ID&TRUST

ID&Trust IDENTITY-J with SAC (PACE) and AA

SECURITY TARGET Lite

COMMON CRITERIA

EAL4+

2019

Classification PUBLIC

Revision history

Version	Date	Description
V1.0	28.05.2019	Initial version
V1.1	03.06.2019	Minor modifications
V1.2	21.07.2019	Further minor modifications
V1.3	25.07.2019	Fix further typos
V1.4	26.07.2019	Fix incorrect references in Table 6

Table of Contents

1. ST introduction

1.1. ST reference

Title:	Security Target Lite -ID&Trust IDentity-J with SAC (PACE) and AA
Author:	ID&Trust Ltd.
Sponsor	Maxell, Ltd.
Version:	v1.4
Date of issue:	26.07.2019

1.2. TOE reference

TOE name:	ID&Trust IDentity-J with SAC (PACE) and AA version 1.0 on IFX M7892 G12 SLJ 52G
TOE short name:	IDentity-J
TOE Identification data:	IDentity-J-v1.0.7052
Evaluation assurance level:	EAL4+ augmented with ALC_DVS.2 and AVA_VAN.5
TOE Certification ID:	ITC-8678
TOE Hardware ID	Infineon Security Controller M7892 Design Steps D11 and G12, with specific IC dedicated firmware and optional software
TOE IC firmware	78.015.14.0 or 78.015.14.1 or 78.015.14.2 or 78.015.18.2
TOE Crypto Library	RSA/EC/Toolbox v2.07.003 and Symmetric Crypto library v2.02.010
Certification ID of TOE Hardware including Crypto Library and IC firmware	BSI -DSZ-CC-0891-V3-2018
TOE OS name and version:	Oracle JCOS v2 – Build 32 - JCDK version 3.0
TOE Platform Certification ID	BSI-DSZ-CC-0869-V2

1.3. TOE overview

1.3.1. TOE Types

The TOE is an ePassport IC (including necessary software). This ePassport IC is composed of IC chip hardware with the contactless communication interface (provided by Infineon), and basic software (operating system which is provided by Oracle) and ePassport application program (IDentity-J), which is developed by ID&Trust Ltd. that are installed in the said hardware (hereinafter, the term an "IC chip" shall mean an “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.

1.3.2. Required non-TOE hardware/software/firmware

The TOE does not require any hardware, software, or firmware to operate, but as described in A.PKI, the passport issuing authorities has to set up and maintain the interoperability the PKI environment both of the issuing and receiving states or organization sides.

1.3.3. TOE Usage and Main Security Functions

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 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[1] 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.

[1] Digital signature is added to individual digital data by the passport issuing authorities in order to prevent the forgery of digital data. The verification process of the digital signature has been standardized as the Passive Authentication by ICAO. PKI that provides interoperability for all member states of ICAO is implemented from the grant of digital signature through the verification thereof with the terminal for the purpose of supporting Passive Authentication. Since the Passive Authentication is performed through verification of digital signature (including background PKI) without involvement of the security functions of the TOE, it is not included in the security requirements for the TOE.

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 [1].

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); and
- Tamper resistance (protection against confidential information leak due to physical attacks).

1.3.4. TOE Life Cycle

The TOE life cycle is described below to clarify the security requirements for the TOE. The TOE life cycle of general IC chips is often described in terms of seven phases in the life cycle.

As for the ePassport IC, however, the life cycle is divided into four phases instead of seven as described in [2].

Phase 1
Development

In this phase 1, threats in the operational environment are not considered, but proper development security shall be maintained to protect the confidentiality and integrity of development data. The composite TOE is certified on EAL4+ (ALC_DVS.2) and the Platform is certified on EAL5+ (ALC_DVS.2) as well, so the development environment of the Platform and the composite TOE developers meet the security assurance requirements.The Developer of IDentity-J uses secure tool of Infineon to upload CAP files for the chip manufacturer (Infineon) as required by the Platform's User Guide.

Phase 2
Manufacturing

In phase 2, the Manufacturer (Infineon) produces the IC chips (with embedded software installed and loaded the IDentity-J (ePassport application). The functional tests of the internal circuit of the IC chip are conducted before the IC chip is sealed. After that, only the contactless communication interface becomes available as an external interface.

Manufacturer produces the wafers and transports them to the IC sheet manufacturer. During the shipment the logical protection of the TOE is ensured by GP keys..

The manufactured IC chip is embedded in the plastic sheet together with the contactless communication antenna by the IC sheet manufacturer.

In phase 2 some pre-personalization activity is performed e.g. instance creation, Transport Key, Active Authentication Access Key and Readout Key generation (initialization, pre-personalization, and activation of IDentity-J by IC sheet manufacturer).

The TOE is identifiable with the IC serial number until the passport authority disables it in the next, Personalization phase. The confidentiality of chip IC serial number is protected by the Readout Key.

During the shipment from IC sheet manufacturer to Personalization Agent (passport issuing authorities) the TOE is protected by the Transport Key.

At the end of this phase, after initialization, pre-personalization and activation of IDentity-J, the TOE is configured as an ePassport and ready for personalization as an MRTD document for MRTD holder in the next phase. The TOE is delivered in the sense of CC at the end of this phase from Maxell to NPB.

Phase 3
Personalization

The TOE in Phase 3 is put under the control of the passport issuing authorities. Although no explicit attack against the TOE is assumed under the control of the passport issuing authorities, the TOE is required to have security functionality that allows only authorized individuals to process the TOE, as the organizational security policy.

The TOE is interfiled in the ePassport booklet and information necessary for ePassport is written therein. This information includes the personal information of the passport holder (e.g. name, information on birth and so on) and cryptographic key used by the security functions.

Personalization activities covers the following:

- Generate TSF-data
- Generate or write the User Data on the TOE.

After the completion of personalization of all information, the ePassport is issued to the holder thereof.

Phase 4

Operational Use

Phase 4 is a phase subsequent to the handover of the passport booklet to the end user, i.e., the holder thereof. The passport booklet is carried along with the holder thereof and used to certify the identity of the holder in various situations, including immigration procedures.

In Phase 4, no information stored in the TOE is altered or deleted. The TOE security function protects the information necessary for immigration procedures against illicit reading, unless the information is read by an authorized terminal. The private key for Active Authentication is only used for the internal processing of the TOE and will never be readout to anywhere other than the TOE. The TOE security functions protect the information assets in the TOE against external unauthorized access. These requirements are ensured as described below:

During the usage of the TOE by the passport holder in operational environment the integrity and authenticity of the User Data are protected by the Passive Authentication, the genuineness of the TOE is ensured by the Active Authentication and the confidentiality of the User Data are protected by the PACE.

