TOSHIBA
Leading Innovation

TOSMART-P080-AAJePassport
Security Target

February 24, 2011

Version 01.00.04
Public ST Version 01.00.00

TOSHIBA CORPORATION

Software Design Group
Smart Card Systems Department
Komukai Operations

TOSHIBA
Leading Innovation

Table of contents

TOSHIBA
Leading Innovation

1. Introduction

This document is the security target for the ePassport extended access control contactless smartcard product based on the T6ND1 IC.

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 3) Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247]. Large parts English translation PP are a literal copy in this ST and if not stated otherwise clearly marked in 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:

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

TOSHIBA
Leading Innovation

TAP	Terminal Authentication Protocol

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-AAJePassport Security Target
Version:	Version 01.00.04
Date of issue:	24 February 2011
TOE identification:	TOSMART-P080-AAJePassport
TOE version:	Version 01.06.04 + NVM Ver.01.00.00
Produced by:	TOSHIBA CORPORATION Social Infrastructure Systems Company

Evaluation Assurance Level: EAL4 augmented with AVA_VAN.5, ALC_DVS.2 and ASE_TSS.2

Application note 1.

For interoperability reasons it is assumed that the receiving state cares for sufficient measures against eavesdropping within the operating environment of the inspection systems and uses the Active Authentication. If the receiving state only uses Basic Access Control to read these less sensitive assets (e.g. the personal data of the MRTD holder which is also printed on the physical MRTD) only AVA_VAN.3 applies for some specific attacks, due to keying weakness in the Basic Access Control protocol.

2.2. TOE overview

The TOE is a composite security IC, consisting of the hardware T6ND1, 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 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 Active Authentication, Basic Access Control, and

facilitates Passive Authentication. 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. It is possible to get the sensitive data with checking the data's integrity by using CRC checksum.
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)
- The Software random wait
- Checking the ROM CRC
- 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).

- Triple DES
- RSA
- SHA

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 organization 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:

