

TOSMART-GP1with Supplemental Access Control (PACE) and Active Authentication Security Target

July 9, 2025

Version01.01.11

Smart Card Development Group
Card Security Systems Department
Komukai Complex
Toshiba Infrastructure Systems & Solutions Corporation

Change History

No	Version	Date	Chapter	Content	Name
01	00.09.00	2016-10-26		New Draft Release	TOSHIBA
02	01.00.00	2017-02-20		Rev.00	TOSHIBA
03	01.00.01	2017-03-21	All	EOR comment reflection.	TOSHIBA
04	01.00.02	2017-05-19	All	EOR comment reflection.	TOSHIBA
05	01.00.03	2017-08-22	All	EOR comment reflection.	TOSHIBA
06	01.00.04	2017-10-13	2.3.2	EOR comment reflection.	TOSHIBA
07	01.00.05	2018-01-11	2.3.2	EOR comment reflection.	TOSHIBA
08	01.01.00	2023-03-02	All	Rev.06	TOSHIBA
09	01.01.01	2023-08-10	All	Rev.07	TOSHIBA
10	01.01.02	2023-08-31	All	Rev.08	TOSHIBA
11	01.01.03	2023-09-22	All	Rev.09	TOSHIBA
12	01.01.04	2023-11-20	All	Rev.10	TOSHIBA
13	01.01.05	2023-12-08	All	Rev.11	TOSHIBA
14	01.01.06	2023-12-19	All	Rev.12	TOSHIBA
15	01.01.07	2024-01-30	2.1	Rev.13	TOSHIBA
16	01.01.08	2024-03-27	2.3.2	Rev.14	TOSHIBA
17	01.01.09	2024-09-18	All	Rev.15	TOSHIBA
18	01.01.10	2025-01-07	2.3.2	Rev.16	TOSHIBA
19	01.01.11	2025-07-09	All	Rev.17	TOSHIBA

Table of contents

1.	Introduction	5
1.1.	Common Criteria requirements.....	5
1.2.	Definitions and abbreviations.....	5
2.	ST introduction	6
2.1.	ST and TOE identification.....	6
2.2.	TOE overview.....	6
2.3.	TOE description.....	7
2.3.1.	Physical scope of the TOE.....	7
2.3.2.	TOE Delivery.....	9
2.3.3.	Logical scope of the TOE.....	10
2.3.4.	Life cycle Boundaries of the TOE.....	11
3.	Conformance claim and rationale	12
3.1.	Conformance claim.....	12
3.2.	Conformance claim rationale.....	12
4.	Security problem definition	13
4.1.	Definition of subjects, objects and operations	13
4.1.1.	Subjects	13
4.2.	Assumptions about operational environment of TOE.....	14
4.3.	Description of Assets.....	15
4.4.	Threats.....	15
4.5.	Organizational Security Policies.....	15
5.	Security Objectives	16

5.1.	Security Objectives for the TOE.....	16
5.2.	Security Objectives for the operational environment.....	16
5.3.	Security objectives rationale.....	17
6.	Extended Component Definition	17
7.	Security Requirements	18
7.1.	Definitions.....	18
7.2.	Security Functional Requirements.....	18
7.2.1.	SFRs from the Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication-	19
7.3.	TOE Security Assurance Requirements.....	23
7.4.	Explicitly stated requirements.....	23
7.5.	Security Requirements Rationale.....	24
7.5.1.	The SFRs meet the Security Objectives for the TOE.....	24
7.5.2.	Reason for choosing Security Assurance Requirements	24
7.5.3.	All dependencies have been met.....	24
8.	TOE Summary Specification	26
8.1.	Statement of Compatibility.....	26
8.1.1.	Security Functional Requirements.....	26
8.1.2.	Security Objectives.....	27
8.1.3.	Conclusion	28
8.2.	TOE meets the SFRs.....	29
8.2.1.	Self-Protection of the TOE.....	29
8.2.2.	Random numbers.....	29
8.2.3.	Cryptographic operations.....	29
8.2.4.	Active Authentication.....	31
8.2.5.	Identification and Authentication.....	31
8.2.6.	Data integrity.....	32
8.2.7.	Data confidentiality.....	32

9. Reference 34

1. Introduction

This document is the Security Target for the contactless smartcard product based on the IFX_CCI_000005h H13 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 5) Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication - [PP-C0499]. Large parts of 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 (=Flash Memory)
MMU	Memory Management Unit
BAC	Basic Access Control
PA	Passive Authentication
AA	Active Authentication

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-GP1 with Supplemental Access Control
(PACE) and Active Authentication Security Target

Version: Version 01.01.11

Date of issue: 9 July 2025

TOE identification: TOSMART-GP1 V01.01.00 (Supporting PACE PP-0499)

TOE Software version: Version 01.01.02

Produced by: Smart Card Development Group
Card Security Systems Department Komukai Complex
Toshiba Infrastructure Systems & Solutions Corporation

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

2.2. TOE overview

The TOE is a composite security IC, consisting of the hardware IFX_CCI_000005h H13, which is used as the evaluated underlying platform and the ePassport (OS and application) software, which is built on this hardware platform. The IFX_CCI_000005h H13 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 (RAM, Flash 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 ePassport.