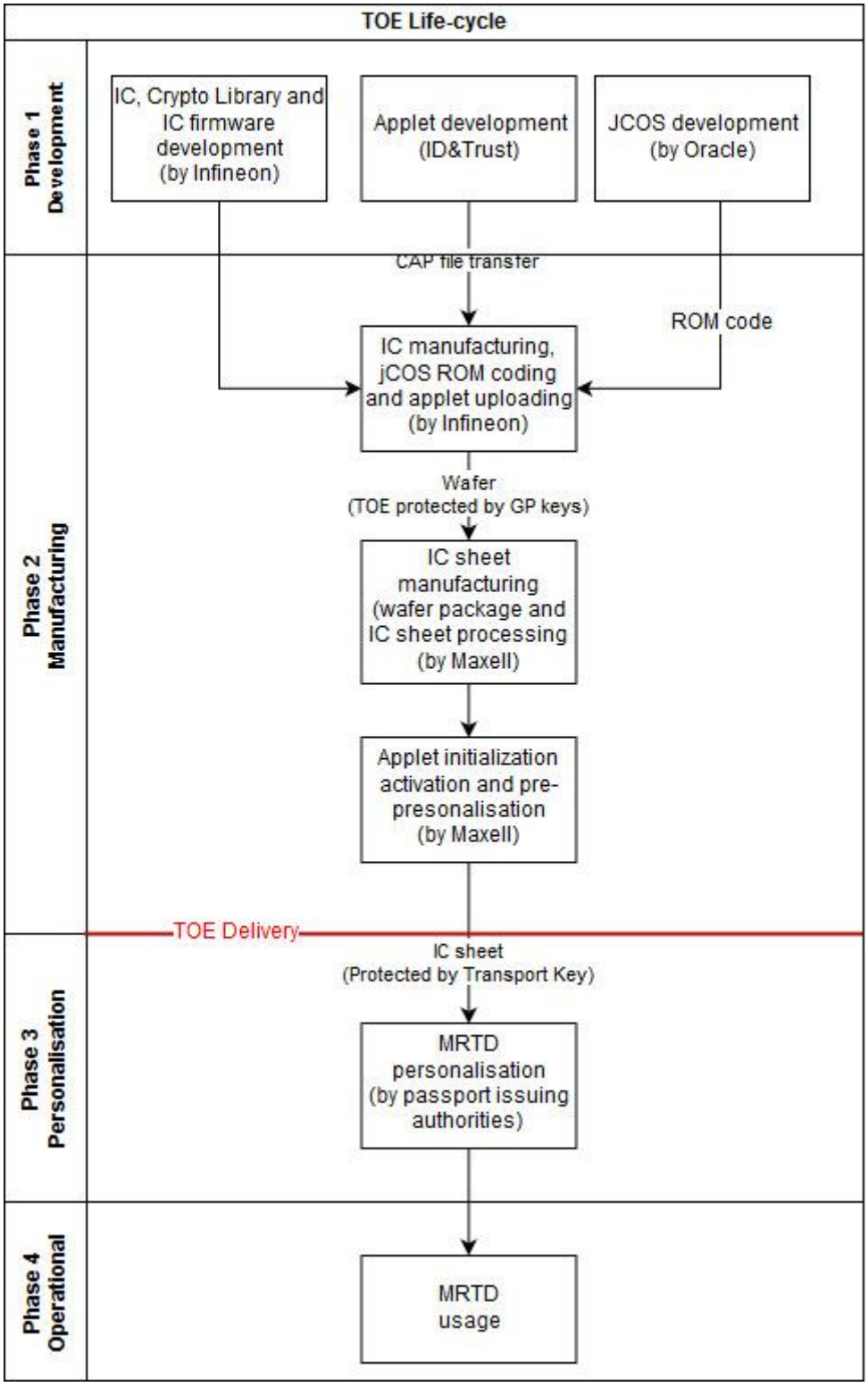

Figure 1 Overview of TOE life-cycle

1.4. TOE description

The composite TOE consists a certified Infineon M7892 G12 secure micro controller with Toolbox and Symmetric Crypto Library with specific IC dedicated software (firmware). An external antenna is connected to the IC chip for contactless communication purpose (ISO 14443). There is a Java Card

Platform, which is certified as well. These are used as certified underlying Platform by the ePassport application (IDentity-J).

The composite TOE is intended to be used as an ePassport. This ePassport 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 TOE provides several security functions:

- 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); and
- Tamper resistance (protection against confidential information leak due to physical attacks).

Furthermore, the TOE supports the Passive Authentication.

1.4.1. TOE physical scope

The TOE physically is a secure IC chip, which contains the following:

- Certified (Smart Card Platform) hardware platform (M7892 G12) with EC and Symmetric Crypto Library and with specific IC dedicated software (firmware);
- Certified Java Card Platform;

For identification data and certification IDs of the above-mentioned parts of the Platform please see section 1.2.

- ePassport application (IDentity-J v1.0) (CAP files);

and related documents:

- [3] (.pdf);
- [4] (.pdf).

The CAP files are uploaded via the secure platform of the chip manufacturer. [3] is sent in .pdf format to the IC sheet manufacturer by encrypted form (pgp encrypted via email).

[4] is the ePassport specification of Japan, which was partly prepared, translated to English and maintained by Maxell for applet developer. This document was received by ID&Trust Ltd. from Maxell as an pgp encrypted .pdf via email

Other part of the TOE (e.g. the antenna) is out of the scope of this TOE.

1.4.2. TOE logical scope

The logical scope of the TOE is described in the following Figure 2 Logical scope of the TOE:

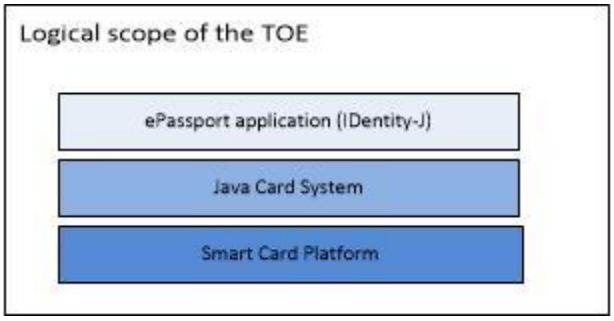

Figure 2 Logical scope of the TOE

The Java Card System (JCS) and the Smart Card Platform (SCP) are certified and described in [5]. JCS and SCP are referenced as Platform in this document. The ePassport application (IDentity-J) relies on the certified Platform as described in this ST.

The IDentity-J uses several important security features of Platform, such as the Crypto Library for cryptographic operations and secure key destruction. Furthermore, Platform protects the TOE against e.g. side-channel attacks for details please see [5].

The Smart Card Platform provides:

- CPUs;
- Memory management unit;
- Memory Encryption/Decryption Unit;
- Coprocessor for DES/AES and RSA/EC processing;
- Secure random number generation;
- Communication protocols (ISO 7816/ISO 14443);
- Tamper resistance (protection against confidential information leak due to physical attacks).

The Java Card System provides:

- Java Card Platform (Java Card 3.0.1 APIs, Java Card 3.0.1 Virtual Machine and Java Card 3.0.1 Runtime Environment);
- Global Platform Layer;
- Optional modules (e.g. LDS secure messaging Accelerators, EC).

ePassport application (IDentity-J v1.0) provides:

- ePassport functionality (compliant to [6]);

- satisfaction of the Platform user guide's requirements;
- 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).

2. Conformance Claim

2.1. CC Conformance Claim

CC, to which the ST conforms, are identified. The PP conforms to the following CC V3.1 (in Japanese version released by JISEC):

- Part 1: Overview and the General Model; April 2017, Version 3.1 Revision 5, CCMB-2017-04-001
- Part 2: Security Functional Components; April 2017, Version 3.1 Revision 5, CCMB-2017-04-002
- Part 3: Security Assurance Components; April 2017, Version 3.1 Revision 5, CCMB-2017-04-003
- Conformance to CC Part 2: CC part 2 extended
- Conformance to CC Part 3: CC part 3 conformant

2.2. ST Claim

The ST claims strict conformance to [7]. [2] is translated from [7].

2.3. Package Claim

In the ST, the assurance package applicable to the TOE is EAL4 augmented. Assurance components augmented are ALC_DVS.2 and AVA_VAN.5.

2.4. Conformance Rationales

The [7] requires strict conformance.

3. Statement of Compatibility

3.1. Security Functionalities

The following Table 1 contains the relevant security functions of the Platform.

Platform Security Functions	Corresponding TOE Security Function	Relevant	Non-Relevant	Remark
SF.Card Manager	TSF.Platform	X	-	The TOE uses the following features: • Card Content Management (CMM) • Card Management Environment • APDU Commands Dispatcher • Life Cycle Management
SF.Secure Channels	TSF.Platform TSF.Crypto	X	-	The TOE uses the following features: • Mutual Authentication • Message Integrity Verification • Message Confidentiality • Secure Messaging acceleration
SF.Secure Channel Key Management	TSF.Platform TSF.Crypto	X	-	The TOE uses the following feature: Session Key/ISD Key Generation
SF.Global PIN Management	-	-	X	The TOE does not use global CVM.
SF.Java Card Firewall	TSF.Platform	X	-	The TOE uses the Java Card Firewall functionalities.
SF.End User Authentication	-	-	X	The TOE does not authenticate applet's user with PIN.
SF.Sensitive Data Cleaner	TSF.Platform TSF.Crypto	X	-	The TOE clears sensitive information (e.g. cryptographic buffer) after usage of sensitive operations (e.g. cryptographic operations).
SF.Atomic_Transactions	TSF.Platform	X	-	The TOE uses the atomic transaction security functions of the Platform.
SF.Security Violation	-	-	X	Not relevant because no other applet in the TOE.
SF.PIN Integrity	-	-	X	The TOE does not authenticate applet's user with PIN.
SF.Key Management	TSF.Platform TSF.Crypto TSF.Authenticate	X	-	The TOE uses the following features: Keys Integrity Protection Keys Confidentiality Protection Keys Secure Generation Keys Secure Deletion Key Secure Agreement.
SF.Cryptographic Operations	TSF.Platform TSF.Crypto TSF.Authenticate	X	-	The TOE uses the following features: Message Digest Generation Signature Generation&Verification Encryption & Decryption Unique Hash Value Random Number Generation

Platform Security Functions	Corresponding TOE Security Function	Relevant	Non-Relevant	Remark
SF.Extended Memory	-	-	X	The TOE does not use the extended memory feature of the Platform.

Table 1 Mapping of Security Functions

3.2. Threats

The following threats are relevant from [5]

Relevant Threats from [5]	Corresponding Threats	Comments
T.CONFID-APPLI-DATA	T.Physical_Attack T.Communication_Attack T.Copy	-
T.CONFID-JCS-DATA	-	No contradiction to composite ST
T.INTEG-APPLI-DATA	-	No contradiction to composite ST
T.INTEG-JCS-DATA	-	No contradiction to composite ST
T.RESOURCES	T.Physical_Attack	-
T.RND	T.Communication_Attack	-
T.PHYSICAL	T.Physical_Attack T.Communication_Attack	-
T.LEAKAGE	T.Communication_Attack	-
T.FAULT	T.Communication_Attack	-
T.SID.2	T.Physical_Attack	-

Table 2 Mapping of Threats

All the relevant Threats from [5] were analysed and there is no contradiction to this ST. Other threats of Platform are not relevant.

