Active Authentication.

The Extended Inspection Systems in addition may also support the terminal part of the Active Authentication protocol. Active authentication is optional and can be enabled or disabled by the manufacturer.

5. Personalization/Initialization Security Objectives

This chapter provides the statement of security objectives and the security objective rationale. For this chapter the MRTD Basic Access Control PP [PP-0055] and the MRTD Extended Access Control PP [PP-0056] can be applied completely. A short overview is given in the following. The security objectives for the optional Active Authentication are added to the appropriate sections in the chapter.

5.1. TOE Security Objectives

The TOE shall provide the following security objectives, taken from MRTD Basic Access Control Protection Profile [PP-0055] and the MRTD Extended Access Control Protection Profile [PP-0056]. The following table lists the security objectives for the TOE of the Protection Profile. Furthermore, a security objective for the optional Active Authentication is added.

Table 5-1 Security objectives for the TOE defined in the MRTD Basic Access Control Protection Profile and in the MRTD Extended Access Control Protection Profile.

Security objectives for the TOE	Titles
OT.AC_Pers	Access Control for personalization of logical MRTD
OT.Data_Int	Integrity of personal data
OT.Data_Conf	Confidentiality of personal data
OT.Sens_Data_Conf	Confidentiality of sensitive biometric reference data
OT.Identification	Identification and Authentication of the TOE
OT.Chip_Auth_Proof	Proof of MRTD's chip authenticity
OT.Prot_Abuse-Func	Protection against Abuse of Functionality
OT.Prot_Inf_Leak	Protection against Information Leakage
OT.Prot_Phys-Tamper	Protection against physical Tampering
OT.Prot_Malfunction	Protection against malfunction

The following security objective for the optional active authentication is added:

OT.Active_Auth_Proof Proof of the MRTD's chip authenticity by Active Authentication.

The TOE must support the Extended Inspection Systems to verify the authenticity of the MRTD's chip as issued by the identified issuing State or Organization. The TOE stores

RSA private key to prove its identity and this is used in the Chip Authentication. This mechanism is described in [ICAO_9303] as 'Active Authentication'.

5.2. Security Objectives for the Operational Environment

According to the MRTD Basic Access Control Protection Profile [PP-0055] and the MRTD Extended Access Control Protection Profile [PP-0056], the following security objectives for the operational environment are specified:

Table 5-2 Security objectives for the Issuing State or Organisation defined in the MRTD Basic Access Control Protection Profile and in the MRTD Extended Access Control Protection Profile

Security objectives for the Issuing State or Organisation	**Titles**
OE.MRTD_Manufact	Protection of the MRTD Manufacturing
OE.MRTD_Delivery	Protection of the MRTD delivery
OE.Personalization	Personalization of logical MRTD
OE.Pass_Auth_Sign	Authentication of logical MRTD by Signature
OE.BAC-Keys ([PP-0055] only)	Cryptographic quality of Basic Access Control Keys
OE.Auth_Key_MRTD ([PP-0056] only)	MRTD Authentication Key
OE.Authoriz_Sens_Data ([PP-0056] only)	Authorization for Use of Sensitive Biometric Reference Data
OE.BAC_PP ([PP-0056] only)	Fulfilment of the Basic Access Control Protection Profile

Table 5-3 Security objectives for the Receiving State or Organisation defined in the MRTD Basic Access Control Protection Profile and in the MRTD Extended Access Control Protection Profile

Security objective for the Receiving State or Organisation	**Titles**
OE.Exam_MRTD	Examination of the MRTD passport book
OE.Passive_Auth_Verif	Verification by Passive Authentication
OE.Prot_Logical_MRTD	Protection of data of the logical MRTD
OE.Ext_Insp_Systems ([PP-0056] only)	Authorization of Extended Inspection Systems

The additional security objectives of the operational environment for the implementation of Active Authentication are:

OE.Active_Auth_Key_MRTD MRTD Active Authentication Key

The issuing State or Organization may establish the necessary public key infrastructure in order to

(i) Generate the MRTD's Active Authentication key Pair,

(ii) Sign and store the Active Authentication public key in the Active Authentication public key data in EF.DG15

(iii) Support extended 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

OE.Active_Auth_Personalization Active Authentication Personalization

The manufacturer enables or disables the Active Authentication function of the TOE according to the decision of the issuing State or Organization. If the Active Authentication function is enabled the Personalization Agents generate the Active authentication keys and store them in the MRTD's chip.

OE.Exam_MRTD_Active_Auth Examination of the MRTD passport book using Active Authentication

During the examination of the MRTD presented to the traveller, the Extended Inspection Systems may perform the Active Authentication protocol [ICAO_9303] to verify the Authenticity of the presented MRTD's chip.

Note that the [HW-ST]'s Security objectives for the security IC embedded software development environment (OE.Plat-Appl) are applied to the T6ND1's Security IC Embedded Software: the MRTD (OS and ePassport application).

5.3. Security objectives rationale

In Table 5-4 each security objective for the TOE and the TOE environment is traced back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

Table 5-4 Tracing between objectives and Threat, Organisational Security Policy or Assumption.

Threat, Organisational Security Policy or Assumption	Security Objective	Sufficiency of countering
T.Chip_ID	OT.Identification, OE.BAC-Keys	See [PP-0055]

T.Skimming	OT.Data_Conf, OE.BAC-keys	See [PP-0055]
T.Eavesdropping	OT.Data_Conf	See [PP-0055]
T.Read_Sensitive_Data	OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	See [PP-0056]
T.Counterfeit	OT.Chip_Auth_Proof, OE.Auth_Key_MRTD, OE.Exam_MRTD	See [PP-0056]
T.Forgery	OT.AC_Pers, OT.Data_Int, OT.Prot_Phys-Tamper, OE.Pass_Auth_Sign, OE.Exam_MRTD, OE.Passive_Auth_Verif	See [PP-0055] and [PP-0056]
T.Abuse_Func	OT.Prot_Abuse-Func , OE.Personalization	See [PP-0055] and [PP-0056]
T.Information_Leakage	OT.Prot_Inf_Leak	See [PP-0055] and [PP-0056]
T.Phys-Tamper	OT.Prot_Phys-Tamper	See [PP-0055] and [PP-0056]
T.Malfunction	OT.Prot_Malfunction	See [PP-0055] and [PP-0056]
P.Personal_data	OT.Data_Int, OT.Data_Conf	See [PP-0055]
P.BAC-PP	OE.BAC-PP	See [PP-0056]
P.Sensitive_data	OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	See [PP-0056]
P.Manufact	OT.Identification	See [PP-0055] and [PP-0056]
P.Personalization	OT.AC_Pers, OT.Identification, OE.Personalization	See [PP-0055] and [PP-0056]
A.BAC_Keys	OE.BAC-Keys	See [PP-0055]
A.Signature_PKI	OE.Pass_Auth_Sign, OE.Exam_MRTD	See [PP-0056]
A.Auth_PKI	OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	See [PP-0056]
A.MRTD_Manufact	OE.MRTD_Manufact	See [PP-0055] and [PP-0056]
A.MRTD_Delivery	OE.MRTD_Delivery	See [PP-0055] and [PP-0056]
A.Pers_Agent	OE.Personalization	See [PP-0055] and [PP-0056]
A.Insp_Sys	OE.Exam_MRTD, OE.Prot_Logical_MRTD	See [PP-0055] and [PP-0056]
T.Counterfeit	OT.Active_Auth_Proof	See Below
P.Pers_Agent_Active_Authentication	OE.Active_Auth_Key_MRTD OE.Active_Auth_Personalization	See Below
P.Insp_Sys_Active_Auth	OE.Exam_MRTD_Active_Auth OE.Prot_Logical_MRTD	See Below

The threat **T.Counterfeit** "MRTD's Chip" addresses the attack of unauthorized copy or reproduction of the genuine MRTD chip. This attack is thwarted by active authentication proving the authenticity of the chip as required by OT.Active_Auth_Proof "Proof of MRTD's chip authenticity by Active Authentication". Using the authentication key pair to be generated by the issuing State or Organization. The Public Active Authentication

Key has to be written into EF.DG15 and signed by means of Documents Security Objects as demanded by OE_Active_Auth_Key_MRTD "MRTD Active Authentication Key". MRTDs must be controlled in order to prevent their usage for production counterfeit MRTDs targeted on by OD.Material.