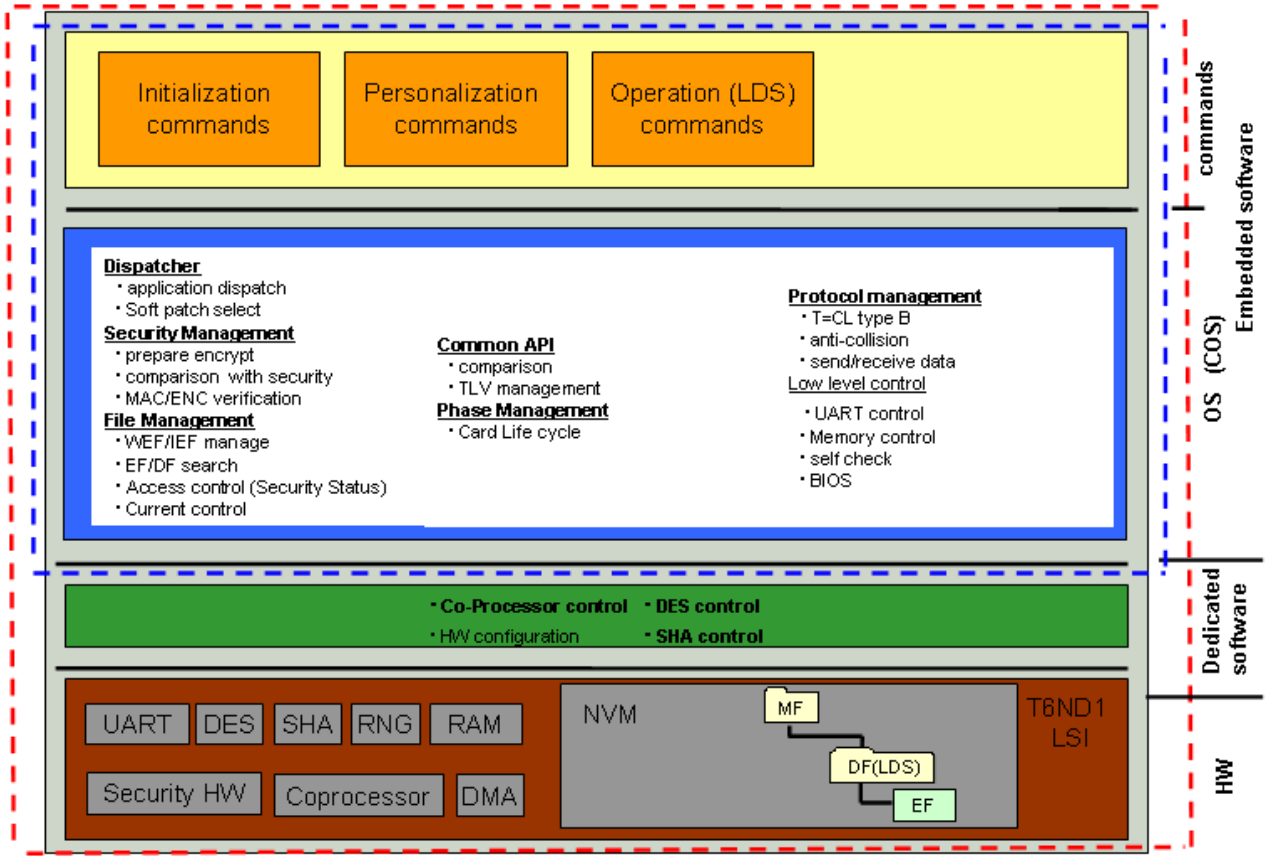

Figure 1 TOE scope (marked by red dashed line) and part additional to hardware (marked by blue dashed line)

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 but are part of this composed TOE. However, in this TOE these components fulfil no security relevant role for the TOE and therefore the antenna is out of the evaluation scope of this TOE.

2.3.2. TOE Delivery

Delivery item type	Identifier	Version	Medium
Hardware	T6ND1	#5.0	Sheet
Software	MRTD＋OS	Ver.01.06.04 With NVM Ver.01.00.00	ROM and NV memory of hardware (user area)
Guidance (for personalization agent)	Guidance Document for Personalization agent	MC-SJ0046-02	Document / pdf
	Preparative guidance	MC-SJ0045-01	Document / pdf
	Application Specification	MC-SM0914-02	Document / pdf
	Personalization Manual for ********	MC-SJ0047-03	Document / pdf
	AA Personalization Manual for ********	MC-SJ0048-03	Document / pdf
	Authentication Manual using ********	MC-SJ0049-03	Document / pdf
	Authentication Manual using MUTUAL AUTHENTICATE command	MC-SJ0050-03	Document / pdf
	Authentication Manual using BAC	MC-SJ0051-03	Document / pdf
	Personalization Specification	MC-SM0812-03	Document / pdf
	Procedural Request of Security Products Delivery and Receipt	MB-ICCARD-W471	Document / pdf

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 and the Data Encryption of 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.

This Security Target addresses 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 Access Keys.

(iii) An access control by the TOE to allow reading data (except for the sensitive biometric data) only to successfully authenticated authorized inspection systems

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 following functionality is provided by the software building upon what was already provided by the hardware on which the software builds.

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:
  - o Enabling the hardware countermeasures
  - o Anti-perturbation countermeasures

2.3.4. Life cycle Boundaries of the TOE

Following [PP-C0247], 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 either take place as 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 conformant and CC Part 3 conformant.

This Security Target claims conformance to Common Criteria Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247] 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.

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

3.2. Conformance claim rationale

The PP-TOE is a MRTD ePassport and that the composite TOE is a MRTD ePassport (with active authentication).
The PP [PP-C0247] requires strict compliance.

4. Security problem definition

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

The Assumptions, Threats and Organisational Security Policies are completely taken from the Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247]. Text in this chapter are taken from English PP [PP-C0247EN].

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, objects and operations to be used in the ST.

4.1.1. Subjects

The subjects in the following table are defined by this ST.