3.3. OSPs

There are no relevant organizational security policies in [5].

3.4. Assumptions

The assumptions of [5] are categorized as IrPA or CfPA in the Table 3 and the Comments column contains more information. There is no SgPA assumption.

Assumption	Classification of the assumption	Comments
A.APPLET	IrPA	There is no other applet on the TOE.
A.VERIFICATION	CfPA	Fulfilled by SAR class ALC.

Table 3 Mapping of Assumptions

3.5. Security Objectives

The following security objectives for the TOE are relevant from [5] and the Table 4 contains the mapping. There is no contradiction between the mapped security objectives for the TOE.

Objective from [5]	Corresponding Security Objectives from the TOE	Comments
O.OPERATE	O.Physical_Attack	
O.RESOURCES	O.Physical_Attack	
O.ALARM	O.Physical_Attack	
O.CIPHER	O.AA O.PACE O.Authority	
O.KEY-MNGT	O.AA O.PACE O.Authority O.Physical_Attack	
O.PIN-MNGT	-	No contradiction to composite ST.
O.RND	O.PACE	
O.GLOBAL_ARRAYS_CONFID	-	No contradiction to composite ST.
O.TRANSACTION	-	No contradiction to composite ST.
O.REALLOCATION	O.AA O.PACE	
O.IC_SUPPORT	O.Physical_Attack	
O.RECOVERY	-	No contradiction to composite ST.
O.OS_SUPPORT	O.Physical_Attack	

Table 4 Mapping of security objectives for the TOE

There are no relevant or significant security objectives for the operational environment.

3.6. Security Requirements

The following security functional requirements are relevant from [5] and the Table 5 contains the mapping. The SFRs from [5], are not relevant if they are not listed in Table 5.

Platform SFRs	Composite TOE SFRs	Comments
FAU_ARP.1	FPT_PHP.3	FAU_ARP.1 provides several security actions if potential security violations happen (e.g. stack overflow, or card tearing).
FCS_CKM.1	-	Not relevant
FCS_CKM.2	-	Not relevant
FCS_CKM.3	-	Not relevant
FCS_CKM.4	FCS_CKM.4	The FCS_CKM.4 uses the FCS_CKM.4 SFR of the Platform during the destruction of PACE session keys and PACE ephemeral key pairs.
FCS_COP.1.1/ACC_CYPHER	FCS_COP.1sp	FCS_COP.1sp uses FCS_COP.1.1/ACC_CYPHER during the secure messaging in case of PACE protocol.
	FTP_ITC.1	FTP_ITC.1 uses FCS_COP.1.1/ACC_CHYPHER for

Platform SFRs	Composite TOE SFRs	Comments
		channel data protection from disclosure
	FDP_UCT.1p	FDP_UCT.1p uses the FCS_COP.1/ACC_CYPHER to protect user data from unauthorized disclosure.
FCS_COP.1.1/ACC_MAC	FIA_UAU.5	FIA_UAU.5 uses FCS_COP.1.1/ACC_MAC for PACE during the mutual authentication
	FTP_ITC.1	FTP_ITC.1 uses several Platform FCS_COP.1 functionalities to establish a secure communication channel and protect the read data from disclosure and modification.
	FCS_COP.1sp	FCS_COP.1sp uses FCS_COP.1/ACC_MAC during the secure messaging in case of PACE protocol.
	FDP_UIT.1p	FDP_UIT.1p uses the FCS_COP.1/ACC_MAC to protect user data from modification, deletion, insertion or replay.
FCS_COP.1.1/AES	FCS_COP.1n	FCS_COP.1n uses the FCS_COP.1.1/AES to encrypt the nonce.
FCS_COP.1.1/EC	FCS_CKM.1e	FCS_CKM.1e uses the FCS_COP.1.1/EC SFR of Platform to generate elliptic curve key pair.
FCS_COP.1.1/ECDH	FCS_CKM.1p	FCS_CKM.1p uses the FCS_COP.1.1/ECDH during the elliptic curve Diffie-Hellman key agreement.
	FCS_COP.1e	FCS_COP.1e uses the FCS_COP.1.1/ECDH function during the key agreement in PACE protocol.
FCS_COP.1.1/ECDSA	FCS_COP.1a	FCS_COP.1a uses the FCS_COP.1.1/ECDSA SFR of the Platform during the digital signature generation.

Platform SFRs	Composite TOE SFRs	Comments
FCS_COP.1.1/PACE_SUPP	FCS_COP.1e	FCS_COP.1e uses FCS_COP.1.1/PACE_SUPP for generic mapping (part of the PACE protocol).
FCS_COP.1.1/DES	-	Not relevant
FCS_COP.1.1/SHA	FCS_COP.1h	FCS_COP.1h uses FCS_COP.1.1/SHA for hash value calculation during the digital signature generation.
	FCS_COP.1hp	The FCS_COP.1hp uses FCS_COP.1.1/SHA for hash value calculation.
	FCS_CKM.1p	FCS_CKM.1p uses FCS_COP.1.1/SHA during the session key generation.
FCS_COP.1.1/DES-MAC	-	Not relevant
FCS_COP.1.1/AES-MAC	FCS_COP.1mp	FCS_COP.1mp uses FCS_COP.1.1/AES-MAC for authentication token generation and verification in AES CMAC mode.
FCS_RNG.1	FCS_CKM.1p	FCS_CKM.1p uses the FCS_RNG.1 SFR of Platform to generate a nonce.
	FCS_CKM.1e	FCS_CKM.1e uses random number - provided by FCS_RNG.1 - for ephemeral key pairs generation.
	FCS_COP.1a	FCS_COP.1a uses random number - provided by FCS_RNG.1 - during digital signature generation.
	FCS_RND.1	FCS_RND.1 uses the FCS_RNG.1 to generate random numbers.
	FIA_UAU.4	FIA_UAU.4 uses the FCS_RNG.1 function to generate a fresh nonce in case of PACE.
FCO_NRO.2/CM	-	Not relevant
FDP_ACC.1/EXT_MEM	-	Not relevant
FDP_ACC.1/GPG	-	Not relevant
FDP_ACC.2/ADEL	-	Not relevant
FDP_ACC.2/FIREWALL	-	Not relevant
FDP_ACF.1/ADEL	-	Not relevant
FDP_ACF.1/EXT_MEM	-	Not relevant
FDP_ACF.1/FIREWALL	-	Not relevant
FDP_ACF.1/GPG	-	Not relevant
FDP_IFC.1/JVCM	-	Not relevant
FDP_IFF.1/JVCM	-	Not relevant
FDP_IFC.2/CM	-	Not relevant
FDP_IFF.1/CM	-	Not relevant
FDP_ITC.2/Installer	-	Not relevant
FDP_RIP.1/ABORT	-	Not relevant
FDP_RIP.1/ADEL	-	Not relevant
FDP_RIP.1/APDU	-	Not relevant
FDP_RIP.1/bArray	-	Not relevant

Platform SFRs	Composite TOE SFRs	Comments
FDP_RIP.1/KEYS	FCS_CKM.4	FCS_CKM.4 uses the FDP_RIP.1/KEYS to deallocate the resource from the cryptographic buffer of the Platform.
FDP_RIP.1/OBJECTS	-	Not relevant
FDP_RIP.1/ODEL	-	Not relevant
FDP_RIP.1/TRANSIENT	-	Not relevant
FDP_ROL.1/FIREWALL	-	Not relevant
FDP_SDI.2	FPT_PHP.3	FDP_SDI.2 provides security functions to check integrity of PIN or keys.
FDP_UIT.1/CM	-	Not relevant
FIA_ATD.1/AID	-	Not relevant
FIA_UID.1/CM	-	Not relevant
FIA_UID.2/AID	-	Not relevant
FIA_UID.1/GPG	-	Not relevant
FIA_USB.1/AID	-	Not relevant
FMT.MSA.3/GPG	-	Not relevant
FMT_MSA.1/ADEL	-	Not relevant
FMT_MSA.1/CM	-	Not relevant
FMT_MSA.1/EXT_MEM	-	Not relevant
FMT_MSA.1/GPG	-	Not relevant
FMT_MSA.1/JCRE	-	Not relevant
FMT_MSA.1/JCVM	-	Not relevant
FMT_MSA.2/FIREWALL_JCVM	-	Not relevant
FMT_MSA.3/CM	-	Not relevant
FMT_MSA.3/ADEL	-	Not relevant
FMT_MSA.3/EXT_MEM	-	Not relevant
FMT_MSA.3/FIREWALL	-	Not relevant
FMT_MSA.3/GPG	-	Not relevant
FMT_MSA.3/JCVM	-	Not relevant
FMT_MTD.1/JCRE	-	Not relevant
FMT_MTD.3/JCRE	-	Not relevant
FMT_SMF.1	-	Not relevant
FMT_SMF.1/ADEL	-	Not relevant
FMT_SMF.1/CM	-	Not relevant
FMT_SMF.1/EXT_MEM	-	Not relevant
FMT_SMF.1/GPG	-	Not relevant
FMT_SMR.1	-	Not relevant
FMT_SMR.1/ADEL	-	Not relevant
FMT_SMR.1/CM	-	Not relevant
FMT_SMR.1/GPG	-	Not relevant
FMT_SMR.1/Installer	-	Not relevant
FPR_UNO.1	-	Not relevant
FPT_EMSEC.1	FPT_PHP.3	FPT_EMSEC.1 protects TOE against SPA, DPA timing attack, etc.
FPT_FLS.1	FPT_PHP.3	FPT_FLS.1 ensures that the TOE preserve secure state if potential security violation happens (as defined in FAU_ARP.1)
FPT_FLS.1/ADEL	-	Not relevant