The ePassport consists of a secure operating system and application on top of the IFX_CCI_000005h H13. The operating system contains the embedded software functions used by the ePassport application.

The ePassport application provides Active Authentication, Password Authenticated Connection Establishment, and facilitates Passive Authentication.

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).

- SHA-384, SHA-256 / SHA-1
- AES(128)、AES(256)
- ECDSA(256)、ECDSA(384)、ECDH(256)、ECDH(384)

The TOE provides the security functions, including

- Write protection function (protection on writing data after issuing a passport);
- Protection function in transport (protection against attacks during transport before issuing the TOE(i.e. Transport key lock)); and
- Tamper resistance (protection against confidential information leak due to physical attacks)

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

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.

Even though the antenna and capacitors do not supply security features, they are needed to enable contactless interface to the ePassport IC.

2.3. TOE description

The TOE is ePassport IC (including necessary software). This ePassport IC is composed of IC chip hardware with the contactless communication interface, and basic software (operating system) and ePassport application program that are installed in the said hardware (hereinafter, the term "IC chip" shall mean the "ePassport IC"). An external antenna is connected to the IC chip for contactless communication purpose, and the IC chip is embedded in the plastic sheet together with the antenna to constitute a portion of a passport booklet.

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:

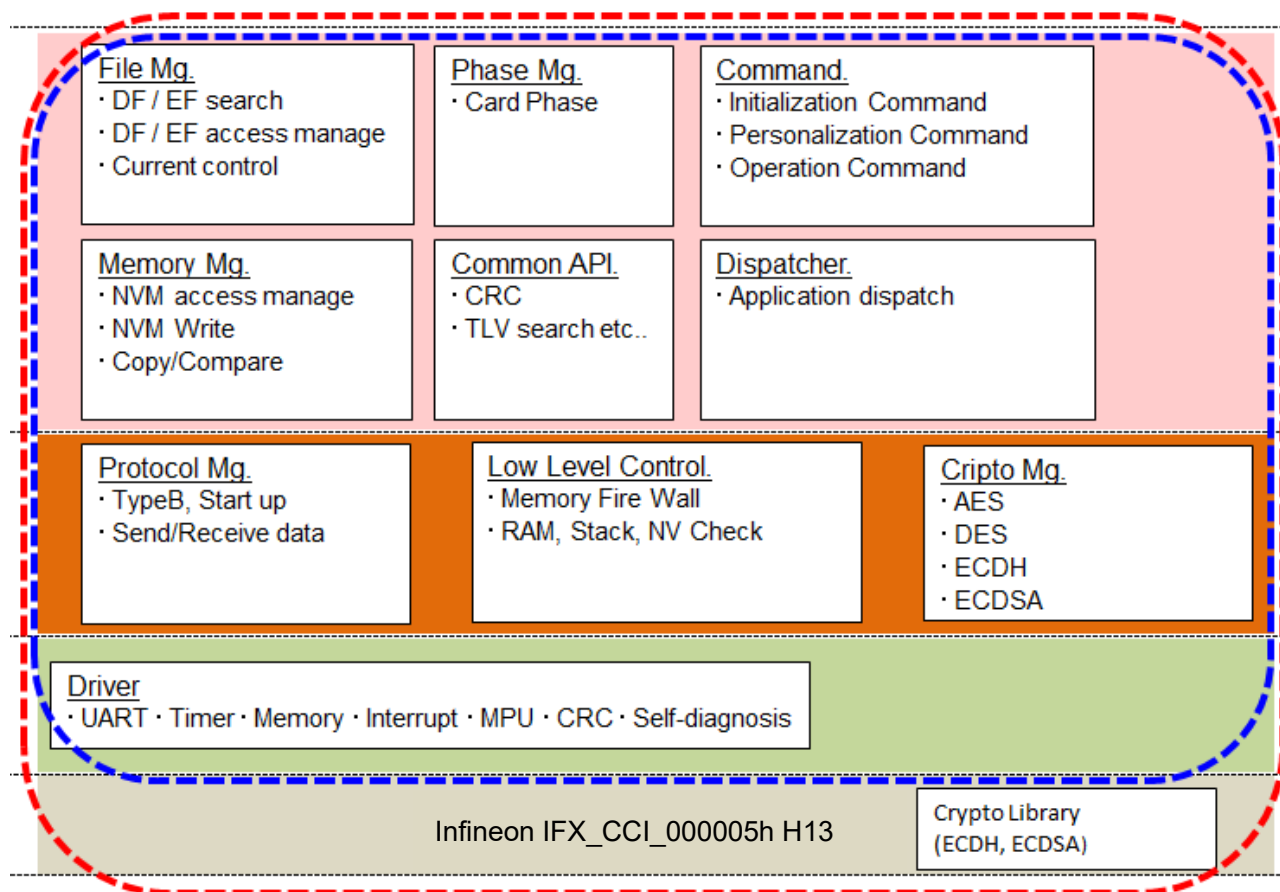


Figure 1 TOE scope (marked by red dashed line) and part additional to hardware (marked by blue dashed line)

The ePassport (OS and ePassport application) consists of a binary package that is implemented in the User Flash memory of the IFX_CCI_000005h H13. It can be divided in two layers, namely the OS providing a number of services to the other layer the application with commands.

