MC-SM1908

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

January 11, 2018

Version01.00.05

Software Design Group
Smart Card Systems Department
Komukai Complex
Toshiba Infrastructure Systems & Solutions Corporation

Table of contents

1. Introduction

This document is the Security Target for the contactless smartcard product based on the IFX_CCI_000005HIC.

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 4) 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 01.00.05
Date of issue:	11 January 2018
TOE identification:	TOSMART-GP1
TOE version:	Version 01.00.00
Produced by:	TOSHIBA CORPORATION Software Design Group Smart Card Systems Department Komukai Operations

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, 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 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. 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.

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

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:

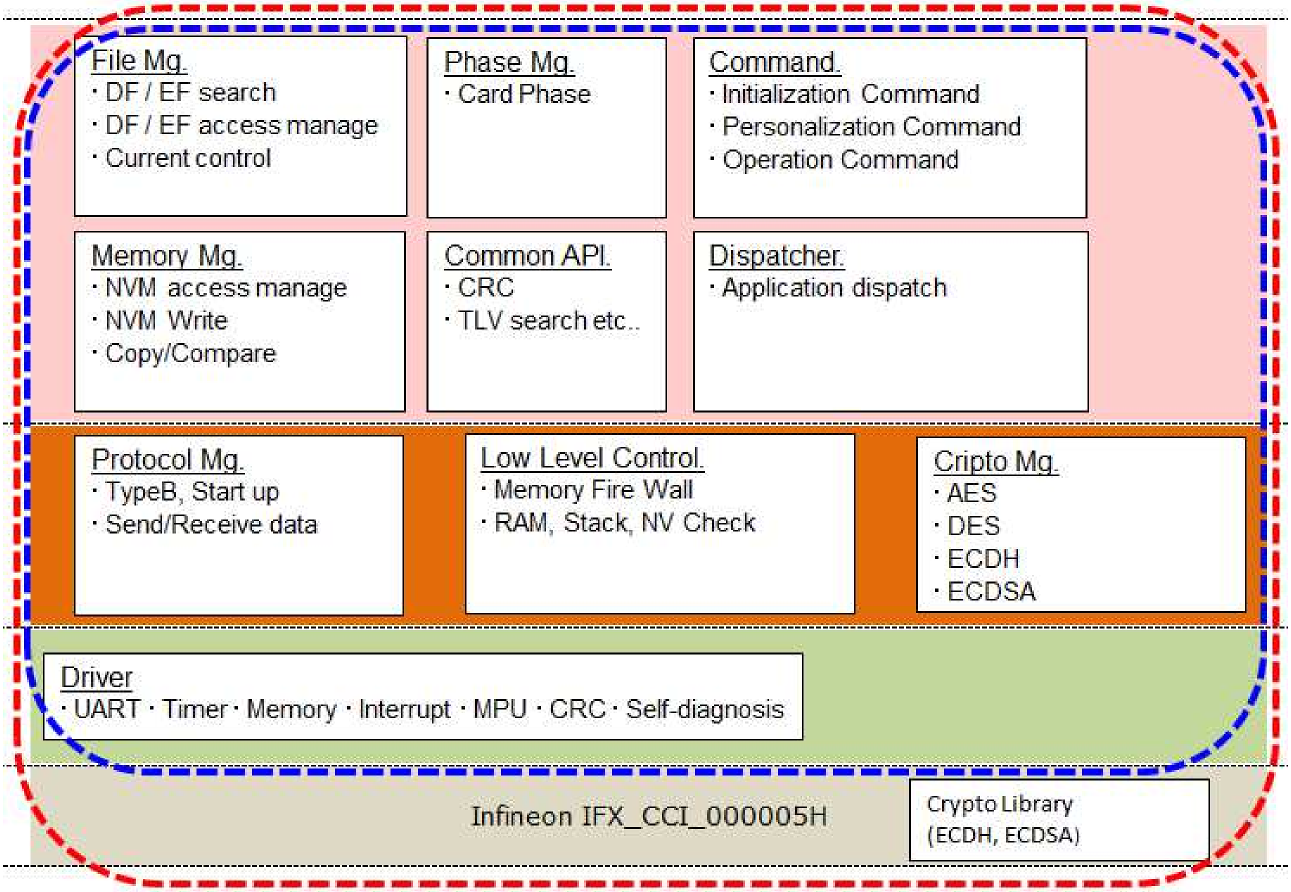

Figure 1TOE scope (marked by red dashed line) and part additional to hardware (marked by blue dashed line)