Platform SFRs	Composite TOE SFRs	Comments
FPT_FLS.1/Installer	-	Not relevant
FPT_FLS.1/ODEL	-	Not relevant
FPT_RCV.3/Installer	-	Not relevant
FPT_RCV.3/SCP	FPT_PHP.3	FPT_RCV.3/SCP in case of power loss and card tearing ensures that the secure initial state is restored.
FPT_RCV.4/SCP	FPT_PHP.3	FPT_RCV.4/SCP ensures that in case of an interrupted reading or writing, the TOE recovers to a consistent and secure state.
FPT_TDC.1	-	Not relevant
FTP_ITC.1/CM	-	Not relevant

Table 5 Mapping of SFRs

The [2] requires applying different cryptographic standards as provided by the Platform of the TOE ([5]) related to FCSP_COP and FCS_CKM SFRs. The developer analysed the different standards and do not found any security relevant differences between the standards, because Platform's cryptographic standards were adopted by the referenced ones in the SFRs of this ST and [7].

The detailed analysis is summarized in the following table:

SFR from this ST	Standard from [2]	SFR from [5]	Standard from [5]	Comments
FCS_CKM.1p	[8] FIPS-180-2	FCS_COP.1.1/SHA	FIPS-180-4	Session key generation (hash function). [8] references to FIPS-180-4 as it is defined as a cryptographically strong hash function. FIPS 180- 4 superseded FIPS 180-2, so the usage of FIPS 180-4 is secure.
FCS_CKM.1e	[8]	FCS_COP.1.1/ECDH	ANSI X9.63	Ephemeral elliptic curve key pair generation. [8] states that its description of ECKA is conformance with ANSI X9.63

SFR from this ST	Standard from [2]	SFR from [5]	Standard from [5]	Comments
FCS_COP.1a	[8]	FCS_COP.1.1/ECDSA	ANSI X9.62	ECDSA digital signature generation [8] states that its description of ECDSA is conformance with ANSI X9.62.
FCS_COP.1h	[8]	FCS_COP.1.1/SHA	FIPS 180-4	Hash function for digital signature generation. [8] references to FIPS-180-4 as it is defined as a cryptographically strong hash function.
FCS_COP.1n	ISO/IEC 10116	FCS_COP.1.1/AES	SP800-38A	Encryption in AES-CBC mode. ISO/IEC 10116 includes all the modes specified in SP800-38A
FCS_COP.1e	[8]	FCS_COP.1.1/ECDH	ANSI X9.63	Key agreement. [8] states that its description of ECKA is conformance with ANSI X9.63
		FCS_COP.1.1/PACE_SUPP	[8]	Key agreement. No contradiction between the cryptographic standards.
FCS_COP.1hp	FIPS 180-2	FCS_COP.1.1/SHA	FIPS 180-4	Session key generation

SFR from this ST	Standard from [2]	SFR from [5]	Standard from [5]	Comments
				FIPS 180- 4 superseded FIPS 180-2, so the usage of FIPS 180-4 is secure.
FCS_COP.1mp	FIPS-197 SP800-38B	FCS_COP.1.1/AES-MAC	FIPS-197 SP800-38B	No contradiction between the cryptographic standards.
FCS_COP.1sp	FIPS 197 ISO/IEC 10116 SP 800-38B	FCS_COP.1/ACC_MAC	FIPS 197 SP800-38A	Secure messaging ISO/IEC 10116 includes all the modes specified in SP800-38A.
		FCS_COP.1/ACC_CYPHER	FIPS 197 SP800-38B	Secure messaging No contradiction between the cryptographic standards.

Table 6 Overview of applied cryptographic standards from [2] and [5]

3.7. Assurance Requirements

This ST requires EAL4 according to Common Criteria v3.1 R5 augmented by ALC_DVS.2 and AVA_VAN.5.

The [5] requires EAL5 according to Common Criteria v3.1 R4 augmented by ALC_DVS.2 and AVA_VAN.5.

As described above the [5] covers all assurance requirements of this ST.

4. Security Problem Definition

This chapter defines security problems related to the TOE. The security problems are defined from the three aspects: Threats (to be countered by the TOE and/or environment), Organizational security policies (to be handled by the TOE and/or environment), and Assumptions (to be met by the environment). The TOE and environment shall address these security problems in a proper way.

The threats, organizational security policies, and assumptions are named using an identifier with the prefix "T.," "P.," or "A.," respectively. Application note is added to individual description as required.

4.1. Threats

This section describes threats that a TOE shall counter. These threats shall be countered by the TOE, its operational environment or combination of these two.

T.Copy

An attacker trying to forge an ePassport may do so by reading personal information along with digital signature from the TOE and writing the copied data in an IC chip having the same functionality as that of the TOE. This attack damages the credibility of the entire passport booklet system including TOEs.

Application note 1 from [2]

If information retrieved from the legitimate TOE is copied into an illicit IC chip, as information stored in the TOE will be copied together with the associated digital signature, forgery protection by means of digital signature verification becomes ineffective. Since the original information can be protected against tampering by means of digital signature, passport forgery may be detected by means of comparative verification of the facial image. However, it is difficult to surely detect forged passport just by comparing the facial image.

T.Logical_Attack

In the operational environment after issuing a TOE embedded passport booklet, an attacker who can read the MRZ data of the passport booklet may try to read confidential information (Active Authentication Private Key) stored in the TOE through the contactless communication interface of the TOE.

Application note 2 form [2]

If an attacker has physical access to a passport booklet, the attacker can visually read personal information printed on the passport booklet and optically read the printed MRZ data. Since the security functions of the TOE cannot prevent such sort of readings, the information and data stated above is not included in the threat-related assets to be protected by the TOE. In other words, the intended meaning of the threat here is an attack aimed to read confidential information (Active Authentication Private Key) stored in the TOE by having access to the said TOE through the contactless communication interface using data that the attacker has read from the MRZ.

T.Communication_Attack

In the operational environment after issuing a TOE embedded passport booklet, an attacker who does not know about MRZ data may interfere with the communication between the TOE and a terminal to disclose and/or alter communication data that should be concealed.

Application note 3 from [2]

As for an attack which interferes with communication between a terminal and a passport booklet, it is considered impossible that the attacker physically accesses the target passport booklet without being noticed by the passport holder and/or an immigration official. An attacker can obtain MRZ data only

when the passport booklet is physically accessible. Therefore, the attacker mentioned here is assumed to be unaware of the MRZ data.

T.Physical_Attack

In the operational environment after issuing a TOE embedded passport booklet, an attacker may attempt to disclose confidential information (Active Authentication Private Key) stored in the TOE, unlock the state of the locked key, or reactivate a deactivated access control function by physical means. This physical means include both of non-destructive attacks made without impairing the TOE functions and destructive attacks made by destroying part of the TOE to have mechanical access to the inside of the TOE.

Application note 4 from [2]

An attacker may attempt to read confidential information (Active Authentication Private Key) or rewrite information stored in the TOE through physical access to the TOE. Making such a physical attack may impair the security function operated by the TOE program to provide the original functionality thereof, resulting in potential violation of SFR. The example of non-destructive attacks includes measurements on leaked electromagnetic wave associated with the TOE operation and induction of malfunctions in security functions by applying environmental stress (e.g. changes in temperature or clock, or application of high-energy electromagnetic fields) to the TOE in operation. The example of destructive attacks shows those collecting, analyzing, and then disclosing confidential information by probing and manipulating the internal circuit. Test pins and power supply pins left in the TOE may be used to make the said attacks. The TOE that has been subject to a destructive attack may not be reused as an ePassport IC. Even in such case, however, the disclosed private key may be abused to forge TOEs.

4.2. Organizational Security Policies

This section describes organizational security policies that apply to TOEs and operational environment. In the ST, the organizational security policies include conformance to the standards provided by ICAO and conditions required by the passport issuing authorities in Japan.

P.PACE

In the operational environment after issuing a TOE embedded passport booklet, the TOE shall allow a terminal to read a certain information from the TOE in accordance with the PACE procedure defined by Part 11 of [1]. This procedure includes mutual authentication and Secure Messaging between the TOE and terminal devices. TOE files to be read are EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, and EF.SOD under the rules stated above. As for any files under the same rules except the files stated above, the handling of such files which are not listed in the ST is not defined.