The IFX_CCI_000005h H13 provides the computing platform and cryptographic support by means of co-processors and crypto library for the ePassport (OS and application) dedicated software. The IFX_CCI_000005h H13 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 IFX_CCI_000005h H13 hardware. These components fulfil no security relevant role for the TOE and therefore the antenna and capacitors are out of the evaluation scope of this TOE.

2.3.2. TOE Delivery

Delivery item type	Identifier	Version	Medium	Shipment method
Hardware	IFX_CCI_000005h H13 (Common criteria certification identifier)	FW-Identifier 80.100.17.0	Sheet	Secure courier
	0013H 0016H 0000H (Chip Type)			
CL52 Asymmetric Crypto Library for Crypto@2304T	CI52-LIB-base-XSMALL-HUGE.lib	v2.06.003		Infineon web site
CL52 Asymmetric Crypto Library for Crypto@2304T	CI52-LIB-ecc-XSMALL-HUGE.lib	v2.06.003		Infineon web site
CL52 Asymmetric Crypto Library for Crypto@2304T	CI52-LIB-toolbox-XSMALL-HUGE.lib	v2.06.003		Infineon web site
Hardware Support Library for SLCx2	HSL-01.22.4346-SLCx2_C65.lib	v1.22.4346		Infineon web site
Software	ePassport application + OS	Ver.01.01.02	Flash memory of hardware (user area)	Infineon web site (*1), CD-R (*2)
Delivery item type	Identifier	Document No. / Version	Medium	Shipment method
Guidance (for personalization agent)	Guidance Document for Personalization agent (USR)	MC-SM1911 / Version 01.01.01	Document / pdf	CD-R
	Preparative guidance (PRE)	MC-SM1905 / Version 01.01.00	Document / pdf	CD-R
	Application Specification	MC-SM1917 / Version 1.1.3	Document / pdf	CD-R
	Authentication Manual using VERIFY command	MC-SJ0131 / Version 01.01.03	Document / pdf	CD-R
	Personalization Specification	MC-SM1895 / Version 1.1.2	Document / pdf	CD-R
	Procedural Request of Security Product Delivery and Receipt	MB-ICCARD-W471 / Version 1.0.4	Document / pdf	CD-R

*1 : Program Download by Infineon

*2 : Program Download by TOSHIBA

2.3.3. Logical scope of the TOE

2.3.3.1. Description of the ePassport functionality

A passport is an identification document, issued by each country's government or equivalent public organization, which certifies, for the purpose of international travel, the identity of its holder, generally in a booklet form (passport booklet). The International Civil Aviation Organization (ICAO) of the United Nations has provided the passport booklet guidelines. As for conventional passports, all information necessary as the identification was printed on a paper booklet, and thereby this could cause these passports to be forged for illicit purposes. In order to prevent such forgery, an IC chip containing personal information with digital signature has been incorporated in a passport booklet. Since valid digital signature can be granted only by the official passport issuing authorities, a high level of forgery prevention effect can be achieved. However, digital signature is not enough to counter forgery of copying personal information with authorized signature to store such information on a different IC chip.

This type of forgery attack can be countered by adding the Active Authentication function to the IC chip and verifying the authenticity of the IC chip with the use of the said function.

The TOE is embedded in a plastic sheet and then interfiled in a passport booklet. At immigration, the immigration official inspects the passport booklet using a passport inspection terminal (hereinafter a "terminal"). Aside from the information printed on the passport booklet in ordinary characters, the same information is encoded, printed on the machine readable zone (MRZ) of the passport booklet, and read by the optical character reader of the terminal. The information is digitized and is stored in the IC chip, i.e., the TOE. These digitalized data are read by the terminal through the contactless communication interface of the TOE. The digitalized data include facial images.

The antenna used for the TOE to perform contactless communication with the terminal is connected to the TOE in the plastic sheet. The TOE operates using wireless signal power supplied from the terminal.

The main security functions of the TOE are to protect data stored in the TOE from illicit reading or writing. The operation of the security functions applied to contactless communication with the terminal shall comply with the PACE, and Active Authentication specifications defined by Part 11 of Doc 9303.

Attacks on protected data in the TOE include those through the contactless communication interface of the TOE and those attempting to disclose internal confidential information (Active Authentication Private Key) through physical attacks on the TOE.

The TOE provides the main security functions, including

- PACE function(mutual authentication and Secure Messaging);
- Active Authentication support function (prevention of copying the IC chip);
- Write protection function (protection on writing data after issuing a passport);
- Protection function in transport (protection against attacks during transport before issuing the TOE(i.e. transport key lock)); and
- Tamper resistance (protection against confidential information leak due to physical attacks)

The TOE also 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 ECDSA 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.

In addition to the IFX_CCI_000005h H13 hardware platform and crypto library, the TOE-Software implements a file system compliant with [JICSAP], 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 IFX_CCI_000005h H13 and crypto library.

- Destruction of the cryptographic keys after usage (FCS_CKM.4)
- Implementation of the IFX_CCI_000005h H13 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-C0499], 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).

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 5 April 2017. Furthermore it claims to be CC Part 2 extended and CC Part 3 conformant.