Table 4-1: Subjects

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 the 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 define in [ICAO_9303]
Terminal	A terminal is any technical system communicating with the TOE through the contactless interface
Inspection System	The 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 additional the Chip Authentication Mechanism. The Extended Inspection System (EIS) is in addition to the General Inspection System (i) implements the Terminal Authentication protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.
MRTD Holder	The rightful holder of the MRTD for whom the issuing state or Organization personalized the MRTD.
Traveller	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder
Attacker	A threat agent trying (i) to identify and to trace the movement of the MRTD's chip remotely (i.e. without known the or optically reading the physical MRTD) (ii) to read or to manipulate the logical MRTD without authorization,. Or (iii) forge a genuine MRTD.

4.2. Assumptions about operational environment of TOE

Since this Security Target claims conformance to the Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247], the assumptions defined in section 3.3 of the Protection Profile are valid for this Security Target. The following table lists the assumptions of the Protection Profile [PP-C0247].

Table 4-2: Assumptions defined in the Protection Profile for IC for ePassport - Active Authentication Support -

Assumptions
A.Administrative_Env

A.PKI

4.3. Description of Assets

Since this Security Target claims conformance to the Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247], the assets defined in section 1.2.3 of the Protection Profile are applied:

The information required for immigration procedure

The private key used for active authentication

4.4. Threats

Since this Security Target claims conformance to the Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247], the threats defined in section 3.1 of the Protection Profile are valid for this Security Target. The following table lists the threats of the Protection Profile.

Table 4-3, Threats defined in the Protection Profile for IC for ePassport - Active Authentication Support -.

Treats
T.Copy
T.Logical_Attack
T.Physical_Attack

4.5. Organizational Security Policies

Since this Security Target claims conformance to the Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247], the Organisational Security Policies defined in section 3.2 of the Protection Profile 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 Protection Profile for IC for ePassport - Active Authentication Support -.

OSP
P.BAC
P.Authority
P.Data_Lock

P.Prohibit

5. Personalization/Initialization Security Objectives

This chapter provides the statement of security objectives and the security objective rationale. For this chapter the Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247] 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.
Text in this chapter are taken from English PP [PP-C0247EN].

5.1. TOE Security Objectives

The TOE shall provide the following security objectives, taken from the Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247]. The following table lists the security objectives for the TOE of the Protection Profile.

Table 5-1: Security objectives for the TOE defined in the Protection Profile for IC for ePassport - Active Authentication Support -.

Security objectives for the TOE
O.AA
O.Logical_Attack
O.Physical_Attack
O.BAC
O.Authority
O.Data_Lock

5.2. Security Objectives for the operational environment

According to the Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247], the following security objectives for the environment are specified.

Table 5-1, Security objectives for the Environment defined in the Protection Profile for IC for ePassport - Active Authentication Support -.

Security objective for the operational environment
OE.Administrative_Env
OE.PKI

5.3. Security objectives rationale

In Table 5-4 each security objective for the TOE is traced back to threats countered by that security objective and OSPs enforced 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.Copy	O.AA	See PP
T.Physical_Attack	O.Physical_Attack	See PP
T.Logical_Attack	O.Logical_Attack	See PP
P.BAC	O.BAC	See PP
P.Authority	O.Authority	See PP
P.Data_Lock	O.Data_Lock	See PP
P.Prohibit	O.Data_Lock	See PP
A.Administrative_Env	OE.Administrative_Env	See PP
A.PKI	OE.PKI	See PP

6. Security Requirements

This chapter presents the statement of security requirements for the TOE and the security requirements rationale. This chapter applies the Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247].

Text in this chapter are taken from English PP [PP-C0247EN].

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

The SFRs are split in two categories, the SFRs from the Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247] that are incorporated by reference in this Security Target.

6.2.1. SFRs from the Protection Profile for IC for ePassport - Active Authentication Support -

Table 6-1, Security Functional Requirements taken from the Protection Profile for IC for ePassport - Active Authentication Support -.