The ePassport (OS and ePassport application) consists of a binary package that is implemented in the User Flash memory of the IFX_CCI_000005H. 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 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 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 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**
Hardware	IFX_CCI_000005H (Common criteria certification identifier) 0013H 0016H 0000H (Chip Type)	FW-Identifier 80.100.17.0	Sheet
CL52 Asymmetric Crypto Library for Crypto@2304T	Cl52-LIB-base-XSMALL-HUGE.lib	v2.06.003	
CL52 Asymmetric Crypto Library for Crypto@2304T	Cl52-LIB-ecc-XSMALL-HUGE.lib	v2.06.003	
CL52 Asymmetric Crypto Library for Crypto@2304T	Cl52-LIB-toolbox-XSMALL-HUGE.lib	v2.06.003	
Hardware Support Library for SLCx2	HSL-01.22.4346-SLCx2_C65.lib	v1.22.4346	
Software	ePassport application ＋OS	Ver.01.00.14	Flash memory of hardware (user area)
Delivery item type	**Identifier**	**Document No. / Version**	**Medium**
Guidance (for personalization agent)	Guidance Document for Personalization agent（USR）	MC-SM1911 / Version 01.00.06	Document / pdf
	Preparative guidance（PRE）	MC-SM1905 / Version 01.00.04	Document / pdf
	Application Specification	MC-SM1917 / Version 1.0.6	Document / pdf
	Authentication Manual using VERIFY command	MC-SJ0131 / Version 01.00.03	Document / pdf
	Personalization Specification	MC-SM1895 / Version 1.0.5	Document / pdf
	Procedural Request of Security Product Delivery and Receipt	MB-ICCARD-W471-03 / Version 1.0.3	Document / pdf

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 aplastic 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 hardware platform and crypto library, the TOE-Software implements a file system, 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 and crypto library.

- Destruction of the cryptographic keys after usage (FCS_CKM.4)
- Implementation of the IFX_CCI_000005H 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 4 September 2012. 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 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	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: (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	The technical system used by the border control officer of the receiving State (i) examining an ePassport presented by the traveller and verifying its authenticity and

	(ii) verifying the traveller as ePassport holder. The Basic Inspection System (BIS) (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. 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.
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	A threat agent trying (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 is denoted, the component has an additional identification /XXXX.

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

7.2. Security Functional Requirements

The SFRs are split in two categories, 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 (Nonce encryption)	
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: cryptographic key destruction method	[PACE session key and Active Authentication secret key clear][1]

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

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 : defined quality standards].**
Assignment defined quality standards	Class PTG2 of the AIS31

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]~~**]** unsuccessful authentication attempts occur related to **[assignment: list of authentication events]**.
Selection:[assignment: positive integer number]	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].**
Assignment: list of actions	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”)

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]	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].**
Assignment: list of actions	permanently stop authentication with the transport key (fix the authentication status with the transport key to “Not authenticated yet”)

FIA_AFL.1r Authentication failure handling (Readout 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]	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].**
Assignment: list of actions	permanently stop authentication with the readout key (fix the authentication status with the readout key to “Not authenticated yet”)

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 orFDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Covered by the PP
FCS_COP.1h	[FDP_ITC.1 orFDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Covered by the PP
FCS_COP.1n	[FDP_ITC.1 orFDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Covered by the PP
FCS_COP.1e	[FDP_ITC.1 orFDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Covered by the PP
FCS_COP.1hp	[FDP_ITC.1 orFDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Covered by the PP
FCS_COP.1mp	[FDP_ITC.1 orFDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	Covered by the PP
FCS_COP.1sp	[FDP_ITC.1 orFDP_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 orFDP_IFC.1], FMT_MSA.3	Covered by the PP
FDP_UCT.1p	[FTP_ITC.1 orFTP_TRP.1], [FDP_ACC.1 orFDP_IFC.1]	Covered by the PP
FDP_UIT.1p	[FDP_ACC.1 orFDP_IFC.1], [FTP_ITC.1 orFTP_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].