This Security Target claims conformance to Common Criteria Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication- [PP-C0499] CC version 3.1.

This Security Target is conforming to assurance package EAL4, augmented with ALC_DVS.2, AVA_VAN.5.

This Security Target also refers to the IFX_CCI_000005h H13 Security Target, which is compliant to the IC platform protection profile [PP-0084].

3.2. Conformance claim rationale

The PP-TOE is a ePassport and that the composite TOE is a ePassport (with Active Authentication).

The PP [PP-C0499] 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 ePassport IC with Supplemental Access Control (PACE) and Active Authentication - [PP-C0499]. Texts in this chapter are taken from English PP [PP-C0499EN].

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 ePassport manufacturer completing the IC to the ePassport'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 ePassport manufacturer using the role Manufacturer
Personalization Agent	<p>The agent is acting on behalf of the issuing State or Organization to personalize the ePassport for the holder by some or all of the following activities:</p> <ul style="list-style-type: none"> (i) establishing the identity of the holder for the biographic data in the ePassport, (ii) enrolling the biometric reference data of the ePassport 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 ePassport 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]
Terminal	A terminal is any technical system communicating with the TOE through the contactless interface
Inspection System	<p>The technical system used by the border control officer of the receiving State</p> <ul style="list-style-type: none"> (i) examining an ePassport presented by the traveller and verifying its authenticity and (ii) verifying the traveller as ePassport holder.

<p>The Basic Inspection System (BIS)</p> <ul style="list-style-type: none"> (i) contains a terminal for the contactless communication with the ePassport's chip (ii) implements the terminals part of the Basic Access Control Mechanism and Supplemental Access Control (PACE) Mechanism and (iii) gets the authorization to read of the logical ePassport under the Basic Access Control by optical reading the ePassport or other parts of the passport book providing this information. <p>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</p> <ul style="list-style-type: none"> (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. 	
ePassport Holder	The rightful holder of the ePassport for whom the issuing state or Organization personalized the ePassport.
Traveller	Person presenting the ePassport to the inspection system and claiming the identity of the ePassport holder
Attacker	<p>A threat agent trying</p> <ul style="list-style-type: none"> (i) to identify and to trace the movement of the ePassport's chip remotely (i.e. without known the or optically reading the physical ePassport) (ii) to read or to manipulate the logical ePassport without authorization,. Or (iii) forge a genuine ePassport.

4.2. Assumptions about operational environment of TOE

Since this Security Target claims conformance to the Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication - [PP-C0499], 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-C0499].

Table 4-2: Assumptions defined in the Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication -

Assumptions
A.Administrative_Env
A.PKI

4.3. Description of Assets

Since this Security Target claims conformance to the Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication - [PP-C0499], 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 ePassport IC with Supplemental Access Control (PACE) and Active Authentication - [PP-C0499], 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 ePassport IC with Supplemental Access Control (PACE) and Active Authentication -.

Treats
T.Copy
T.Logical_Attack
T.Communication_Attack
T.Physical_Attack

4.5. Organizational Security Policies

Since this Security Target claims conformance to the Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication - [PP-C00499], 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 ePassport IC with Supplemental Access Control (PACE) and Active Authentication -.

OSP
P.PACE

P.Authority
P.Data_Lock
P.Prohibit

5. Security Objectives

This chapter provides the statement of security objectives and the security objective rationale. For this chapter the Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication - [PP-C0499] 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.

Texts in this chapter are taken from English PP [PP-C0499EN].

5.1. Security Objectives for the TOE

The TOE shall provide the following security objectives, taken from the Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication - [PP-C0499]. 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 ePassport IC with Supplemental Access Control (PACE) and Active Authentication.

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

5.2. Security Objectives for the operational environment

According to the Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication - [PP-C0499], the following security objectives for the environment are specified.

Table 5-2, Security objectives for the Environment defined in the Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication -

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

5.3. Security objectives rationale

In Table 5-3 each security objective for the TOE is traced back to threats countered by that security objective and OSPs enforced by that security objective.

Table 5-3, 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
T.Communication_Attack	O.PACE	See PP
P.PACE	O.PACE	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. Extended Component Definition

This chapter presents the extended components for the TOE.

This chapter applies the Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication - [PP-C0499].

Texts in this chapter are taken from English PP [PP-C0499EN].

The following table lists the extended components for the TOE of the Protection Profile.

Table 6-1: Extended component for the TOE defined in the Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication -.

Extended components for the TOE	Each component is given a level
FCS_RND	FCS_RND.1

7. 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 ePassport IC with Supplemental Access Control (PACE) and Active Authentication - [PP-C0499].

Texts in this chapter are taken from English PP [PP-C0499EN].

7.1. Definitions

In the next sections the following the notation used

Whenever iteration and strike-through are denoted, using the same notation of the PP.

When the refinement, selection or assignment operation is used, these operations shown in bold.

7.2. Security Functional Requirements

The SFRs from the Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication - [PP-C0499] that are incorporated by reference in this Security Target.

7.2.1. SFRs from the Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication-

Table 7-1, List of Security Functional Requirements taken from the Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication -.