The justification related to the OSP **P.Pers_Agent_Active_Authentication** "Personalization of the MRTD's chip including Active Authentication" is as follows:
The security objectives for the TOE environment OE.Active_Auth_Key_MRTD and OE.Active_Auth_Personalization include the enrolment, the protection with digital signature and the storage of the MRTD holder active authentication data (EF.DG15) on the TOE by the Personalization Agent and the enabling of this security feature of the TOE during initialization by the manufacturer.

The OSP **P.Insp_Sys_Active_Auth** "Inspection systems for global interoperability supporting Active Authentication" is covered by the security objective for the TOE environment OE.Exam_MRTD_Active_Auth "Examination of the MRTD passport book using Active Authentication" which optionally gives the ability to Extended Inspection Systems to verify the Authenticity of the presented MRTD's chip by means of the Active Authentication protocol [ICAO_9303]. The security objectives of the TOE environment OE.Prot_Logical_MRTD "protection of data of the MRTD" require the Inspection System to protect the logical MRTD data during the transmission and the internal handling.

6. Security Requirements

This chapter presents the statement of security requirements for the TOE and the security requirements rationale. This chapter applies the MRTD Basic Access Control Protection Profile [PP-0055] and the MRTD Extended Access Control Protection Profile [PP-0056].

6.1. Definitions

In the next sections the following the notation used

Whenever iteration is denoted, the component has an additional identification /XXXX.

When the refinement, selection or assignment operation is used these cases are indicated

6.2. Security Functional Requirements

Section 6.2.1 lists the Security Functional Requirements that are directly taken from the MRTD Basic Access Control Protection Profile [PP-0055] and the MRTD Extended Access Control Protection Profile [PP-0056] including all open assignment and selection operations. The SFRs FIA_API.1, FMT_LIM.1, FMT_LIM.2, FAU_SAS.1, FCS_RND.1 and FPT_EMSEC.1 are extended security requirements, completely defined in the PP.

The SFRs are split in two categories, the SFRs from the BAC Protection Profile [PP-0055] and EAC Protection Profile [PP-0056] that are incorporated by reference in this Security Target, and the SFRs added in this ST to cover the optional Active Authentication.

6.2.1. SFRs from the MRTD Basic and Extended Access Control Protection Profiles

Table 6-1 Security Functional Requirements taken from the MRTD Basic And Extended Access Control Protection Profiles.

Security functional requirements	In [PP-00xx]		Titles	Open operations
	55	56		
FAU_SAS.1	x	x	Audit Storage	-
FCS_CKM.1	x	x	Cryptographic key generation – Generation of Document Basic Access Keys by the TOE	*[PP-0055]* - *[PP-0056]* [selection: based on the key Diffie-Hellman key

				derivation Protocol compliant to PKCS#3, ECDH compliant to ISO 15946]
FCS_CKM.4	x	x	Cryptographic key destruction - MRTD	*[PP-0055] and [PP-0056]* [assignment: cryptographic key destruction method] [assignment: list of standards]
FCS_COP.1/SHA	x	x	Cryptographic operation – Hash for Key Derivation	*[PP-0055]* [selection: SHA-1 or other approved algorithms] [selection: FIPS 180-2 or other approved standards] *[PP-0056]* [selection: SHA-1, SHA-224, SHA-256 or other approved algorithms] [selection: FIPS 180-2 or other approved standards]
FCS_COP.1/SYM		x	Cryptographic operation – Symmetric Encryption / Decryption	*[PP-0056]* [assignment: cryptographic algorithm] [assignment: cryptographic key sizes]
FCS_COP.1/AUTH	x		Cryptographic operation – Authentication	*[PP-0055]* [selection: Triple-DES, AES] [selection: 112, 128, 168, 192, 256] [selection: FIPS 46-3 [9], FIPS 197 [12]]
FCS_COP.1/MAC	x	x	Cryptographic operation – Retail MAC	*[PP-0055]* - *[PP-0056]* [assignment: cryptographic algorithm] [assignment: cryptographic key sizes]
FCS_COP.1/SIG_VER		x	Cryptographic operation – Signature verification by MRTD	*[PP-0056]* [assignment: cryptographic algorithm]
FCS_COP.1/ENC	x		Cryptographic operation – Encryption / Decryption Triple DES	-
FCS_RND.1	x	x	Quality metric for random numbers	*[PP-0055] and [PP-0056]* [assignment: a defined quality metric]
FIA_UID.1	x	x	Timing of identification	-

FIA_UAU.1	x	x	Timing of authentication	-
FIA_UAU.4	x	x	Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE	*[PP-0055] and [PP-0056]* [selection: Triple-DES, AES or other approved algorithms]
FIA_UAU.5	x	x	Multiple authentication mechanisms	*[PP-0055]* [selection: Triple-DES, AES] [selection: the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key, [assignment other]] *[PP-0056]* [selection: Triple-DES, AES or other approved algorithms] [selection: the Symmetric Authentication Mechanism with Personalization Agent Key, the Terminal Authentication Protocol with Personalization Agent Keys]
FIA_UAU.6	x	x	Re-authenticating – Re-authenticating of Terminal by the TOE	-
FIA_AFL.1	x		Authentication failure handling	*[PP-0055]* [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]] [assignment: list of authentication events] [assignment: met or surpassed] [assignment: list of actions]
FIA_API.1		x	Authentication Proof of Identity	-
FDP_ACC.1	x	x	Subset access control – Basic Access control	-
FDP_ACF.1	x	x	Basic Security attribute based access control – Basic Access	-

			Control	
FDP_UCT.1	x	x	Basic data exchange confidentiality - MRTD	-
FDP_UIT.1	x	x	Data exchange integrity - MRTD	-
FMT_SMF.1	x	x	Specification of Management Functions	-
FMT_SMR.1	x	x	Security roles	-
FMT_LIM.1	x	x	Limited capabilities	-
FMT_LIM.2	x	x	Limited availability	-
FMT_MTD.1/INI_ENA	x	x	Management of TSF data – Writing of Initialization Data and Prepersonalization Data	-
FMT_MTD.1/INI_DIS	x	x	Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data	-
FMT_MTD.1/CVCA_INI		x	Management of TSF data – Initialization of CVCA Certificate and Current Date	*[PP-0056]* [assignment: the authorised identified roles]
FMT_MTD.1/CVCA_UPD		x	Management of TSF data – Country Verifying Certification Authority	-
FMT_MTD.1/DATE		x	Management of TSF data – Current date	-
FMT_MTD.1/KEY_WRITE	x	x	Management of TSF data – Key Write	-
FMT_MTD.1/CAPK		x	Management of TSF data – Chip Authentication Private Key	*[PP-0056]* [selection: create, load] [assignment: the authorised identified roles]
FMT_MTD.1/KEY_READ	x	x	Management of TSF data – Key Read	-
FMT_MTD.3		x	Secure TSF data	-
FPT_EMSEC.1	x	x	TOE Emanation	*[PP-0055] and [PP-0056]* [assignment: types of emissions] [assignment: specified limits]

				[assignment: list of types of user data] [assignment: list of types of user data]
FPT_FLS.1	x	x	Failure with preservation of secure state	-
FPT_TST.1	x	x	TSF testing	*[PP-0055] and [PP-0056]* [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]]
FPT_PHP.3	x	x	Resistance to physical attack	-

The TOE summary specification describes how the TOE protects itself against bypass, logical tampering and inference. (see section 7.3.1 and 7.3.2).