P.Authority

The TOE under the control of the passport issuing authorities shall allow only authorized users (persons who succeeded in verification of readout key, transport key, or Active Authentication Information Access Key) to have access to the internal data of the TOE, as shown in Table 7.

Authentication status[2]	File subject to access control	Operation permitted	Reference: Data to be operated
Successful verification with readout key	EF.DG13[3]	Read	IC chip serial number (entered by manufacturer)
Successful verification with transport key	Transport key file	Write	Transport key data (update of old data)
	Password key file		Password key
	EF.DG1	Read or write	MRZ data
	EF.DG2		Facial image
	EF.DG13[3]		Management data (Passport number and Booklet management number)
	EF.DG14		PACE v2 Security information Active Authentication hash function information
	EF.COM[4]		Common data
	EF.SOD		Security data related to Passive Authentication defined by Part of [1].
	EF.CardAccess	Write	PACE v2 Security information
	EF.DG15	Read	Active Authentication Public Key
Successful verification with Active Authentication Information Access Key	EF.DG15	Write	Active Authentication Public Key
	Private key file		Active Authentication Private Key

Table 7 Internal data of the TOE access control by passport issuing authorities

[2]The readout key, transport key, and Active Authentication Information Access Key are configured by the manufacturer. The transport key can be changed (updated) by an authorized user. With regard to the files subject to access control included in this table and files storing the read key and Active Authentication Information Access Key which may vary the authentication status, user access that is not stated in this table or Notes is prohibited. (The access controls to information in the TOE from terminals after issuing a TOE embedded passport booklet to the passport holder, i.e., PACE are separately specified.

[3]In EF.DG13, an IC chip serial number has been recorded by the manufacturer, and the management data is appended to the file by the passport issuing authorities.

[4]EF.COM file may not be created according to the passport issuing authorities' instructions.

All files stated in the table above store user data or TSF data. The transport key file stores TSF data, and all other files store user data (cryptographic keys are managed as user data). The TSF data file is not included in files subject to access control stated in Security Requirements, but treated in FMT_MTD.1.

P.Data_Lock

When the TOE detects a failure in authentication with the transport key, readout key or Active Authentication Information Access Key, it will permanently disable authentication related to each key, thereby prohibiting reading, or writing the file based on successful authentication thereof. Table 7 shows the relationship between the key used for authentication and its corresponding file in the TOE.

P.Prohibit

Any and all writings to the files in the TOE and readings from the files in the TOE based on successful authentication with readout key are prohibited after issuing an ePassport to the passport holder. Disabling authentication through authentication failure with the transport key, readout key, and Active Authentication Information Access Key (see P.Data_Lock) shall be used as the means for that purpose.

4.3. Assumptions

This section describes assumptions to be addressed in the operational environment of TOEs. These assumptions need to be true for TOE's security functionality becomes effective.

A.Administrative_Env

The TOE that was delivered from the TOE manufacturer to the passport issuing authorities and is under the control of the authorities shall be securely controlled and go through an issuing process until it is finally issued to the passport holder.

A.PKI

In order for the passport inspection authorities of the receiving state or organization to verify the authenticity of information that has been digitally signed by the passport issuer and stored in the TOE (including the Active Authentication Public Key), the interoperability of the PKI environment both of the issuing and receiving states or organizations of the passport shall be maintained by passport issuing authorities.

5. Security Objectives

This chapter describes security objectives for TOEs and its environment for the security problems described in Chapter 4. Section 5.1 describes the security objectives to be addressed by the TOEs, while

Section 5.2 describes those to be addressed by its environment. In addition, Section 5.3 describes rationales for the appropriateness of the security objectives for solving the security problems.

The security objectives for the TOEs and the security objectives for the operational environment are represented by an identifier with the prefix "O." or "OE." respectively.

5.1. Security Objectives for the TOE

This section describes security objectives that TOEs should address to solve problems with regard to the threats and organizational security policies that are defined as the security problems.

O.AA

TOEs shall provide a means to verify the authenticity of the IC chip itself that composes the TOE in order to prevent the copy of personal information including the digital signature on an illicit IC chip and the forgery of the passport. This means shall be standardized so as to ensure the global interoperability of ePassport and, for this purpose, shall support the Active Authentication defined by Part 11 of [1].

O.Logical_Attack

TOEs shall, under any circumstances, prevent confidential information in them (Active Authentication Private Key) from being externally read through the contactless communication interface of the TOE.

O.Physical_Attack

TOEs shall prevent the confidential information (Active Authentication Private Key) within the TOEs from being disclosed or the information relating to the security from being tampered with by the attackers using physical means. TOEs shall counter attacks applicable to TOEs themselves out of known attacks against IC chips, considering physical means including both non-destructive attacks and destructive attacks.

O.PACE

This security objective applies to the operational environment after issuing the passport booklet. PACE procedure defined by Part 11 of [1], if the terminals require, shall be used to ensure the global interoperability of the ePassport. This procedure shall be used in the mutual authentication and Secure Messaging between the TOE and terminals. Information the terminal reads from the TOE is stored in the EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, and EF.SOD files among the files contained in the rules stated above. The TOE shall permit only the terminal that has succeeded in mutual authentication to read the files stated above. As for any files under the same rules except the files stated above, the handling of such files which are not listed in the ST is not defined.

O.Authority

The TOE shall limit users who can access the internal TOE data and their operations, in the environment under the control of the passport issuing authorities according to Table 7 described in the organizational security policy P.Authority.

O.Data_Lock

The operation of the internal TOE data shall be available only to the authorized user (i.e., authorized personnel under the control of the passport issuing authorities or the terminal after issuing the passport) to prevent illicit reading and writing by any users other than those stated above. As a means for this purpose, if the TOE detects an authentication failure with the readout key, transport key, or Active Authentication Information Access Key, it shall be permanently prohibited to read and to write the internal TOE data permitted according to authentication related to each of the said keys. This security objective shall also apply in the event that the passport issuing authorities disable readout key, transport key, or Active Authentication Information Access Key by causing an authentication failure intentionally before the TOE is issued to the passport holder. The relationship between the readout key, transport key, and Active Authentication Information Access Key and their corresponding internal TOE data is as listed in Table 7 of the organizational security policy P.Authority. After the security objective O.Data_Lock is achieved, only the access to TOE stated in the security objective O.PACE is permitted.

5.2. Security Objectives for the Operational Environment

This section describes security objectives that TOEs should address in the operational environment to solve problems regarding the threats and organizational security policies and assumptions defined as the security problems.

OE.Administrative_Env

The TOEs under the control of the passport issuing authorities are subjected to secure management and treatment until each of these TOEs is delivered to the passport holder through the issuing procedures.

OE.PKI

In order for the ePassport inspection authorities of the receiving state or organization to verify the authenticity of information that has been digitally signed by the passport issuing state or organization and stored in the TOE (i.e., information on the passport holder and the Active Authentication Public Key), passport issuing authorities shall maintain the interoperability of the PKI environment in both the passport issuing state and receiving state.

5.3. Security Objectives Rationales

This chapter describes rationales for the effectiveness of the security objectives stated above for individual parameters of the security problem definition. Section 5.3.1 describes that each of the security objective can be traced back to any of the security problems, while Section 5.3.2 describes that any of the security problems is effectively addressed by the corresponding security objective.

5.3.1. Correspondence between Security Problem Definition and Security Objectives

Table 8 shows the correspondence between the security problem definition and the security objectives. As shown in the table, all security objectives can be traced back to one (or more) item(s) in the security problem definition.

Security Problem Definition / Security objective	O.AA	O.Logical_Attack	O.Physical_Attack	O.PACE	O.Authority	O.Data_Lock	OE.Administrative_Env	OE.PKI
T.Copy	X	-	-	-	-	-	-	-
T.Logical_Attack	-	X	-	-	-	-	-	-
T.Communication_Attack	-	-	-	X	-	-	-	-
T.Physical_Attack	-	-	X	-	-	-	-	-
P.PACE	-	-	-	X	-	-	-	-
P.Authority	-	-	-	-	X	-	-	-
P.Data_Lock	-	-	-	-	-	X	-	-
P.Prohibit	-	-	-	-	-	X	-	-
A.Administrative_Env	-	-	-	-	-	-	X	-
A.PKI	-	-	-	-	-	-	-	X

Table 8 Correspondence between security problem definition and security objectives

5.3.2. Security Objectives Rationale

This section describes rationales for the security objectives for the TOE and the operational environment to thoroughly counter all identified threats, implement organizational security policies, and properly meet the assumptions.

T.Copy

If an attacker copies the personal information (with digital signature) read from the TOE to the IC chip having the same functionality as that of the TOE, the forged passport cannot be detected through the verification of digital signature. To prevent this attack, the security objective for the TOE: O.AA addresses embedding of data that enables verifying the authenticity of the IC chip itself in the TOE.

This enables the TOE to detect illicit IC chips and prevent the forgery of passports, thus removing the threat of T.Copy.