Security functional requirements	Titles	Open operations
FCS_CKM.1p	Cryptographic key generation (PACE, session keys)	
FCS_CKM.1e	Cryptographic key generation (PACE, ephemeral key pairs)	
FCS_CKM.4	Cryptographic key destruction	[selection: method for erasing cryptographic keys on volatile memory by shutting down power supply, overwriting new cryptographic key data, and [assignment: other cryptographic key destruction method]]
FCS_COP.1a	Cryptographic operation (Active Authentication, signature generation)	
FCS_COP.1h	Cryptographic operation (Active Authentication, hash functions)	
FCS_COP.1n	Cryptographic operation (Nonce encryption)	
FCS_COP.1e	Cryptographic operation (Key agreement)	
FCS_COP.1hp	Cryptographic operation (PACE, hash functions)	
FCS_COP.1mp	Cryptographic operation (PACE, mutual authentication)	
FCS_COP.1sp	Cryptographic operation (PACE, Secure Messaging)	
FCS_RND.1	Quality standards for random numbers	[assignment: defined quality standard]
FDP_ACC.1a	Subset access control (Issuance	

	procedure)	
FDP_ACC.1p	Subset access control (PACE)	
FDP_ACF.1a	Security attribute based access control (Issuance procedure)	
FDP_ACF.1p	Security attribute based access control (PACE)	
FDP_ITC.1	Import of user data without security attributes	
FDP_UCT.1p	Basic data exchange confidentiality (PACE)	
FDP_UIT.1p	Data exchange integrity (PACE)	
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 (Readout key)	[assignment: positive integer number]
FIA_UAU.1	Timing of authentication	
FIA_UAU.4	Single-use authentication mechanism	
FIA_UAU.5	Multiple authentication mechanisms	
FIA_UID.1	Timing of identification	
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 8.2.1).

Table 7-1 lists the Security Functional Requirements that are directly taken from the Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication - [PP-C0499] including all open assignment and selection operations.

Completion of operations from the Protection Profile for ePassport IC with Supplemental Access Control (PACE) and Active Authentication - [PP-C0499] is as follows:

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: selection: method for erasing cryptographic keys on volatile memory by shutting down power supply, overwriting new cryptographic key data, and [assignment: other cryptographic key destruction method]] that meets the following [assignment: none]
assignment: other cryptographic key destruction method	<i>Cryptographic key is destroyed by random number.</i>

FCS_RND.1 Quality standards for random numbers

FCS_RND.1.1	The TSF shall provide a random number generation mechanism that meets the following: [assignment : <i>defined quality standards</i>] .
Assignment defined quality standards	<i>Class PTG2 of the AIS31</i>

FIA_AFL.1a Authentication failure handling (Active Authentication Information Access Key)

FIA_AFL.1.1	The TSF shall detect when [selection:<i>[assignment: positive integer number]</i>, an administrator configurable positive integer within [assignment: range of acceptable values] unsuccessful authentication attempts occur related to [assignment: <i>list of authentication events</i>] .
Selection:[assignment: positive integer number]	3
assignment: list of authentication events	<i>authentication with the Active Authentication Information Access Key</i>
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [Selection: met, surpassed], the TSF shall [assignment: <i>list of actions</i>] .
Assignment: list of actions	<i>permanently stop authentication with the Active Authentication Information Access Key (fix the authentication status with the Active Authentication Information Access Key to "Not authenticated yet")</i>

FIA_AFL.1d Authentication failure handling (Transport key)

FIA_AFL.1.1	The TSF shall detect when [selection: <i>[assignment: positive integer number]</i>, an administrator configurable positive integer within [assignment: range of acceptable values] unsuccessful authentication attempts occur related to [assignment: <i>list of authentication events</i>] .
Selection:[assignment: positive integer number]	3
assignment: list of authentication events	<i>authentication with the transport key</i>
FIA_AFL.1.2	When the defined number of unsuccessful authentication

	attempts has been [Selection: <i>met</i> , <i>surpassed</i>], the TSF shall [assignment: <i>list of actions</i>] .
Assignment: list of actions	<i>permanently stop authentication with the transport key (fix the authentication status with the transport key to “Not authenticated yet”)</i>

FIA_AFL.1r Authentication failure handling (Readout key)

FIA_AFL.1.1	The TSF shall detect when [selection:<i>assignment: positive integer number</i>, <i>an administrator configurable positive integer within [assignment: range of acceptable values]</i>] unsuccessful authentication attempts occur related to [assignment: <i>list of authentication events</i>] .
Selection:[assignment: positive integer number]	3
assignment: list of authentication events	<i>authentication with the read key</i>
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [Selection: <i>met</i> , <i>surpassed</i>], the TSF shall [assignment: <i>list of actions</i>] .
Assignment: list of actions	<i>permanently stop authentication with the readout key (fix the authentication status with the readout key to “Not authenticated yet”)</i>

7.3. 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.

7.4. Explicitly stated requirements

See [PP-C0499] Chapter 6.2.