Security functional requirements	Titles	Open operations
FCS_CKM.1	Cryptographic key generation	
FCS_CKM.4	Cryptographic key destruction	[selection: cryptographic key deletion on the volatile memory due to power disconnection and overwrite of new cryptographic key data, [assignment: other cryptographic key destruction methods]]
FCS_COP.1a	Cryptographic Operation (Active Authentication)	[assignment: cryptographic algorithm] [assignment: cryptographic key length]
FCS_COP.1m	Cryptographic Operation (Mutual Authentication)	
FCS_COP.1s	Cryptographic Operation (Secure Messaging)	
FDP_ACC.1a	Subset Access Control (Issue Processing)	
FDP_ACC.1b	Subset Access Control (Basic Access Control)	
FDP_ACF.1a	Security Attribute Based Access Control (Issue Processing)	
FDP_ACF.1b	Security Attribute Based Access Control (Basic Access Control)	

FDP_ITC.1	Import of User Data without Security Attributes	[assignment: issue processing access control SFP] [assignment: link a file to be written to the data as shown in the "allowed access" in Table 3-1 of, the organizational security policy, P.Authority]
FDP_UCT.1	Basic Data Exchange Confidentiality	
FDP_UIT.1	Data Exchange Integrity	
FIA_AFL.1a	Authentication Failure Handling (Active Authentication Information Access Key)	[assignment: positive integer number]
FIA_AFL.1d	Authentication Failure Handling (Transport Key)	[assignment: positive integer number]
FIA_AFL.1r	Authentication Failure Handling (Read Key)	[assignment: positive integer number]
FIA_UAU.2	User Authentication before Action	
FIA_UAU.4	Single-use Authentication Mechanisms	
FIA_UAU.5	Multiple Authentication Mechanisms	
FIA_UID.2	User Identification before Action	
FMT_MTD.1	Management of TSF Data	
FMT_SMF.1	Specification of Management Functions	
FMT_SMR.1	Security Roles	
FPT_PHP.3	Resistance to Physical Attack	
FTP_ITC.1	Inter-TSF Trusted Channel	

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).

Table 6-1 lists the Security Functional Requirements that are directly taken from the Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247] including all open assignment and selection operations.

Completion of operations from the Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247] is as follows:

FCS_CKM.4 Cryptographic key destruction – MRTD

FCS_CKM.4.1/ MRTD	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.1a Cryptographic operation (Active Authentication)

FCS_COP.1.1a	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 for data for active authentication
Assignment cryptographic algorithm	RSA
Assignment: cryptographic key sizes	1024bit, 1280bit, 1536bit, 1792bit, 2048bit
Assignment: list of standards	the digital signature standard (conforming to ISO/IEC 9796-2:2002 Digital signature scheme 1) used for the active authentication provided by ICAO Doc9303 Part1

FIA_AFL.1a Authentication Failure Handling (Active Authentication Information Access Key)

FIA_AFL.1.1	The TSF shall detect when **[selection:[assignment:positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]**

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

	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	authentication with the active authentication information access key
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [Selection: met, surpassed], the TSF shall **[assignment: list of actions].**
Selection: met, surpassed	Met or surpassed
Assignment: list of actions	permanent termination of authentication with the active authentication information access key (the state of the authentication with the active authentication information access key is fixed to be “Without authentication”)

FIA_AFL.1d Authentication Failure Handling (Transport Key)

FIA_AFL.1.1	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	authentication with the transport key
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [Selection: met, surpassed], the TSF shall **[assignment: list of actions].**
Selection: met, surpassed	Met or surpassed

Assignment: list of actions	permanent termination of the authentication with the transport key (the state of the authentication with the transport key is fixed to be “Without authentication”)

FIA_AFL.1r Authentication Failure Handling (Read Key)

FIA_AFL.1.1	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	authentication with the read key
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [Selection: met, surpassed], the TSF shall **[assignment: list of actions].**
Selection: met, surpassed	Met or surpassed
Assignment: list of actions	permanent termination of the authentication with the read key (the state of the authentication with the read key is fixed to be “Without authentication”)

6.3. 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.

6.4. Explicitly stated requirements

See [PP-C0247] Chapter 6.2.