T.Logical_Attack

The security objective for the TOE: O.Logical_Attack makes it possible to prohibit reading confidential information (Active Authentication Private Key) in the TOE through the contactless communication interface of the TOE, under any circumstances.

Thus, the threat of T.Logical_Attack is removed.

T.Communication_Attack

The security objectives for the TOE: O.PACE make it possible to use a secure communication path for the communication between the terminals and the TOE. Thus, the threat of disclosure and alteration of the communication data of T.Communication_Attack can be diminished to an adequate level for the practical use.

T.Physical_Attack

The security objective for the TOE: O.Physical_Attack makes it possible to counter an attack to disclose confidential information (Active Authentication Private Key) in the TOE or tamper security-related information not via the contactless communication interface of the TOE but physical means. Regarding the physical means, both non-destructive attacks and destructive attacks are considered, and countermeasures shall be implemented so that the TOE can counter known attacks against the IC chip.

Thus, the threat can be diminished to an adequate level for the practical use.

P.PACE

The security objective for the TOE: O.PACE allows only the authorized personnel (terminal) to read the internal TOE data through a secure communication path by applying PACE procedure defined by Part 11 of [1]. O.PACE includes all contents of P.PACE, thus the organizational security policy P.PACE is properly implemented.

P.Authority

The security objective for the TOE: O.Authority provides the contents to directly implement the organizational security policy P.Authority.

P.Data_Lock

The security objective for the TOE: O.Data_Lock includes the contents required by the organizational security policy P.Data_Lock and properly implements P.Data_Lock.

P.Prohibit

The organizational security policy P.Prohibit requires the implementation of an intentional authentication failure by the authorized TOE user as the implementation means. Actions required for the TOE to address P.Prohibit are the same as those for the organizational security policy P.Data_Lock that has assumed an illicit attack on the TOE. Therefore, the security objective for the TOE: O.Data_Lock will also implement the contents of P.Prohibit.

A.Administrative_Env

The security objective for the operational environment: OE.Administrative_Env directly corresponds to the assumption A.Administrative_Env, thus this assumption is met.

A.PKI

The security objective for the operational environment: OE.PKI directly corresponds to the assumption A.PKI, thus this assumption is met.

6. Extended Components Definition

The ST uses the following extended components, which is defined by [2].

6.1. FCS_RND: Random number generation

Family Behaviour

This family defines quality requirements for the generation of random numbers to be used for cryptographic purposes.

Component levelling

FCS_RND: Random number generation	1

FCS_RND.1 Random number generation requires the random numbers to meet defined quality standards.

Management: FCS_RND.1

There is no management activity foreseen.

Audit: RCS_RND.1

There is no auditable event foreseen.

FCS_RND.1 Quality standards for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a random number generation mechanism that meet [assignment: *defined quality standard*].

7. Security Requirements

7.1. Security Functional Requirements

Table 9 shows the list of the security functional requirements (SFRs) of the ST.

Chapter No.	Identifier name	
7.1.1	FCS_CKM.1p	Cryptographic key generation (PACE, session keys)
7.1.2	FCS_CKM.1e	Cryptographic key generation (PACE, ephemeral key pairs)
7.1.3	FCS_CKM.4	Cryptographic key destruction
7.1.4	FCS_COP.1a	Cryptographic operation (Active Authentication, signature generation)
7.1.5	FCS_COP.1h	Cryptographic operation (Active Authentication, hash functions)
7.1.6	FCS_COP.1n	Cryptographic operation (Nonce encryption)
7.1.7	FCS_COP.1e	Cryptographic operation (Key agreement)
7.1.8	FCS_COP.1hp	Cryptographic operation (PACE, hash functions)
7.1.9	FCS_COP.1mp	Cryptographic operation (PACE, mutual authentication)
7.1.10	FCS_COP.1sp	Cryptographic operation (PACE, Secure Messaging)
7.1.11	FCS_RND.1	Quality standards for random numbers
7.1.12	FDP_ACC.1a	Subset access control (Issuance procedure)
7.1.13	FDP_ACC.1p	Subset access control (PACE)
7.1.14	FDP_ACF.1a	Security attribute based access control (Issuance procedure)
7.1.15	FDP_ACF.1p	Security attribute based access control (PACE)
7.1.16	FDP_ITC.1	Import of user data without security attributes
7.1.17	FDP_UCT.1p	Basic data exchange confidentiality (PACE)
7.1.18	FDP_UIT.1p	Data exchange integrity (PACE)
7.1.19	FIA_AFL.1a	Authentication failure handling (Active Authentication Information Access Key)
7.1.20	FIA_AFL.1d	Authentication failure handling (Transport key)
7.1.21	FIA_AFL.1r	Authentication failure handling (Readout key)
7.1.22	FIA_UAU.1	Timing of authentication
7.1.23	FIA_UAU.4	Single-use authentication mechanisms
7.1.24	FIA_UAU.5	Multiple authentication mechanisms
7.1.25	FIA_UID.1	Timing of identification
7.1.26	FMT_MTD.1	Management of TSF data
7.1.27	FMT_SMF.1	Specification of management functions
7.1.28	FMT_SMR.1	Security roles
7.1.29	FPT_PHP.3	Resistance to physical attack
7.1.30	FTP_ITC.1	Inter-TSF trusted channel

Table 9 List of SFRs

SFR is defined by performing as-needed operation on the security functional component defined by [9]. The operation is denoted for each SFR by the following method:

- SFR subject to iteration operation is identified by adding a low-case alphabetic character such as "a" and a parenthesized brief description showing the purpose of SFR (e.g. "Active Authentication") after the corresponding component identifier.
- The point of assignment or selection operation is shown as [assignment: *XXX* (italicized)] or [selection: *XXX* (italicized)]. Refinement is also italicized.
- For the selection operation, items not subject to selection are shown by strike-through (~~Strikethrough~~).
- The [2] has some uncompleted operations, which are shown as [assignment: *XXX* (Italicized and underlined) in [2]. The ST author completed these uncompleted operations with same denotation in this document.

The following section describes SFRs of the TOE

7.1.1. FCS_CKM.1p

Cryptographic key generation (PACE, session keys)

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1p	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: S*ession key generation algorithm in PACE specified by Part 11 of* [1] *and* [8]] and specified cryptographic key sizes [assignment: *128 bits and 256 bits*] that meet [assignment: *Standards for session key generation in PACE specified by Part 11 of* [1] *and* [8]].

7.1.2. FCS_CKM.1e

Cryptographic key generation (PACE, ephemeral key pairs)

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1e	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *Elliptic Curve Key Pair Generation*] and specified cryptographic key sizes [assignment: *256 bits and*](#)

384 bits] that meet [assignment: S*tandards for the key pair generation specified by* [8]].

7.1.3. FCS_CKM.4

Cryptographic key destruction

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *[selection: ~~method for erasing cryptographic keys on volatile memory by shutting down power supply, overwriting new cryptographic key data, or~~ [assignment: physically overwriting the keys with zeros]]*] that meets the following: [assignment:*none*].

Application note 6 (from ST author)

FCS_CKM.4 covers the destruction of password key, PACE session Keys ,PACE ephemeral key pair and Active Authentication private key in volatile memory.

7.1.4. FCS_COP.1a

Cryptographic operation (Active Authentication, signature generation)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1a	The TSF shall perform [assignment: *generation of digital signature for Active Authentication data*] in accordance with a specified cryptographic algorithm [assignment: *ECDSA*] and cryptographic key sizes [assignment: *256 bits and 384 bits]* that meet the following: [assignment: *the Digital Signature Standards specified by* [8]].

Application note 7 from [2]

Only the combination of 256 bits and SHA-256 or that of 384 bits and SHA-384 is permitted as the key sizes for this requirement and the hash algorithm of FCS_COP.1h.

7.1.5. FCS_COP.1h

Cryptographic operation (Active Authentication, hash functions)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1h The TSF shall perform [assignment: *generation of data for Active Authentication*] in accordance with a specified cryptographic algorithm [assignment: *SHA-256 and SHA-384*] and cryptographic key sizes [assignment: *none*] that *meet the following: [assignment: the Digital Signature Standards specified by* [8]].

7.1.6. FCS_COP.1n

Cryptographic operation (Nonce encryption)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1n The TSF shall perform [assignment: *nonce encryption*] in accordance with a specified cryptographic algorithm [assignment: *AES-CBC*] and cryptographic key sizes [assignment: *128 bits and 256 bits*] that meet the following: [assignment*: Standards for the PACE procedure specified by Part 11 of* [1]].

7.1.7. FCS_COP.1e

Cryptographic operation (Key agreement)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1e The TSF shall perform [assignment: *key agreement*] in accordance with a specified cryptographic algorithm [assignment: *ECDH*] and cryptographic key sizes [assignment: *256 bits and 384 bits*] that meet the following: [assignment: *Standards for the PACE procedure specified by Part 11 of* [1]].