7.5. Security Requirements Rationale

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

7.5.1. 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.1p, FDP_ACF.1p	See PP
O.Physical_Attack	FPT_PHP.3	See PP
O.AA	FCS_CKM.4, FCS_COP.1a, FCS_COP.1h, FDP_ACC.1a, FDP_ACF.1a, FDP_ITC.1	See PP
O.PACE	FCS_CKM.1p, FCS_CKM.1.e, FCS_CKM.4, FCS_COP.1n, FCS_COP.1e, FCS_COP.1hp, FCS_COP.1mp, FCS_COP.1sp, FCS_RND.1, FDP_ACC.1p, FDP_ACF.1p, FDP_ITC.1, FDP_UCT.1p, FDP_UIT.1p, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UID.1, FTP_ITC.1	See PP
O.Authority	FDP_ACC.1a, FDP_ACF.1a, FDP_ITC.1, FIA_UAU.1, FIA_UAU.5, FIA_UID.1, 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

7.5.2. Reason for choosing Security Assurance Requirements

The Security Assurance Requirements have been chosen to meet the requirements of [PP-C0499]. This was augmented to provide the potential consumers of this TOE a clearer view on the protection provided against bypassing and modification of the TOE.

7.5.3. All dependencies have been met

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

Table 6-7, Dependencies of SFRs.

SFR	Dependencies	Fulfilment of dependencies
FCS_CKM.1p	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	Covered by the PP
FCS_CKM.1e	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	Covered by the PP
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Covered by the PP
FCS_COP.1a	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Covered by the PP
FCS_COP.1h	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Covered by the PP
FCS_COP.1n	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Covered by the PP
FCS_COP.1e	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Covered by the PP
FCS_COP.1hp	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Covered by the PP
FCS_COP.1mp	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Covered by the PP
FCS_COP.1sp	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Covered by the PP
FCS_RND.1	No dependencies	n.a.
FDP_ACC.1a	FDP_ACF.1	Covered by the PP
FDP_ACC.1p	FDP_ACF.1	Covered by the PP.
FDP_ACF.1a	FDP_ACC.1 FMT_MSA.3	Covered by the PP
FDP_ACF.1p	FDP_ACC.1 FMT_MSA.3	Covered by the PP
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.3	Covered by the PP
FDP_UCT.1p	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1]	Covered by the PP
FDP_UIT.1p	[FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1 or FTP_TRP.1]	Covered by the PP
FIA_AFL.1a	FIA_UAU.1	Covered by the PP
FIA_AFL.1d	FIA_UAU.1	Covered by the PP
FIA_AFL.1r	FIA_UAU.1	Covered by the PP
FIA_UAU.1	FIA_UID.1	Covered by the PP
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a.
FIA_UID.1	No dependencies	n.a.
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Covered by the PP
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1	Covered by the PP
FPT_PHP.3	No dependencies	n.a.
FTP_ITC.1	No dependencies	n.a.

8. TOE Summary Specification

8.1. Statement of Compatibility

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

8.1.1. Security Functional Requirements

Table 8-1, Mapping of SFRs for RP_SFR-SERV

Relevant Platform-SFR	Description	Correspondence in composite ST
FCS_COP.1/AES	"Cryptographic operation – AES"	FCS_COP.1sp, FCS_COP.1mp
FCS_COP.1/ECDSA-3	"Cryptographic Operation – ECDSA"	FCS_COP.1a
FCS_COP.1/ECDH-3	"Cryptographic Operation – ECDH"	FCS_COP.1e
FCS_RNG.1/TRNG	"Random number generation - TRNG"	FCS_RND.1
FCS_CKM.1/EC-3	"Cryptographic key management - EC"	FCS_CKM.1e
FPT_PHP.3	"Resistance to physical attack"	FPT_PHP.3

Table 8-2, Mapping of SFRs for RP_SFR-MECH

Relevant Platform-SFR	Description	Correspondence in composite ST
FDP_ACC.1	"Subset access control"	Memory access control [HW-ST] 7.1.3 is used by composite TOE.
FDP_ACF.1	"Security attribute based access control"	Memory access control [HW-ST] 7.1.3 is used by composite TOE.
FMT_MSA.3	"Static attribute initialisation"	Memory access control [HW-ST] 7.1.3 is used by composite TOE.

FMT_MSA.1	"Management of security attributes"	Memory access control [HW-ST] 7.1.3 is used by composite TOE.
FMT_SMF.1	"Specification of Management functions"	Memory access control [HW-ST] 7.1.3 is used by composite TOE.
FDP_SDI.2	"Stored data integrity monitoring and action"	Data integrity [HW-ST] 7.1.5 is used by composite TOE.
FPT_TST.2	"Subset TOE testing"	Subset of TOE testing [HW-ST] 7.1.2 is used by composite TOE.
FCS_RNG.1/DRNG	"Random number generation - DRNG"	DRNG [HW-ST] 7.1.1.1.3 is used by composite TOE.
FAU_SAS.1	"Audit storage"	Audit storage [HW-ST] 7.1.1.2 is used by composite TOE.
FMT_LIM.1/Loader	"Limited Capabilities"	Support of the Flash Loader [HW-ST] 7.2 is used by composite TOE. (*1)
FMT_LIM.2/Loader	"Limited Availability - Loader"	Support of the Flash Loader [HW-ST] 7.2 is used by composite TOE. (*1)

*1 : The Hex file is loaded to the IC sheet in Toshiba. Although a Flash Loader functionality is used in that case, this functionality is permanently deactivated when shipping as product.