Completion of operations from the both PP's [PP-0055] and [PP-0056] is as follows:

FCS_CKM.1 Cryptographic key generation – Generation of Document Basic Access Keys by the TOE

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: [ICAO_9303], normative appendix 58.

FCS_CKM.1/DH Cryptographic key generation – Diffie-Hellman Keys by the MRTD

FCS_CKM.1.1/DH	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[selection: based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH compliant to ISO 15946]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: [TG_ASM_MRTD] , Annex A.1
[selection: based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH compliant to ISO 15946]	based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3

[assignment: cryptographic key sizes]	1024bit, 1280bit, 1536bit, 2048bit

FCS_CKM.1/ECDH Cryptographic key generation – Elliptic Curve Diffie-Hellman Keys by the MRTD

FCS_CKM.1.1/ECDH	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[selection: based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH compliant to ISO 15946]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: [TG_ASM_MRTD], Annex A.1
[selection: based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH compliant to ISO 15946]	ECDH compliant to ISO 15946
[assignment: cryptographic key sizes]	160bit, 192bit, 224bit, 256bit, 384bit

FCS_CKM.4 Cryptographic key destruction – MRTD

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment: cryptographic key destruction method]** that meets the following: **[assignment: list of standards]**
[assignment: cryptographic key destruction method]	BAC session key clear[1]
[assignment: list of standards]	[ICAO_9303]

FCS_COP.1/SHA1 Cryptographic operation – Hash for Key Derivation MRTD

FCS_COP.1.1/SHA1	The TSF shall perform hashing in accordance with a specified cryptographic algorithm **[selection: SHA-1, SHA-224, SHA-256 or other approved algorithms]** and cryptographic key sizes none that meet the following: **[selection: FIPS 180-2 or other**

[1] It is noted that the key destruction method is independent of the keys that are destructed using this method.

	approved standards]
[selection: SHA-1, SHA-224, SHA-256 or other approved algorithms]	SHA-1
[selection: FIPS 180-2 or other approved standards]	FIPS 180-2

FCS_COP.1/SHA224 Cryptographic operation – Hash for Key Derivation MRTD

FCS_COP.1.1/SHA224	The TSF shall perform hashing in accordance with a specified cryptographic algorithm **[selection: SHA-1, SHA-224, SHA-256 or other approved algorithms]** and cryptographic key sizes none that meet the following: **[selection: FIPS 180-2 or other approved standards]**
[selection: SHA-1, SHA-224, SHA-256 or other approved algorithms]	SHA-224
[selection: FIPS 180-2 or other approved standards]	FIPS 180-2

FCS_COP.1/SHA256 Cryptographic operation – Hash for Key Derivation MRTD

FCS_COP.1.1/SHA256	The TSF shall perform hashing in accordance with a specified cryptographic algorithm **[selection: SHA-1, SHA-224, SHA-256 or other approved algorithms]** and cryptographic key sizes none that meet the following: **[selection: FIPS 180-2 or other approved standards]**
[selection: SHA-1, SHA-224, SHA-256 or other approved algorithms]	SHA-256
[selection: FIPS 180-2 or other approved standards]	FIPS 180-2

Application note: The TOE implements the additional SHA-224 and SHA-256 for signature verification and generation.

FCS_COP.1/SYM Cryptographic operation – Symmetric Encryption / Decryption

FCS_COP.1.1/SYM	The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: 'TR-03110', [TG_ASM_MRTD].
[assignment: cryptographic algorithm]	Triple-DES
[assignment: cryptographic key sizes]	112 bit

FCS_COP.1/AUTH Cryptographic operation – Symmetric Encryption / Decryption

FCS_COP.1.1/AUTH	The TSF shall perform symmetric authentication – encryption and decryption in accordance with a specified cryptographic algorithm **[selection: Triple-DES, AES]** and cryptographic key sizes **[selection: 112, 128, 168, 192, 256]** bit that meet the following: **[selection: FIPS 46-3 [9], FIPS 197 [12]]**
[selection: Triple-DES, AES]	Triple-DES
[selection: 112, 128, 168, 192, 256]	112
[selection: FIPS 46-3 [9], FIPS 197 [12]]	FIPS 46-3 [FIPS46-3]

FCS_COP.1/MAC Cryptographic operation – MAC

FCS_COP.1.1/MAC	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: 'TR-03110', [TG_ASM_MRTD].
[assignment: cryptographic	Retail MAC

algorithm]	
[assignment: cryptographic key sizes]	112 bit

FCS_COP.1/SIG_VER_RSA_TA Cryptographic operation – Signature verification by MRTD

FCS_COP.1.1/SIG_VER_RSA_TA	The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.
[assignment: cryptographic algorithm]	RSA
[assignment: cryptographic key sizes]	1024bit, 1280bit, 1536bit, 2048bit, 3072bit, 4096bit
[assignment: list of standards]	RSASSA-PKCS1-v1_5, RSASSA-PSS [PKCS#1]

FCS_COP.1/SIG_VER_ECDSA_TA Cryptographic operation – Signature verification by MRTD

FCS_COP.1.1/SIG_VER_RSA_TA	The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.
[assignment: cryptographic algorithm]	ECDSA
[assignment: cryptographic key sizes]	160bit, 192bit, 224bit, 256bit, 384bit
[assignment: list of standards]	ECDSA [TR-03111]

FCS_RND.1 Quality metric for random numbers

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

Assignment: a defined quality metric	Class K3 of AIS 20 [AIS_20].

FIA_UAU.4/BAC Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE

FCS_UAU.4.1/BAC	The TSF shall prevent reuse of authentication data related to 1. Basic Access Control Authentication Mechanism, 2. Authentication Mechanism based on **[selection: Triple-DES, AES or other approved algorithms]**.
[selection: Triple-DES, AES or other approved algorithms]	Triple-DES

FIA_UAU.4/EAC Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE

FCS_UAU.4.1/EAC	The TSF shall prevent reuse of authentication data related to 1. Terminal Authentication Protocol, 2. Authentication Mechanism based on **[selection: Triple-DES, AES or other approved algorithms]**.
[selection: Triple-DES, AES or other approved algorithms]	Triple-DES

FIA_UAU.5/BAC Multiple authentication mechanisms

FCS_UAU.5.1/BAC	The TSF shall provide 1. Basic Access Control Authentication Mechanism 2. Symmetric Authentication Mechanism based on **[selection: Triple-DES, AES]** to support user authentication.
[selection: Triple-DES, AES]	Triple-DES
FCS_UAU.5.2/BAC	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) **[selection: the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric**

	Authentication Mechanism with the Personalization Agent Key, [assignment other]], 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.
[selection: the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key, [assignment other]]	the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key