6.5. Security Requirements Rationale

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

6.5.1. The SFRs meet the Security Objectives for the TOE

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

Security Objectives for the TOE	SFRS	Rationale
O.Logical_Attack	FDP_ACC.1b, FDP_ACF.1b	See PP
O.Physical_Attack	FPT_PHP.3	See PP
O.AA	FCS_COP.1a, FDP_ACC.1a, FDP_ACF.1a, FDP_ITC.1	See PP
O.BAC	FCS_CKM.1, FCS_CKM.4, FCS_COP.1m, FCS_COP.1s, FDP_ACC.1b, FDP_ACF.1b, FDP_UCT.1, FDP_UIT.1, FDP_ITC.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.5, FIA_UID.2, FTP_ITC.1	See PP
O.Authority	FDP_ACC.1a, FDP_ACF.1a, FDP_ITC.1, FIA_UAU.2, FIA_UAU.5, FIA_UID.2, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1	See PP
O.Data_Lock	FIA_AFL.1a, FIA_AFL.1d, FIA_AFL.1r	See PP

6.5.2. Reason for choosing Security Assurance Requirements

The Security Assurance Requirements have been chosen to meet the requirements of [PP-C0247]. 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.

6.5.3. All dependencies have been met

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

Table 6-7, Dependencies of SFRs.

SFR	Dependencies	Fulfillment of dependencies

FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 cryptographic operations], FCS_CKM.4 cryptographic key destruction	Covered by the PP
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 the PP
FCS_COP.1a	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Covered by the PP
FCS_COP.1m	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key	Covered by the PP

	generation] FCS_CKM.4 Cryptographic key destruction	
FCS_COP.1s	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Covered by the PP
FDP_ACC.1a	FDP_ACF.1 Security attribute based access control	Covered by the PP
FDP_ACC.1b	FDP_ACF.1 Security attribute based access control	Covered by the PP.
FDP_ACF.1a	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	Covered by the PP
FDP_ACF.1b	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	Covered by the PP
FDP_ITC.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	Covered by the PP
FDP_UCT.1	[FTP_ITC.1 Inter-TSF	Covered by the

	trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	PP
FDP_UIT.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	Covered by the PP
FIA_AFL.1a	FIA_UAU.1 Timing of authentication	Covered by the PP
FIA_AFL.1d	FIA_UAU.1 Timing of authentication	Covered by the PP
FIA_AFL.1r	FIA_UAU.1 Timing of authentication	Covered by the PP
FIA_UAU.2	FIA_UID.1 Timing of identification	Covered by the PP
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a.
FIA_UID.2	No dependencies	n.a.
FMT_MTD.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Covered by the PP
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Covered by the PP
FPT_PHP.3	No dependencies	n.a.
FTP_ITC.1	No dependencies	n.a.

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 FPT_PHP.3, FCS_COP.1[DES], FCS_COP.1[RSA].
The other platform-TSF (IP-TSF) FRU_FLT.2, FPT_FLS.1, FMT_LIM.1, FMT_LIM.2, FAU_SAS.1, FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FCS_RNG.1, FCS_COP.1[DH], FCS_COP.1[SHA], FCS_COP.1[ECDSA] and FCS_COP.1[ECDH] 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 and [HW-ST] are both written for general smartcard environment with secure initialization and personalization process.

Assumption A.Plat-Appl from [HW-ST] is fulfilled automatically, due to strict conformance to the PP's: "1.2.3 Life Cycle of TOE" of [PP-C0247] 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

Self-Protection [FPT_PHP.3] is implemented by the underlying hardware platform. For detailed protection provided through the hardware LSI refer to [HW_ST].

7.2.2. Random numbers

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.1a, FCS_COP.1m and FCS_COP.1s. All these cryptographic operations are implemented by the certified crypto library and underlying hardware platform [HW-ST].

7.2.4. Chip authentication proof

The cryptographic operations (FCS_COP.1a, FCS_COP.1m and FCS_COP.1s) are implemented by the underlying hardware platform. The random number generation is also implemented by the underlying platform.