Other platform SFR's are not used.

8.1.2. Security Objectives

Table 8-3, Mapping of security objectives for the TOE

Security Objectives of Platform	Corresponding Security Objectives of the TOE
O.Phys-Manipulation	O.Physical_Attack
O.Phys-Probing	O.Physical_Attack
O.Malfunction	O.Logical_Attack O.Physical_Attack

O.Leak-Inherent	O.Physical_Attack
O.Leak-Forced	O.Physical_Attack
O.Abuse-Func	O.Authority O.Data_Lock
O.RND	O.PACE
O.Cap_Avail_Loader	not relevant
O.Authentication	not relevant
O.Ctrl_Auth_Loader	not relevant
O.AES	O.PACE
O.Add-Functions	O.AA O.PACE
O.Mem-Access	O.Logical_Attack
O.Prot_TSF_Confidentiality	O.Logical_Attack
O.Ctrl_Auth_CCL	not relevant
O.Prot_Integrity	not relevant
O.Prot_Confidentiality	not relevant
O.Data_IntegrityService	not relevant

Table 8-4, Security objectives for the environment of the platform

Security Objectives for the Environment of Platform	Summary	Group
OE.Process-Sec-IC	Protection during composite product manufacturing	IrOE
OE.Lim_Block_Loader	Limitation of capability and blocking the Loader	IrOE
OE.TOE_Auth	Authentication to external entities	IrOE
OE.Loader_Usage	Secure communication and usage of the Loader	IrOE
OE.Resp-Appl	Treatment of User data of the Composite TOE	IrOE

8.1.3. Conclusion

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.

Assumptions A.Resp-Appl and A.Key-function from [HW-ST] are fulfilled automatically by O.Logical_Attack and O.Physical_Attack in the Composite ST.

8.2. TOE meets the SFRs

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

8.2.1. Self-Protection of the TOE

Self-Protection [FPT_PHP.3] is implemented by the underlying hardware platform and software composing the TSF. For detailed protection provided through the hardware LSI refer to [HW-ST].

8.2.2. Random numbers

The random number generator (FCS_RND.1) is implemented by the underlying hardware platform [HW-ST]. The TRNG in the underlying platform has a physical noise source and fulfils the requirements of functionality class PTG2 of [AIS_31].

The TRNG is used by the following commands:

- GENERAL AUTHENTICATE(Step1) (nonce, ephemeral key pairs generation)

The DRNG is used internally.

8.2.3. Cryptographic operations

The cryptographic operations relate to the SFRs FCS_CKM.1e, FCS_COP.1a, FCS_COP.1n and FCS_COP.1e. All these cryptographic operations are implemented by the certified crypto library and underlying hardware platform [HW-ST].

The following functions are implemented by the software cryptogram modules in accordance with specified cryptographic algorithms SHA-1 and SHA-256.

FCS_COP.1h and FCS_COP.1hp

The following functions are realized underlying hardware platform [HW-ST].

FCS_COP.1mp and FCS_COP.1sp

The following function is implemented according to 8.2.3.1. PACE.

FCS_CKM.1p

8.2.3.1. PACE

The Algorithm and Format used for PACE is described below:

(1) OID : id-PACE-ECDH-GM-AES-CBC-CMAC-128

- Key Agreement : ECDH
- Domain Parameter : NIST-P256

- Mapping : Generic
- Sym.Cipher and Key length : AES 128bit
- Secure Messaging : CBC / CMAC
- Auth. Token : CMAC

(2) OID : id-PACE-ECDH-GM-AES-CBC-CMAC-256 (Only the parts different from (1) are listed)

- Domain Parameter : NIST-P384
- Sym.Cipher and Key length : AES 256bit

Either of the above OIDs is chosen at personalization, stored in the TOE.

The outline of PACE procedure is described below.

TOE generates a nonce s (random number) to share with the Inspection system.

The nonce s is encrypted in AES-CBC mode using K_{π} . The key length of K_{π} is 128 or 256 bits.

K_{π} is derived from the password (MRZ) using a key derivation function (KDF).

KDF takes the shared secret value K and counter c as input, hashes the concatenated value, and outputs result.

Hash function uses SHA-1 for AES 128 bits key and SHA-256 for AES 256 bits key.

* For K_{π} , shared secret value K is MRZ and counter c is 3.

Generic Mapping is used for mapping nonce s .

TOE uses ECDH for Key Agreement that include the Generic Mapping.

The key length of EC key for ECDH is 256 or 384 bits, and the corresponding domain parameters are NIST-P256 and NIST-P384.

Secure Messaging keys are derived from value K shared by Key Agreement using KDF.

For ENC session key, counter c is 1. For MAC session key, counter c is 2.

Both key lengths are the same as K_{π} .

Mutual authentication is performed in AES-CMAC mode using the MAC Session Key.

After successful mutual authentication by PACE, the TOE and Inspection system will exchange commands using Secure Messaging.

ENC/MAC session keys are used for Secure Messaging, command data is encrypted in AES-CBC mode using ENC session key, MAC generation is performed in AES-CMAC mode using

the MAC session key.