FIA_UAU.5/EAC Multiple authentication mechanisms

FCS_UAU.5.1/EAC	The TSF shall provide 1. Terminal Authentication Protocol, 2. Secure messaging in MAC-ENC mode, 3. Symmetric Authentication Mechanism based on **[selection: Triple-DES, AES or other approved algorithms]** to support user authentication.
[selection: Triple-DES, AES or other approved algorithms]	Triple-DES
FCS_UAU.5.2/EAC	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 **[selection: the Symmetric Authentication Mechanism with Personalization Agent Key, the Terminal Authentication Protocol with Personalization Agent Keys]** . 2. After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message

	authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism. 3. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses the public key presented during the Chip Authentication Protocol and the secure messaging established by the Chip Authentication Mechanism
[selection: the Symmetric Authentication Mechanism with Personalization Agent Key, the Terminal Authentication Protocol with Personalization Agent Keys]	the Terminal Authentication Protocol with Personalization Agent Keys

FIA_AFL.1 /Auth_PA Authentication failure handling, of authentication of the Personalization Agent

FIA_AFL.1.1/Auth_PA	The TSF shall detect when **[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]** unsuccessful authentication attempts occur related to **[assignment: list of authentication events]**.
[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]	3
[assignment: list of authentication events]	Basic Access Control by the Personalization Agent, Symmetric Authentication by the Personalization Agent
FIA_AFL.1.2/Auth_PA	When the defined number of unsuccessful authentication attempts has been **[assignment: met or surpassed]**, the TSF

	shall **[assignment: list of actions]**.
[assignment: met or surpassed]	Met or surpassed
[assignment: list of actions]	Block permanently

FIA_AFL.1/Auth_OU Authentication failure handling

FIA_AFL.1.1/Auth_OU	The TSF shall detect when **[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]** unsuccessful authentication attempts occur related to **[assignment: list of authentication events]**.
selection:[assignment:positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]	1
assignment: list of authentication events	Basic Access Control Authentication, Terminal Authentication
FIA_AFL.1.2/Auth_OU	When the defined number of unsuccessful authentication attempts has been **[assignment: met or surpassed]**, the TSF shall **[assignment: list of actions]**.
Selection: met, surpassed	Met or surpassed
Assignment: list of actions	Return error status

FMT_MTD.1/CVCA_INI Management of TSF Data – Initialization of CVCA Certificate and Current Date

FMT_MTD.1.1/CVCA_INI	The TSF shall restrict the ability to write the 1. initial Country Verifying Certification Authority Public Key, 2. initial Country Verifying Certification Authority Certificate, 3. initial Current Date to **[assignment: the authorised identified roles]**.
[assignment: the authorised identified roles]	Personalization Agent

FMT_MTD.1/CAPK Management of TSF data – Chip Authentication Private key

FMT_MTD.1.1/CAPK	The TSF shall restrict the ability to **[selection: create, load]** the Chip Authentication Private Key to **[assignment: the authorised identified roles]**.
[selection: create, load]	Load
[assignment: the authorised identified roles]	Personalization Agent

FPT_EMSEC.1 TOE emanation

FPT_EMSEC.1.1	The TOE shall not emit **[assignment: types of emissions]** in excess of **[assignment: specified limits]** enabling access to Personalization Agent Key(s) *and Chip Authentication Private Key* and **[assignment: list of types of user data]**.
[assignment: types of emissions]	Side channel
[assignment: specified limits]	Limits of the state of the art
[assignment: list of types of user data]	none
FPT_EMSEC.1.2	The TSF shall ensure any users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Key(s) *and Chip Authentication Private Key* and **[assignment: list of types of user data]**.
[assignment: list of types of user data]	none

FPT_TST.1 TSF testing

FPT_TST.1.1	The TSF shall run a suite of self tests **[selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self test should occur]]** to demonstrate the correct operation of the TSF.
[selection: during initial start-up, periodically	during initial start-up, periodically during normal operation, at the request of the authorized user,

during normal operation, at the request of the authorized user, at the conditions] [assignment: conditions under which self test should occur]	
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of the TSF data.
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

6.3. The SFRs that are added implement the optional Active Authentication

FCS_COP.1/SIG_GEN_RSA_AA Cryptographic operation – Signature verification MRTD RSA for Active Authentication

FCS_COP.1.1/SIG_GEN_RSA_AA	The TSF shall perform **[assignment: list of cryptographic operations]** in accordance with a specified algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following **[assignment: list of standards]**
Assignment: list of cryptographic operations	Digital signature generation
Assignment cryptographic algorithm	RSA
Assignment: cryptographic key sizes	1024bit, 1280bit, 1536bit, 1792bit, 2048bit
Assignment: list of standards	Digital Signature scheme 1[ISO9796-2]

FIA_API/AA Authentication Proof of identity – Active Authentication

FIA_API.1.1/AA	The TSF shall provide a **[assignment: authentication**

	mechanism] to prove the identify of the **[assignment: authorized user or rule]**
assignment: authentication mechanism	Active Authentication
assignment: authorized user or rule	TOE
Dependencies	No dependencies

FMT_MTD.1/AA Management of TSF data – Active Authentication Private Key

FMT_MTD.1.1/AA	The TSF shall restrict the ability to **[selection: create, load]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**
selection: create, load	Load
assignment: list of TSF data	Active Authentication Private Key
assignment: the authorized identified roles	Personalization Agent
Dependencies	FMT_SMR.1 Security roles, FMT_SMF.1 Specification of management functions

FMT_MTD.1/KEY_READ_AA Management of TSF data – Key Read Active Authentication

FMT_MTD.1.1/KEY_READ_AA	The TSF shall restrict the ability to **[selection:change_default, query, modify, delete, clear, [assignment:other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**
selection:change_default, query, modify, delete, clear, [assignment:other operations]	Read
assignment: list of TSF data	Active Authentication Private Key
assignment: the authorized identified roles	None

Dependencies	FMT_SMR.1 Security roles, FMT_SMF.1 Specification of management functions

FMT_MOF.1/AA Management of function in TSF – Active Authentication

FMT_MOF.1.1/AA	The TSF shall restrict the ability to **[Selection: determine the behaviour of, disable, enable, modify the behaviour of]** the functions **[assignment: list of functions]** to **[assignment: the authorized identified roles]**
Selection: determine the behaviour of, disable, enable, modify the behaviour of	disable and enable
assignment: list of functions	TSF Active Authentication
assignment: the authorized identified roles	Manufacturer
Dependencies	FMT_SMR.1 Security roles, FMT_SMF.1 Specification of management functions

6.4. TOE Security Assurance Requirements

The TOE security assurance requirements are conformant to the CC Evaluation Assurance Level EAL4 augmented with AVA_VAN.5, ALC_DVS.2 and ASE_TSS.2. For the Basic Access Control mechanism, only AVA_VAN.3 is applicable.

6.5. Explicitly stated requirements

See [PP-0055] Chapter 4 and [PP-0056] Chapter 4.

6.6. Security Requirements Rationale

The purpose of the Security Requirements Rationale is to demonstrate that the security requirements are suitable to meet the Security Objectives.