7.1.8. FCS_COP.1hp

Cryptographic operation (PACE, hash functions)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1hp The TSF shall perform [assignment: *generation of session keys for PACE*] in accordance with a specified cryptographic algorithm [assignment: *SHA-1 and SHA-256*] and cryptographic key sizes [assignment: *none*] that meet the following: [assignment: *Standards for session key generation in PACE specified by Part 11 of* [1]].

7.1.9. FCS_COP.1mp

Cryptographic operation (PACE, mutual authentication)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1mp	The TSF shall perform [assignment: *authentication token generation and verification*] in accordance with a specified cryptographic algorithm [assignment: *AES-CMAC*] and cryptographic key sizes [assignment: *128 bits and 256 bits*] that meet the following: [assignment: *Standards for mutual authentication included in PACE specified by Part 11 of* [1]].

7.1.10. FCS_COP.1sp

Cryptographic operation (PACE, Secure Messaging)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1sp	The TSF shall perform [assignment: *cryptographic operation shown in Table 10*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm shown in Table 10*] and cryptographic key sizes [assignment: *cryptographic key sizes shown in Table 10*] that meet the following: [assignment: *Standards for Secure Messaging included in PACE specified by* [1]].

Cryptographic algorithm	*Cryptographic key sizes*	*Cryptographic operation*
AES in CBC mode	*128 bits and 256 bits*	*Message encryption and decryption*
AES-CMAC	*128 bits and 256 bits*	*Generation and verification of Message Authentication Code*

Table 10 Cryptographic mechanisms in Secure Messaging (PACE)

Application note 8 from [2]

Whether Secure Messaging is applied or not depends on the type of commands. Therefore, data encryption and message authentication codes are not necessarily applied to all commands and responses.

7.1.11. FCS_RND.1

Quality standards for random numbers

Hierarchical to:	No other components.
Dependencies:	No dependencies

FCS_RND.1.1 The TSF shall provide a random number generation mechanism that meet the following: [assignment:*DRG.4 according to BSI-AIS20 v2.1*].

7.1.12. FDP_ACC.1a

Subset access control (Issuance procedure)

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1a The TSF shall enforce the [assignment: *Issuance procedure access control SFP*] on [assignment: *Subject[User process], Objects [Files shown in Table 7 of Organizational security policy P.Authority] and List of operations among subjects and objects addressed by SFP [Data Input/Output operation to/from object]*].

7.1.13. FDP_ACC.1p

Subset access control (PACE)

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1p The TSF shall enforce the [assignment: *PACE SFP*] on [assignment: *Subject[Process on behalf of terminal], Objects [Files EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM , EF.SOD, password key file, transport key file, and private key file*] *and list of operations among subjects and objects addressed by SFP* [*Reading data from object]*].

Application note 9 from [2]

PACE SFP is the access control policy applied after succeeding in mutual authentication based on PACE.

7.1.14. FDP_ACF.1a

Security attribute based access control (Issuance procedure)

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1a The TSF shall enforce the [assignment: *Issuance procedure access control SFP*] to objects based on the following: [assignment: *Subject controlled under the indicated SFP [User process], objects [Files shown in Table 7 of the organizational security policy P.Authority*], *and, the SFP-relevant security attributes* [*Authentication status shown in Table 7 of the organizational security policy P.Authority] according to each*].

FDP_ACF.1.2a The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *When the authentication status shown in Table 7 of the organizational security policy P.Authority is met, an operation to the file associated with the said authentication status is allowed*].

FDP_ACF.1.3a	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *none*].
FDP_ACF.1.4a	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *Access to files that are not listed in Table 7 of the organizational security policy P.Authority is prohibited.*].

7.1.15. FDP_ACF.1p

Security attribute based access control (PACE)

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1p	The TSF shall enforce the [assignment: *PACE SFP*] to objects based on the following: [assignment: *Subject controlled under the indicated SFP [Process on behalf of terminal], objects [Files EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, EF.SOD, password key file, transport key file, and private key file], and the SFP-related security attributes [Authentication status of terminal based on mutual authentication]*].
FDP_ACF.1.2p	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *Where the authentication status of terminal has been successful, subjects are allowed to read data from objects*].
FDP_ACF.1.3p	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *none*].
FDP_ACF.1.4p	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment*: Subjects are prohibited to write data to or read data from the transport key file, password key file, and private key file*].

7.1.16. FDP_ITC.1

Import of user data without security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation
FDP_ITC.1.1	The TSF shall enforce the [assignment: *Issuance procedure access control SFP*] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *none*].

7.1.17. FDP_UCT.1p

Basic data exchange confidentiality (PACE)

Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]
FDP_UCT.1.1p	The TSF shall enforce of [assignment: *PACE SFP*] to [selection: *transmit, receive*] user data in a manner protected from unauthorised disclosure.

7.1.18. FDP_UIT.1p

Data exchange integrity (PACE)

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path]
FDP_UIT.1.1p	The TSF shall enforce the [assignment: *PACE SFP*] to [selection: *transmit, receive*] user data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors.
FDP_UIT.1.2p	The TSF shall be able to determine, on receipt of user data, whether [selection*: modification, deletion, insertion, replay*] has occurred.

7.1.19. FIA_AFL.1a

Authentication failure handling (Active Authentication Information Access Key)

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1a	The TSF shall detect when [selection: [assignment: *3*]~~, *an administrator configurable positive integer within [assignment: range of acceptable values]*~~] unsuccessful authentication attempts occur related to [assignment: *authentication with the Active Authentication Information Access Key*].
FIA_AFL.1.2a	When the defined number of unsuccessful authentication attempts has been [selection: *met*~~*, surpassed*~~], the TSF shall [assignment: *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'')*].

7.1.20. FIA_AFL.1d

Authentication failure handling (Transport key)

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1d The TSF shall detect when [selection: [assignment: *3*], ~~*an administrator configurable positive integer within [assignment: range of acceptable values]*~~] unsuccessful authentication attempts occur related to [assignment: *authentication with the transport key*].

FIA_AFL.1.2d When the defined number of unsuccessful authentication attempts has been [selection: *met*, ~~*surpassed*~~], the TSF shall [assignment: *permanently stop authentication with the transport key (fix the authentication status with the transport key to ''Not authenticated yet'')*].

7.1.21. FIA_AFL.1r

Authentication failure handling (Readout key)

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1r The TSF shall detect when [selection: [assignment: *3*], ~~*an administrator configurable positive integer within [assignment: range of acceptable values]*~~] unsuccessful authentication attempts occur related to [assignment: *authentication with the readout key*].

FIA_AFL.1.2r When the defined number of unsuccessful authentication attempts has been [selection: *met*, ~~*surpassed*~~], the TSF shall [assignment: *permanently stop authentication with the readout key (fix the authentication status with the readout key to ''Not authenticated yet'')*].

7.1.22. FIA_UAU.1

Timing of authentication

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [assignment: *readout of EF.CardAccess and EF.ATR/INFO*], on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

7.1.23. FIA_UAU.4

Single-use authentication mechanisms

Hierarchical to: No other components.
Dependencies: No dependencies

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [assignment: *mutual authentication mechanism with the PACE procedure*].

7.1.24. FIA_UAU.5

Multiple authentication mechanisms

Hierarchical to: No other components.
Dependencies: No dependencies

FIA_UAU.5.1 The TSF shall provide [assignment: *multiple authentication mechanisms shown in Table 11*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [assignment: *rules describing how the multiple authentication mechanisms shown in Table 11 provide authentication*].

Authentication mechanism name	*Rule applicable to authentication mechanism*
Transport Key	*Rule of authenticating the authorized personnel of the passport issuing authorities by verifying transport key that have been already stored in the TOE.*
Readout Key	*Rule of authenticating the authorized personnel of the passport issuing authorities by verification with readout key that have been already stored in the TOE*
Active Authentication Information Access Key	*Rule of authenticating the authorized personnel of the passport issuing authorities by verification with Active Authentication Information Access Key that have been already stored in the TOE.*
Mutual authentication	*Rule of authenticating terminals according to the mutual authentication procedure in PACE defined by* [1]

Table 11 Multiple authentication mechanisms

7.1.25. FIA_UID.1

Timing of identification

Hierarchical to: No other components.
Dependencies: No dependencies

FIA_UID.1.1 The TSF shall allow [assignment: *readout of EF.CardAccess and EF.ATR/INFO*], on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

7.1.26. FMT_MTD.1

Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: ~~*change_default, query,* modify, delete, clear, [assignment: other operations]~~] the [assignment: *transport key*] to [assignment: *the authorized personnel of the passport issuing authorities*].

Application note 10 from [2]

This requirement has to do with the configuration of transport key used to transport the TOE from the passport booklet manufacturer to a regional passport office in Phase 3. In this requirement, the authorized personnel who are allowed to manage TSF data are the staff of the passport manufacturer. The staff has no chance to rewrite the transport key after the TOE has been transported to the regional passport office.