8.2.4. Active Authentication

The SFRs FCS_COP.1a and FCS_COP.1h 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 random number. (FCS_CKM.4)

8.2.5. Identification and Authentication

FIA_UID.1 and FIA_UAU.1 provides the TOE service for the user that has succeeded in identification and authentication. Before an identification and an authentication, EF.CardAccess and EF.ATR/INFO are read.

User authentication requires the General Authentication procedure with the Password Authenticated Connection Establishment control method defined by ICAO, which is defined by FIA_UAU.5.

This General Authentication procedure requires new authentication data based on random numbers for each authentication using mutual authentication mechanism with the PACE procedure, which is defined by FIA_UAU.4.

The EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM and EF.SOD are able to read after successful of GENERAL AUTHENTICATE command. Under this situation, the password key file, transport key file and private key file are not able to read (FDP_ACC.1p, FDP_ACF.1p).

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

The TOE provides a file structure in which the each secret keys are encrypted and kept in IEFs. Furthermore the TOE does not implement functionality which reads IEFs to the outside of TOE. During Personalization, access to EF is controlled by authentication status of three Personalization Agent Keys (Transport key, Readout key and Active Authentication Information Access Key) and security attribute configured to each EFs. This access control mechanisms using security attributes prevents access to the file of the unauthorized user. These mechanisms and file structure are all compliant to JICSAP [JICSAP]. (FDP_ACC.1a, FDP_ACF.1a)

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. This functionality is achieved by IEF with counter/limit (FIA_AFL.1a, FIA_AFL.1d and FIA_AFL.1r).

The personalization Agent must use the VERIFY command with the 16 byte Transport key, Readout key and Active Authentication Information Access Key (FIA_UAU.5).

The modification of transport key is enabled after successful of transport key verification (FMT_MTD.1, FMT_SMF.1 and FMT_SMR.1).

The session key is destructed to random number, 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.

The security attributes are not imported when user data are written. WRITE BINARY and CHANGE REFERENCE DATA commands are used for writing user data. The data access of these commands are controlled under the SFP (FDP_ITC.1).

8.2.6. Data integrity

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).

Other user roles like the Inspection systems are only allowed to read the data after successful General Authentication. Furthermore, the secure messaging is used to communicate between the TOE and the authenticated Inspection System (FDP_UIT.1p, FTP_ITC.1). After use the session keys are destroyed using (FCS_CKM.4) to all random number, when an error occurs in Password Authenticated Connection Establishment (PACE) secure messaging.

8.2.7. Data confidentiality

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, and FDP_ACF.1a).

Other user roles like the Inspection systems are only allowed to read the data after successful General Authentication. Furthermore, the secure messaging is used to communicate between the TOE and the authenticated Inspection System (FDP_UCT.1p, FTP_ITC.1). After use the

session keys are destroyed using (FCS_CKM.4) to all random number, when an error occurs in Password Authenticated Connection Establishment (PACE) processor when an error in secure messaging.

9. Reference

No	Title	Date	Version	publisher	Document number
[CC_1]	Common Criteria for Information Technology Security Evaluation, Part 1: Outline and General Model	April 2017	Revision 5		
[CC_2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components	April 2017	Revision 5		
[CC_3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components	April 2017	Revision 5		
[CEM]	Common Methodology for Information Technology Security Evaluation (CEM), Part 2: Evaluation Methodology	April 2017	Revision 5		
[PP-0084]	Security IC Platform Protection Profile with Augmentation Packages Version 1.0	19.02.2014	3.1 R4	Bundesamt für Sicherheit in der Informationstechnik (BSI)	
[PP-C0499EN]	Protection Profile for ePassport IC with SAC (PACE) and Active Authentication	March 8, 2016	1.00	Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan	

				JBMIA	
[PP-C0499]	旅券冊子用 IC のための プロテクションプロファイ ル –SAC 対応(PACE) 及び能動認証対応–	2016 年 3 月 8 日	第 1.00 版	外務省領事局旅 券課 JBMIA	JISEC C0499
[CC_AAP]	Common Criteria Supporting Document Mandatory Technical Document Application of Attack Potential to Smartcards	May 2013	Version 2.9		CCDB-2013- 05-002
[ICAO_9303]	Machine Readable Travel Documents Seventh Edition — 2015 Doc 9303 Part 11 Security Mechanisms for MRTDs	2015	Seventh Edition	Authority of the secretary general, International Civil Aviation Operation	
[HW-ST]	Common Criteria Public Security Target EAL6 augmented / EAL6+ IFX_CCI_000003h IFX_CCI_000005h IFX_CCI_000008h IFX_CCI_00000Ch IFX_CCI_000013h IFX_CCI_000014h IFX_CCI_000015h IFX_CCI_00001Ch IFX_CCI_00001Dh IFX_CCI_000021h IFX_CCI_000022h H13 Resistance to attackers with HIGH attack potential	Date: 2022-03- 28	Revision 2.0	Infineon Technologies AG	

[AIS_31]	A proposal for: Functionality classes for random number generators ¹	2011-09-18	Version 2.0	Bundesamt für Sicherheit in der Informationstech nik (BSI)	
[JICSAP]	Specification of IC cards with contacts Complying with Japanese Industrial Standard	1998	1.1	Japan Ic Card System Application council (JICSAP)	

End of Document