6.6.1. The SFRs meet the Security Objectives for the TOE

Table 6-2 Tracing between SFRs and objectives for the TOE

Security Objectives for	SFRs	Rationale

the TOE		
OT.AC_Pers	FCS_CKM.1, FCS_CKM.1/DH, FCS_CKM.1/ECDH[2], FCS_CKM.4, FCS_COP.1/SHA1[3], FCS_COP.1/SHA224[4], FCS_COP.1/SHA256[5], FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/MAC, FCS_COP.1/SYM, FCS_COP.1/SIG_VER_RSA_TA[6], FCS_COP.1/SIG_VER_ECDSA_TA[7], FCS_RND.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.4/BAC, FIA_UAU.4/EAC, FIA_UAU.5/BAC, FIA_UAU.5/EAC, FIA_UAU.6, FDP_ACC.1, FDP_ACF.1, FDP_UCT.1, FDP_UIT.1, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ, FPT_EMSEC.1, FPT_FLS.1, FPT_PHP.3	See [PP-0055] and [PP-0056]
OT.Data_Int	FCS_CKM.1, FCS_CKM.1/DH, FCS_CKM.1/ECDH, FCS_COP.1/SHA1, FCS_COP.1/SHA224, FCS_COP.1/SHA256, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/MAC, FCS_COP.1/SYM, FCS_RND.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.4/BAC, FIA_UAU.4/EAC, FIA_UAU.5/BAC, FIA_UAU.5/EAC, FIA_UAU.6, FDP_ACC.1, FDP_ACF.1, FDP_UCT.1, FDP_UIT.1, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ, FMT_MTD.1/CAPK	See [PP-0055] and [PP-0056]
OT.Data_Conf	FCS_CKM.1, FCS_CKM.1/DH, FCS_CKM.1/ECDH, FCS_CKM.4, FCS_COP.1/SHA1, FCS_COP.1/SHA224, FCS_COP.1/SHA256, FCS_COP.1/ENC, FCS_COP.1/MAC, FCS_RND.1, FIA_UID.1, FIA_AFL.1, FIA_UAU.1, FIA_UAU.4/BAC, FIA_UAU.4/EAC, FIA_UAU.5/BAC, FIA_UAU.5/EAC, FIA_UAU.6, FDP_ACC.1, FDP_ACF.1, FDP_UCT.1, FDP_UIT.1, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ	See [PP-0055]
OT.Sens_Data_Conf	FCS_CKM.1/DH, FCS_CKM.1/ECDH, FCS_CKM.4, FCS_COP.1/SHA1, FCS_COP.1/SHA224, FCS_COP.1/SHA256, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_COP.1/SIG_VER_RSA_TA, FCS_COP.1/SIG_VER_ECDSA_TA, FCS_RND.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.4/EAC, FIA_UAU.5/EAC, FIA_UAU.6, FDP_ACC.1, FDP_ACF.1, FDP_UCT.1, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD,	See [PP-0056]

[2] additional iteration of FCS_CKM.1/DH to fit the ECDH besides the DH

[3] iteration of FCS_COP.1/SHA to fit the SHA-1

[4] iteration of FCS_COP.1/SHA to fit the SHA-224

[5] iteration of FCS_COP.1/SHA to fit the SHA-256

[6] iteration of FCS_COP.1/SIG_VER to fit RSA for Terminal Authentication

[7] iteration of FCS_COP.1/SIG_VER to fit ECDSA for Terminal Authentication

	FMT_MTD.1/DATE, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FMT_MTD.3	
OT.Identification	FAU_SAS.1, FIA_UID.1, FIA_AFL.1, FIA_UAU.1, FMT_MTD,1/INI_ENA, FMT_MTD.1/INI_DIS	See [PP-0055] and [PP-0056]
OT.Chip_Auth_Proof	FCS_CKM.1/DH, FCS_CKM.1/ECDH, FCS_COP.1/SHA1, FCS_COP.1/SHA224, FCS_COP.1/SHA256, FCS_COP.1/SYM, FCS_COP.1/MAC, FIA_API.1, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ	See [PP-0056]
OT.Prot_Inf_Leak	FPT_EMSEC.1, FPT_TST.1, FPT_FLS.1, FPT_PHP.3	See [PP-0055] and [PP-0056]
OT.Prot_Phys-Tamper	FPT_PHP.3	See [PP-0055] and [PP-0056]
OT.Prot_Malfunction	FPT_TST.1, FPT_FLS.1	See [PP-0055] and [PP-0056]
OT.Prot_Abuse-Func	FMT_LIM.1, FMT_LIM.2	See [PP-0055] and [PP-0056]
OT.Active_Auth_Proof	FCS_COP.1/SIG_GEN_RSA_AA, FMT_MOF.1/AA, FIA_API.1/AA, FDP_ACC.1, FDP_ACF.1, FMT_MTD.1/AA, FMT_MTD.1/KEY_READ_AA, FCS_COP.1/SHA1, FCS_COP.1/SHA256, FCS_RND.1	See below

In the TOE summary specification (see 7.3.1 and 7.3.2) is described how the TOE protects itself against logical tampering, interference and bypass.

The rationale for the additional **OT.Active_Auth_Proof** is as follows:
The proof of authenticity of the TOE IC is ensured by the Active Authentication protocol, implemented by FIA_API.1/AA, FDP_ACC.1 and FDP_ACF.1 proving the identity and authenticity of the TOE. The Active Authentication relies on FCS_COP.1/SIG_GEN_RSA_AA, FCS_COP.1/SHA1, FCS_COP.1/SHA256, FCS_CKM.4 and FCS_RND.1. The Active Authentication relies on a confidential private key internally stored in the TOE as required by FMT_MTD.1/AA and FMT_MTD.1/KEY_READ_AA. During the manufacturing phase the option to use active authentication is enabled or disabled with FMT_MOF.1/AA.

6.6.2. Reason for choosing Security Assurance Requirements

The Security Assurance Requirements have been chosen to meet the requirements of [PP-0055] and or [PP-0056]. This was augmented with ASE_TSS.2 to provide the potential consumers of this TOE a clearer view on the protection provided against bypassing and modification of the TOE.

6.6.3. All dependencies have been met

In the following table the satisfaction of the dependencies is indicated.

Table 6-3 Dependencies of SFRs.

SFR	Dependencies	Fulfilment of dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 cryptographic operations], FCS_CKM.4 cryptographic key destruction	Covered by [PP-0055]
FCS_CKM.1/DH FCS_CKM.1/ECDH[8]	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 cryptographic operations], FCS_CKM.4 cryptographic key destruction	Covered by [PP-0056]
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]	Covered by [PP-0055] and [PP-0056]
FCS_COP.1/SHA1 FCS_COP.1/SHA224 FCS_COP.1/SHA256[9]	[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], FCS_CKM.4 Cryptographic key destruction	Covered by [PP-0055] and [PP-0056]
FCS_COP.1/SYM	[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], FCS_CKM.4 Cryptographic key destruction	Covered by [PP-0056]
FCS_COP.1/AUTH	[FDP_ITC.1 Import of user data without security	Covered by [PP-0055]

[8] FCS_CKM.1/ECDH_MRTD is the iteration added for ECDH key exchange

[9] FCS_COP.1/SHA1_MRTD, FCS_COP.1/SHA224_MRTD and FCS_COP.1/SHA1_MRTD are iterations of FCS_COP.1/SHA_MRTD for the different cryptographic implementations of SHA

	attributes, 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/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], FCS_CKM.4 Cryptographic key destruction	Covered by [PP-0055] and [PP-0056]
FCS_COP.1/SIG_VER_RSA_TA FCS_COP.1/SIG_VER_ECDSA_TA[10]	[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], FCS_CKM.4 Cryptographic key destruction	Covered by [PP-0056]
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], FCS_CKM.4 Cryptographic key destruction	Covered by [PP-0055]
FCS_RND.1	No dependencies	n.a.
FIA_UID.1	No dependencies	n.a
FIA_UAU.1	FIA_UID.1 timing of authentication	Covered by [PP-0055] and [PP-0056]
FIA_UAU.4/BAC FIA_UAU.4/EAC	No dependencies	n.a.
FIA_UAU.5/BAC FIA_UAU.5/EAC	No dependencies	n.a.
FIA_UAU.6	No dependencies	n.a.
FIA_AFL.1/Auth_PA	FIA_UAU.1. Timing of authentication	Covered by [PP-0055]