Table 8-1, Mapping of SFRs

Relevant Platform-SFR	Description	Correspondence in composite ST
FCS_COP.1/AES (1)	"Cryptographic operation – AES"	The following functions are realized by processing by software using the function of AES which a cryptographic library offers. FCS_COP.1sp, FCS_COP.1mp
FCS_COP.1/ECDSA	"Cryptographic Operation – ECDSA"	FCS_COP.1a
FCS_COP.1/ECDH	"Cryptographic Operation – ECDH"	FCS_COP.1e
FCS_RNG.1/TRNG	"Random number generation - TRNG"	FCS_RND.1
FCS_CKM.1/EC	"Cryptographic key management - EC"	FCS_CKM.1e
FPT_PHP.3	"Resistance to physical attack"	FPT_PHP.3
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	Memory access control

	attributes"	[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.
FMT_LIM.2/Loader	"Limited Availability - Loader"	Support of the Flash Loader [HW-ST] 7.2 is used by composite TOE.

Other platform SFR’s are not used.

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 RNG in the underlying platform has a physical noise source and fulfils the requirements of functionality class PTG2 of [AIS_31].

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].

FCS_COP.1h and FCS_COP.1hp (SHA-256) are implemented by the Secure Hash Algorithm SHA-2 Library. FCS_COP.1hp (SHA-1) and FCS_CKM.1p are implemented by the application software.

The following functions are realized by processing by software using the function of cryptographic libraries offer.

FCS_COP.1mp and FCS_COP.1sp

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)

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. (FDP_ACC.1a, FDP_ACF.1a, FIA_AFL.1a, FIA_AFL.1d and FIA_AFL.1r)

8.2.5. Identification and Authentication

During phase 2 “manufacturing” and phase 3 ”personalization of the TOE”, the TOE can be identified using a special APDU ‘GET MASK VERSION’. 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”.

FIA_UID.1 and FIA_UAU.1 provides the TOE service for the user that has succeeded in identification and authentication. Before an authentication, EF.CardAccess is 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, which is defined by FIA_UAU.4.

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

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 personalization Agent must use the VERIFY command with a 16 byte secret personalization agent key (FIA_UAU.5).

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.

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.

At the end of the personalization the TOE is brought to the 'operational' life cycle, by running three times of a VERIFY command using incorrect keys[2]. From this point on a user has to be properly authorized to read any data from the TOE. (FIA_AFL.1a, FIA_AFL.1d and FIA_AFL.1r)
Readout key is used for read-out of EF.DG13.
Active Authentication Information Access Key is used in order to write in the Active Authentication private key and EF.DG15.
Transport key is used in order to personalize the data other than the above.

Access control of TOE conforms to “Chapter 3.2Table 1 TOE Internal Information Access Control by Passport Issuance Authority” in [PP-C0499](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 (FCS_CKM.1p, FCS_CKM.1e, FCS_COP.1n, FCS_COP.1e, FCS_COP.1hp, FCS_COP.1mp, FCS_COP.1sp, FDP_ACC.1p, FDP_ACF.1p, FIA_UID.1, FIA_UAU.1, FIA_UAU.5 and FIA_UAU.4). 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 (FCS_CKM.1p, FCS_CKM.1e, FCS_COP.1n, FCS_COP.1e,

[2] It is noted that this VERIFY command cannot be used to authenticate the Personalization Agent to the TOE

FCS_COP.1hp, FCS_COP.1mp, FCS_COP.1sp, FDP_ACC.1p, FDP_ACF.1p, FIA_UID.1, FIA_UAU.1, FIA_UAU.5 and FIA_UAU.4). 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	September 2012	Revision 4		
[CC_2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components	September 2012	Revision 4		
[CC_3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components	September 2012	Revision 4		
[CEM]	Common Methodology for Information Technology Security Evaluation (CEM), Part 2: Evaluation Methodology	September 2012	Revision 4		
[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	Tbd	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]	Public Security Target Common Criteria v3.1 – 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 H13 Resistance to attackers with HIGH attack potential	Date: 2017-05-22	Revision 0.5	Infineon Technologies AG	

[AIS_31]	A proposal for: Functionality classes for random number generators1	2011-09-18	Version 2.0	Bundesamt für Sicherheit in der Informationstechnik (BSI)	

End of Document