The SFRs FCS_COP.1a is 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 FIA_UID.2 and FIA_UAU.2.

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. 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 (FIA_UID.2 and FIA_UAU.2)

Authentication during Personalization relates to the SFRs FIA_UAU.4, FIA_UAU.5, FMT_SMF.1, FMT_SMR.1, FIA_AFL.1a, FIA_AFL.1d and FIA_AFL.1r.

The SFRs, FCS_COP.1a, FCS_COP.1m and FCS_COP.1s are implemented by the underlying hardware platform.

The personalization agent must use method to authenticate to the TOE during personalization.
If the authentication during personalization fails three times the TOE blocks permanently (FIA_AFL.1a, FIA_AFL.1d and FIA_AFL.1r).

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).
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.

Access control of TOE conforms to “Table 3-1 TOE Internal Information Access Control by Passport Issuance Authority” in [PP-C0247] (FDP_ITC.1).

7.2.6. Data integrity

The integrity of personal data relates to the SFRs FCS_CKM.1, FCS_CKM.4, FCS_COP.1s, FIA_UID.2, FIA_UAU.2, FIA_UAU.4, FIA_UAU.5, FDP_ACC.1a, FDP_ACF.1a, FDP_UIT.1, FMT_SMF.1, FMT_SMR.1 and FMT_MTD1.

The SFRs FCS_CKM.1, FCS_COP.1a, FCS_COP.1m and FCS_COP.1s 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, FDP_ACC.1a, FDP_ACF.1a, FIA_UID.2, FIA_UAU.2).

Other user roles like the Inspection systems are only allowed to read the data after successful appropriate authentication (FMT_MTD.1, FDP_ACC.1b, FDP_ACF.1b, FIA_UID.2, FIA_UAU.2, FIA_UAU.5 and FIA_UAU.4). Furthermore, is a secure messaging used to communicate between the TOE and the authenticated Inspection System (FDP_UCT.1, FDP_UIT.1 and FTP_ITC.1). After use the session keys are destroyed using (FCS_CKM.4) to all '00' , when an error occurs in Basic Access Control processor when an error in secure messaging.

7.2.7. Data confidentiality

The data confidentiality relates to the SFRs FCS_CKM.1, FCS_CKFM.4, FCS_COP.1s, FIA_UID.2, FIA_UAU.2, FIA_UAU.4, FIA_UAU.5, FDP_ACC.1b, FDP_ACF.1b, FDP_UCT.1, FDP_UIT.1, FMT_SMF.1, FMT_SMR.1 and FMT_MTD.1.

The cryptographic SFRs and Random number generator implemented by the underlying hardware platform (FCS_COP.1s).

For the data confidentiality the TOE distinguishes two levels namely after personalization the successfully authenticated Basic Inspection System is allowed to read EF.DG1 to EF.DG16. This distinction and access control is mandated by the SFRs (FDP_ACC.1b and FDP_ACF.1b)

After successful authentication both using Basic Access Control (FCS_CKM.1, FCS_COP.1m, FIA_UAU.4, FIA_UAU.5), secure messaging is used when the TOE is communicating with the Inspection System. (FCS_COP.1s, FDP_UCT.1, FDP_UIT.1 and FTP_ITC.1). The session keys are destroyed after use (FCS_CKM.4) to all '00, when an error occurs in Basic Access Control process or an error in secure messaging.

If authentication fails on the MUTUAL AUTHENTICATE of Basic Access Control, the card returns error status.

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. The non-bypassibility by the hardware component refer 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-C0247EN]	Protection Profile for ePassport IC with Active Authentication	February 15, 2010	1.00	Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan JBMIA	

[PP-C0247]	旅券冊子用 IC のためのプロテクションプロファイル –能動認証対応–	2010年2月15日	第1.00版	外務省領事局旅券課 JBMIA	JISEC C0247
[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	
[HW_ST]	T6ND1 series Integrated Circuit with Crypto Library v1.0 Security Target	28.Dec.2010	Version 2.16	Toshiba	CC-T6ND1-ST-ENG
[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)	

End of Document