[10] Different iterations of FCS_COP.1/SIG_VER for the different methods of signature verification

FIA_AFL/Auth_OU		
FIA_API.1	No dependencies	n.a
FDP_ACC.1	FDP_ACF.1 Security attribute base access control	Covered by [PP-0055] and [PP-0056]
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Covered by [PP-0055] and [PP-0056]
FPD_UCT.1	[FDP_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]	Covered by [PP-0055] and [PP-0056]
FDP_UIT.1	[FDP_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]	Covered by [PP-0055] and [PP-0056]
FMT_SMF.1	No dependencies	Covered by [PP-0055] and [PP-0056]
FMT_SMR.1	FIA_UID.1 Timing of identification	Covered by [PP-0055] and [PP-0056]
FMT_LIM.1	FMT_LIM.2	Covered by [PP-0055] and [PP-0056]
FMT_LIM.2	FMT_LIM.1	Covered by [PP-0055] and [PP-0056]
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Covered by [PP-0055] and [PP-0056]
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Covered by [PP-0055] and [PP-0056]
FMT_MTD.1/CVCA_INI	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Covered by [PP-0056]
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Covered by [PP-0056]
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Covered by [PP-0056]
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Covered by [PP-0055] and [PP-0056]
FMT_MTD.1/CAPK	FMT_SMF.1 Specification of management functions,	Covered by [PP-0056]

	FMT_SMR.1 Security roles	
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Covered by [PP-0055] and [PP-0056]
FMT_MTD.3	FMT_MTD.1 management of TSF data	Covered by [PP-0056]
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.
FMT_MOF.1/AA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FIA_API.1/AA	No dependencies	n.a
FMT_MTD.1/AA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/KEY_READ_AA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FCS_COP.1/SIG_GEN_RSA_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], FCS_CKM.4 Cryptographic key destruction	See below

The FCS_COP.1/SIG_GEN_RSA_AA uses the private key to generate certificates for the active authentication protocol. The security attributes are managed by FMT_MTD.1/AA and FMT_MTD.1/KEY_READ_AA. The copy of the private key is securely destroyed after generation of the certificate using FCS_CKM.4. Therefore, the dependencies are either fulfilled or it is explained why they are not fulfilled.

7. TOE Summary Specification

7.1. Statement of Compatibility

This section presents the compatibility between this Security Target for the composite product and the Platform Security Target [HW-ST].

The relevant platform-TSF (RP-TSF) used by the current ST-are FMT_LIM.1, FMT_LIM.2, FPT_FLS.1, FPT_PHP.3, FCS_RNG.1, FCS_COP.1[DES], FCS_COP.1[RSA], FCS_COP.1[DH], FCS_COP.1[SHA], FDP_ITT.1, FPT_ITT.1, FDP_IFC.1.
The other platform-TSF (IP-TSF) FRU_FLT.2 and FAU_SAS.1 are not used by the current ST.

The current ST and [HW-ST] match, i.e. there is no conflict between security environments, security objectives, and security requirements. Reason is that the current ST uses two PP's that are built upon [PP0035], which is the conforming PP for [HW-ST].

Assumption A.Plat-Appl from [HW-ST] is fulfilled automatically, due to strict conformance to the PP's: Paragraph 15 of [PP-0055] and Paragraph 19 of [PP-0056] state about life-cycle phase 1 "Development":
(Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the MRTD application and the guidance documentation associated with these TOE components.

7.2. TOE meets the SFRs

For each SFR we demonstrate that the TOE meets it. The tracings are provided implicitly by the rationales.

7.2.1. Self-Protection of the TOE

The self-protection of the TOE is divided in four functions that implement the protection of the TOE.

Abuse of functionality

Abuse of functionality relates to the SFRs FMT_LIM.1 and FMT_LIM.2, The ePassport application and OS do not have a test-mode. These SFRs are implemented by the underlying hardware platform. To the ST of the Hardware platform is referred for more detailed information [HW-ST]

Leakage

Leakage of information relates to the SFRs FPT_EMSEC.1, FPT_TST.1, FPT_FLS.1 and FPT_PHP.3. The SFRs FPT_FLS.1 and FPT_PHP.3 are implemented by the underlying hardware platform [HW_ST]. FPT_EMSEC.1 is also implemented by the underlying hardware platform [HW_ST], by the SFRs FDP_ITT.1, FPT_ITT.1, FDP_IFC.1 (the secure implementation of the different cryptographic operations in the crypto library and hardware TOE). The ePassport application and underlying OS perform a number of tests during start-up, normal operation and at request of an authorized user to preserve the integrity of the TSF data and the TSF executable code.

Malfunction

Malfunction relates to the SFRs FPT_TST.1 and FPT_FLS.1. Protection to malfunction is implemented by the underlying hardware platform [HW ST]. The ePassport application and underlying OS implement the SFR FPT_TST.1. The ePassport application and underlying OS perform a number of tests during start-up, normal operation and at request of an authorized user to preserve the integrity of the TSF data and the TSF executable code. The tests also include the self-diagnosis of the underlying hardware (Coprocessor, HW-DES, RNG) before these components are used. The ePassport application and underlying OS perform CRC check for sensitive data, flag and perform double checking

Physical manipulation and probing

Physical manipulation and probing relates to FPT_PHP.3. Protection against physical manipulation and probing is implemented by the underlying hardware platform [HW_ST].

7.2.2. Random numbers

The random number generation relates to the SFR FCS_RND.1. The random number generator is implemented by the underlying hardware platform [HW-ST]. The RNG in the underlying platform has a physical noise source and fulfils the requirements of functionality class K3 of [AIS_20].

7.2.3. Cryptographic operations

The cryptographic operations relate to the SFRs FCS_COP.1/SHA1, FCS_COP.1/SHA224, FCS_COP.1/SHA256, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/SIG_VER_RSA_TA, FCS_COP.1/SIG_VER_ECDSA_TA, FCS_COP.1/SIG_GEN_RSA_AA, FCS_CKM.1/DH, and FCS_CKM.1/ECDH. All these cryptographic operations are implemented by the certified crypto library and underlying hardware platform [HW-ST].

7.2.4. Chip authentication proof

The chip authentication proof relates to the SFRs FCS_CKM.1, FCS_CKM.1/DH, FCS_CKM.1/ECDH, FCS_COP.1/SHA1, FCS_COP.1/SHA256, FCS_COP.1/SYM, FCS_COP.1/MAC, FIA_API.1, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FCS_COP.1/SIG_GEN_RSA_AA, FMT_MOF.1/AA, FIA_API.1/AA, FMT_MTD.1/AA, FMT_MTD.1/KEY_READ_AA and FCS_RND.1.

The cryptographic operations, namely FCS_CKM.1/DH, FCS_CKM.1/ECDH, FCS_COP.1/SHA1, FCS_COP.1/SHA256, FCS_COP.1/ENC, FCS_COP.1/SYM, FCS_COP.1/MAC, and FCS_COP.1/SIG_GEN_RSA_AA, are implemented by the underlying hardware platform. The random number generation (FCS_RND.1) is also implemented by the underlying platform.

The SFRs FCS_CKM.1/DH, FCS_CKM.1/ECDH, FIA_API.1, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FCS_COP.1/SHA1, FCS_COP.1/SHA256, FCS_COP.1/SYM, FCS_COP.1/MAC implement the Chip Authentication protocol additional to the Basic Access Control according to [TG_ASM_MRTD].

The SFRs FCS_COP.1/SIG_GEN_RSA_AA, FMT_MOF.1/AA, FIA_API/AA, FMT_MTD.1/AA and FMT_MTD.1/KEY_READ_AA are implemented additional by the ePassport application and underlying OS to provide optional Active Authentication. The Active Authentication protocol is implemented as specified in [ICAO_9303]. After generation of the signature the copy of the private key kept in memory is destructed by overwriting the key value with ‘00’. (FCS_CKM.4).

The TOE provides a file structure in which the different secret keys are kept in special IEFs. These IEFs do not provide normal read access to interfaces outside the TOE. Also access control mechanisms using security attributes are in place to prevent that an unauthorized user gets access to files.

7.2.5. Identification and Authentication

Identification of the TOE's IC and making sure that when the TOE is in phase 4 "operational use" only identification is allowed after successful authentication by the Inspection System is implemented by the SFRs FAU_SAS.1, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FIA_UID.1 and FIA_UAU.1.

During phase 2 "manufacturing" and phase 3 "personalization of the TOE", the TOE can be identified using a special APDU. The unique identification is part of the initialization data written by the manufacturer in phase 2 (FAU_SAS.1, FMT_MTD.1.1/INI_ENA). This command is no longer available without successful authentication when the TOE is in phase 4 "operational use". When the TOE is in phase 4 "operational use" the special ADPU can be used only after successful basic authentication of the Inspection System (FMT_MTD.1/INI_DIS, FIA_UID.1 and FIA_UAU.1)

Authentication during Personalization relates to the SFRs FCS_CKM.1, FCS_COP.1/SHA1, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_RND.1, FIA_UAU.4/BAC, FIA_UAU.4/EAC, FIA_UAU.5/BAC, FIA_UAU.5/EAC, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/KEY_READ, FIA_AFL.1/Auth_PA and FPT_EMSEC.1.

The SFRs, FCS_COP.1/SHA1, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_RND.1 and FPT_EMSEC.1 are implemented by the underlying hardware platform.

The personalization agent can choose among three methods to authenticate to the TOE during personalization.
The Personalization agent can use Basic Access Control (FCS_RND.1, FCS_CKM.1, FCS_COP.1/SHA1) with the personalization keys to authenticate to the TOE during personalization, when the TOE is in life-cycle phase 3. If the authentication during personalization fails three times the TOE blocks permanently (FIA_AFL.1/Auth_PA). The SFRs FMT_MTD.1/KEY_READ and FPT_EMSEC.1 ensure the confidentiality of the personalization agent keys. Furthermore, the TOE can be personalized under secure messaging with a MAC for message integrity (FCS_COP.1/ENC, FCS_COP.1/SYM, FCS_COP.1/MAC)

As second method the Personalization Agent can use a Symmetric Authentication mechanism, with the personalization agent keys (FCS_RND.1, FCS_COP.1/AUTH, and

FCS_COP.1/SYM, FIA_UAU.4/BAC, FIA_UAU.4/EAC, FIA_UAU.5/BAC, FIA_UAU.5/EAC). After three unsuccessful authentication attempts the TOE blocks permanently (FIA_AFL.1/Auth_PA)

As third method, the Personalization Agent can use an asymmetric authentication mechanism.

The session key is destructed, when an error occurs in during the personalization agent authentication process (FCS_CKM.4). After successful authentication the personalization agents are allowed to write the contents of the different files on the TOE only once. The application and OS check, by the contents of the file that no write action already is performed on the selected file, at the start of writing.

Read access to the secret Personalization Agent Keys is prevented and the confidentiality of the keys is kept (FMT_MTD.1/KEY_READ and FPT_EMSEC.1).
During personalization no secure messaging is applied for writing to the TOE when Symmetric Authentication is selected for authentication of the Personalization Authentication. Each write action is followed by an automatic verification, so the data on the TOE is directly checked upon writing. The personalization agent does not need read access to check the correctness of the personalized data on the TOE. Also during personalization it is not possible to read the biometric data files of the TOE (EF.DG3 and EF.DG4), without being authenticated using the Extended Access Control.

At the end of the personalization the TOE is brought to the 'operational' life cycle. From this point on a user has to be properly authorized to read any data from the TOE.

7.2.6. Data integrity

The integrity of personal data relates to the SFRs FCS_CKM.1, FCS_CKM.1/DH, FCS_CKM.1/ECDH, FCS_CKM.4, FCS_COP.1/SHA1, FCS_COP.1/SYM, FCS_COP.1/ENC, FCS_COP.1/MAC, FIA_UID.1, FIA_UAU.1, FIA_UAU.4/BAC, FIA_UAU.4/EAC, FIA_UAU.5/BAC, FIA_UAU.5/EAC, FIA_UAU.6, FDP_ACC.1, FDP_ACF.1, FDP_UIT.1, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FMT_MTD1/KEY_WRITE, and FMT_MTD.1/CVCA_INI,

The SFRs FCS_CKM.1/DH, FCS_CKM.1/ECDH, FCS_COP.1/SHA1, FCS_COP.1/SYM, FCS_COP.1/ENC, and FCS_COP.1/MAC are implemented by the underlying hardware platform [HW-ST].

Only the authorized personalization agent is allowed to write the contents of the files and load secret keys during personalization (FMT_MTD.1/KEY_WRITE. FMT_MTD.1/CAPK, FMT_MTD.1/AA, FDP_ACC.1, FDP_ACF.1, FIA_UID.1, FIA_UAU.1, FMT_MTD.1/CVCA_INI).

Other user roles like the Inspection systems are only allowed to read the data after successful appropriate authentication (FMT_MTD.1/KEY_READ, FDP_ACC.1, FDP_ACF.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.4/BAC, FIA_UAU.4/EAC, FIA_UAU.5/BAC, and FIA_UAU.5/EAC). Furthermore, secure messaging is used to communicate between the TOE and the authenticated Inspection System (FIA_UAU.6, FDP_UIT.1). After use the session keys are destroyed using (FCS_CKM.4) to all '00', when an error occurs in the Basic Access Control process, in secure messaging, or in the MAC calculation during Extended Access Control.

Finally, data integrity during writing of sensitive data is ensured by using an atomic transaction mechanism to write this data.

7.2.7. Data confidentiality

The data confidentiality is related to the SFRs FCS_CKM.1, FCS_CKM.1/DH, FCS_CKM.1/ECDH, FCS_CKM.4, FCS_COP.1/SHA1, FCS_COP.1/SHA224, FCS_COP.1/SHA256, FCS_COP.1/SYM, FCS_COP.1/ENC, FCS_COP.1/MAC, FCS_COP.1/SIG_VER_RSA_TA, FCS_COP.1/SIG_VER_ECDSA_TA, FCS_RND.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.4/BAC, FIA_UAU.4/EAC, FIA_UAU.5/BAC, FIA_UAU.5/EAC, FIA_UAU.6, FIA_AFL.1/Auth_OU, FDP_ACC.1, FDP_ACF.1, FDP_UCT.1, FDP_UIT.1, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, and FMT_MTD.3

The cryptographic SFRs and random number generator implemented by the underlying hardware platform (FCS_CKM.1/DH, FCS_CKM.1/ECDH, FCS_COP.1/SHA1, FCS_COP.1/SHA224, FCS_COP.1/SHA256, FCS_COP.1/SYM, FCS_COP.1/ENC, FCS_COP.1/MAC, FCS_COP.1/SIG_VER_RSA_TA, FCS_COP.1/SIG_VER_ECDSA_TA, and FCS_RND.1).

For the data confidentiality the TOE distinguishes two levels: after personalization the successfully authenticated Basic Inspection System is allowed to read EF.DG1 to

EF.DG16 except for EF.DG3 and EF.DG4. Only a successfully authenticated Extended Inspection System is allowed to read EF.DG1 to EF.DG16 including EF.DG3 and EF.DG4. This distinction and access control is mandated by the SFRs (FDP_ACC.1 and FDP_ACF.1)

After successful authentication using both Basic Access Control (FCS_RND.1, FCS_CKM.1, FCS_COP.1/SHA1, FIA_UAU.4/BAC, FIA_UAU.5/BAC) and Extended Access Control (FCS_RND.1, FCS_COP.1/SHA1, FCS_COP.1/SHA224, FCS_COP.1/SHA256, FCS_CKM.1, FCS_CKM.1/DH, FCS_CKM.1/ECDH, FCS_COP.1/SIG_VER_RSA_TA, FCS_COP.1/SIG_VER_ECDSA_TA), secure messaging is used when the TOE is communicating with the Inspection System. (FCS_COP.1/SYM, FCS_COP.1/ENC, FCS_COP.1/MAC, FIA_UAU.6, FDP_UCT.1, FDP_UIT.1). The session keys are destroyed after use (FCS_CKM.4) to all '00', when an error occurs in the Basic Access Control process, in secure messaging, or in the MAC calculation during Extended Access Control.

If authentication fails (FIA_AFL.1/Auth_OU) on the MUTUAL AUTHENTICATE of Basic Access Control, the card returns the error status.

To allow a verification of the certificate chain, the CVCA's public key and certificate as well as the current date are updated by the authorized identified role (FMT_MTD.3, FMT_MTD.1/CVCA_UPD, and FMT_MTD.1/DATE).

7.3. The TOE protects itself against interference, logical tampering and bypass

In addition to the measures described in section 7.2.1, the following self-protection measures are implemented in the TOE.

7.3.1. TOE protects itself against interference and logical tampering

The interaction of the underlying hardware platform and the ePassport and OS together provide the required protection. The potential effects of attacks are varied, and so are the security measures to counter them. The ePassport application and underlying OS depend on the hardware platform to provide a first line of defense by providing detection and prevention mechanisms, and a secondary set of defenses that seek to randomize the results of perturbation attacks. The ePassport augments this by providing additional detection mechanisms, which have a high chance to detect perturbation attacks.

The software runs in two different memory firewall configurations: “normal” and, “transmission”. The underlying OS ensures that during transmission, the only areas accessible are those necessary for the transmission, so no accidental access to the general RAM and EEPROM and coprocessors is possible.

The underlying hardware platform reacts to access outside the configured boundaries with a hardware security reset.

The integrity of sensitive data being copied from memory to the CPU registers is verified by CRC before committing the operation. Just before the use of sensitive data, the integrity of the data is verified. Data whose integrity is incorrect is not used for the operation. Depending on the function and error, a failed integrity check leads to an error message or a card mute.

All files and meta-data are stored with automatic data integrity protection by the Card OS’s File Management. Failure of the integrity checks causes to return an appropriate error message.

7.3.2. TOE protects itself against bypass

The underlying hardware platform protects itself and the ePassport and OS against bypass via physical means. To augment this protection, the ePassport and OS store all internal files (IEFs) with automatic encryption/decryption such that they are stored encrypted in NVM.

The underlying hardware platform protects itself and the ePassport and OS against bypass via side channel analysis. To augment this protection, the ePassport and OS incorporate additional timing countermeasures surrounding sensitive operations, perform comparisons of sensitive data in a time constant way with additional blinding of the values compared.

For the non-bypassibility of the hardware component is referred to [HW-ST].

8. Reference

No	Title	Date	Version	publisher	Document number
[CC_1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model	July 2009	Revision 3		
[CC_2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements	July 2009	Revision 3		
[CC_3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements	July 2009	Revision 3		
[CEM]	Common Methodology for Information Technology Security Evaluation (CEM), Part 2: Evaluation Methodology	July 2009	Revision 3		
[PP-0035]	IC Platform Protection Profile	15.06.2007	1.0	Bundesamt für Sicherheit in der Informationstechnik (BSI)	BSI-PP-0035
[PP-0055]	Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control	25.03.2009	1.10	Bundesamt für Sicherheit in der Informationstechnik (BSI)	BSI-CC-PP-0055
[PP-0056]	Common Criteria	25.03.2009	1.1	Bundesamt für	BSI-CC-PP-

	Protection Profile Machine Readable Travel Document with „ICAO Application”, Extended Access Control			Sicherheit in der Informationstechnik (BSI)	0056
[PP-ePassport]	Protection profile for IC for the passport booklet	24.09.2004	1.0	Ministry of Foreign Affairs - Consular Affairs Bureau - Passport Division	JBMIA e-MRP/WG3
[CC_AAP]	Common Criteria Supporting Document Mandatory Technical Document Application of Attack Potential to Smartcards	March 2009	Version 2.7 Revision 1	Common Criteria Development Board	CCDB-2009-03-001
[ICAO_9303]	Machine Readable Travel Documents Sixth Edition — 2006 Doc 9303 Part 1 Machine Readable Passports Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capability	2006	Sixth Edition	Authority of the secretary general, International Civil Aviation Operation	
[TG_ASM_MRTD]	Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents- Extended Access control (EAC)		1.11	Bundesamt für Sicherheit in der Informationstechnik (BSI)	TR-03110
[HW_ST]	T6ND1 series Integrated Circuit with Crypto	28 December 2010	Version 2.16	Toshiba	CC-T6ND1-ST-ENG

	Library v1.0 Security Target				
[AIS_20]	Application Notes and Interpretation of the Scheme (AIS), AIS 20: Functionality classes and evaluation methodology for deterministic random number generators	2.12.1999	1	Bundesamt für Sicherheit in der Informationstechnik (BSI)	
[PKCS#3]	PKCS#3: Diffie-Hellman key-agreement standard RSA Laboratories Technical Note	November 1, 1993	1.4	RSA Laboratories	
[ISO15946-1]	ISO/IEC 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves –Part1: General	2002-12-01		ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission)	
[ISO15946-3]	ISO/IEC 15946-3. Information technology – Security techniques – Cryptographic techniques based on elliptic curves –Part3:Keyestablishment	2002-12-01		ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission)	
[TR-03111]	Technical Guideline TR-03111 Elliptic Curve Cryptography(ECC) based on ISO 15946	2007-02-14	1.00	Bundesamt für Sicherheit in der Informationstechnik (BSI)	
[ISO9796-2]	ISO/IEC 9796-2. Information technology	2002-10-01		ISO (the International	

	— Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms			Organization for Standardization) and IEC (the International Electrotechnical Commission)	
[PKCS#1]	PKCS#1 v2.1: RSA cryptography standard. RSA Laboratories Technical Note	June 14, 2002		RSA Laboratories	
[FIPS180-2]	FIPS PUB 180-2 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Secure Hash Standard (SHS) and change notice to include SHA-224	August, 2002		National Institute of Standards and Technology	
[FIPS46-3]	FIPS PUB 46-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Data Encryption Standard (DES)	Reaffirmed 1999, October 25		National Institute of Standards and Technology	

End of Document