On the other hand, when the TOE is located in either the passport manufacturer or a regional passport office, there is also no threat that an attacker illicitly rewrites the transport key. Therefore, there is no necessity to distinguish between the staff of the National Printing Bureau and that of the regional passport office. For this reason, this requirement makes no distinction between them and refers the authorized administrator as the "authorized personnel of the passport issuing authorities".

7.1.27. FMT_SMF.1

Specification of management functions

Hierarchical to:	No other components.
Dependencies:	No dependencies

FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [assignment: *modification of transport key*].

7.1.28. FMT_SMR.1

Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification

FMT_SMR.1.1	The TSF shall maintain the roles [assignment: *authorized personnel of the passport issuing authorities*].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

7.1.29. FPT_PHP.3

Resistance to physical attack

Hierarchical to:	No other components.
Dependencies:	No dependencies

FPT_PHP.3.1	The TSF shall resist [assignment: *attacks defined by the CC Supporting Documents related to Smartcards*] to the [assignment: *hardware of the TOE and software composing the TSF*] by responding automatically such that the SFRs are always enforced.

Application note 11 from [2]

The [2] requires the following: "The supporting documents that are the latest version at the time of the evaluation for the TOE are applied." The document at the time of ST issuance is the "Application of Attack Potential to Smartcards, Version 2.9, May 2013."

7.1.30. FTP_ITC.1

Inter-TSF trusted channel

Hierarchical to:	No other components.
Dependencies:	No dependencies

FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit [selection: ~~*the TSF,*~~ *another trusted IT product*] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [assignment*: reading data from the TOE*].

Application note 12 from [2]

Communication between terminal and TSF shall be performed via the Secure Messaging channel defined by [1]. After the Secure Messaging channel is established, only the Secure Messaging channel is to be available for the communication path between terminal and TOE.

7.2. Security Assurance Requirements

Security assurance requirements applicable to this TOE are defined by assurance components shown in Table 12. These components are all included in CC Part 3. Components except ALC_DVS.2 and AVA_VAN.5 are included in the EAL4 assurance package. ALC_DVS.2 is a high-level component of ALC_DVS.1 and AVA_VAN.5 is a high-level component of AVA_VAN.3.

The [2] and the current ST apply no operation to all components shown in Table 12.

Assurance class	Assurance component
Security target evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Development	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3
Guidance documents	AGD_OPE.1
	AGD_PRE.1
Life-Cycle support	ALC_CMC.4
	ALC_CMS.4

Assurance class	Assurance component
	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.1
Tests	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability assessment	AVA_VAN.5

Table 12 Assurance components

7.3. Security Requirements Rationale

7.3.1. Security Functional Requirements Rationale

This chapter describes rationales for that the defined SFRs properly achieve the security objectives for the TOE.

Section 7.3.1.1 describes that each of the SFRs can be traced back to any of the security objectives for the TOE, while Section 7.3.1.2 describes that each of the security objectives for the TOE is properly met by the corresponding effective SFR.

7.3.1.1. Tracing between Security Objectives and Security Functional Requirements

Table 13 shows the SFRs corresponding to the security objectives for the TOE. This table provides the rationales for the traceability of all SFRs to at least one security objective for the TOE.

	O.Logical_Attack	O.Physical_Attack	O.AA	O.PACE	O.Authority	O.Data_Lock
FCS_CKM.1p	-	-	-	X	-	-
FCS_CKM.1e	-	-	-	X	-	-
FCS_CKM.4	-	-	X	X	-	-
FCS_COP.1a	-	-	X	-	-	-
FCS_COP.1h	-	-	X	-	-	-
FCS_COP.1n	-	-	-	X	-	-
FCS_COP.1e	-	-	-	X	-	-
FCS_COP.1hp	-	-	-	X	-	-
FCS_COP.1mp	-	-	-	X	-	-
FCS_COP.1sp	-	-	-	X	-	-
FCS_RND.1	-	-	-	X	-	-
FDP_ACC.1a	-	-	X	-	X	-
FDP_ACC.1p	X	-	-	X	-	-
FDP_ACF.1a	-	-	X	-	X	-
FDP_ACF.1p	X	-	-	X	-	-

	O.Logical_Attack	O.Physical_Attack	O.AA	O.PACE	O.Authority	O.Data_Lock
FDP_ITC.1	-	-	X	X	X	-
FDP_UCT.1p	-	-	-	X	-	-
FDP_UIT.1p	-	-	-	X	-	-
FIA_AFL.1a	-	-	-	-	-	X
FIA_AFL.1d	-	-	-	-	-	X
FIA_AFL.1r	-	-	-	-	-	X
FIA_UAU.1	-	-	-	X	X	-
FIA_UAU.4	-	-	-	X	-	-
FIA_UAU.5	-	-	-	X	X	-
FIA_UID.1	-	-	-	X	X	-
FMT_MTD.1	-	-	-	-	X	-
FMT_SMF.1	-	-	-	-	X	-
FMT_SMR.1	-	-	-	-	X	-
FPT_PHP.3	-	X	-	-	-	-
FTP_ITC.1	-	-	-	X	-	-

Table 13 Tracing between security objectives for the TOE and SFRs

7.3.1.2.Justification for the tracing

This section describes rationales for that the security objectives for the TOE are met by their corresponding SFRs and, at the same time, indicates that individual SFRs have effectiveness in meeting the security objectives for the TOE.

O.AA

To achieve the security objective O.AA, it shall address the Active Authentication procedure defined by Part 11 of [1]. This Active Authentication is a process for a terminal to authenticate the IC chip of the TOE, and the TOE itself is not required to provide any authentication mechanism. The TOE is authenticated by properly responding the authentication procedure. To meet requirements for the authentication procedure from the terminal, the TOE incorporates the public key and private key pair, performs cryptographic operation using the private key defined by FCS_COP.1a, and hashing operation defined by FCS_COP.1h. The public key and private key pair are imported to the TOE by FDP_ITC.1. Access control associated with FDP_ITC.1 is defined by FDP_ACC.1a and FDP_ACF.1a. Destruction of the private key on RAM is defined by FCS_CKM.4.

The security objective O.AA is sufficiently achieved by the said SFRs.

O.Logical_Attack

Confidential information (Active Authentication Private Key) subject to protection is stored in the private key file of the TOE. It is denied for the user process on behalf of the terminal to read data from the private key file, by FDP_ACC.1p and FDP_ACF.1p applied to the TOE after issuing the TOE embedded passport.

The security objective O.Logical_Attack is sufficiently achieved by the said SFRs.

O.Physical_Attack

Attack scenarios trying to disclose the Active Authentication Private Key that is confidential information, and to tamper security-related information within the TOE, by physical means are stated in the list of attacks shown in the FPT_PHP.3 section. The TSF automatically resists the attacks according to FPT_PHP.3 to protect against the disclosure of the confidential information. With that, the security objective O.Physical_Attack is sufficiently achieved.

O.PACE

FIA_UID.1 and FIA_UAU.1 provide the TOE service for the user who has succeeded in identification and authentication. User authentication requires the mutual authentication procedure with PACE defined by ICAO, which is defined by FIA_UAU.5. The mutual authentication procedure requires new authentication data based on a random number for each authentication, which is defined by FIA_UAU.4. Likewise, Secure Messaging required by PACE is defined by the requirements for the protection of transmitted and received data by FDP_UCT.1p and FDP_UIT.1p, and the requirement of cryptographic communication channels by FTP_ITC.1. Furthermore, with regard to cryptographic processing required for the PACE procedure, FCS_COP.1mp defines cryptographic operations necessary for the mutual authentication procedure and FCS_COP.1sp defines cryptographic operations for Secure Messaging. With regard to the cryptographic keys used for Secure Messaging, FDP_ITC.1 defines the import of password key, FCS_CKM.1e defines the generation of ephemeral key pairs, FCS_COP.1e defines the key agreement, FCS_CKM.1p and FCS_COP.1hp define the generation of session keys, FCS_RND.1 defines the generation of random numbers such as random Nonce, FCS_COP.1n defines the encryption of Nonce, and FCS_CKM.4 defines the destruction of these keys. In order for only permitted personnel to read given information from the TOE, rules governing access control with FDP_ACC.1p and FDP_ACF.1p are defined.

O.PACE is sufficiently achieved by the said SFRs.

O.Authority

During the TOE process done by the passport issuing authorities, the identification and authentication requirements FIA_UID.1 and FIA_UAU.1 are applied in order to grant the processing authority only to the duly authorized user. As for the user authentication mechanisms, FIA_UAU.5 defines the use of the transport key, readout key, or Active Authentication Information Access Key. If a user is successfully authenticated by the verification with the key, the user is permitted to access to the internal data of the TOE defined by O.Authority, applying the access control rule FDP_ACC.1a and FDP_ACF.1a. The user operation includes writing of the authentication key (transport key), cryptographic keys (Active Authentication Public Key and private key pair and password key for Secure Messaging), and other user data in the TOE. The association between objects and security attributes when writing is defined by FDP_ITC.1. O.Authority includes updating (rewriting) of the transport keys by the authorized personnel of the passport issuing authorities and is defined by FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1.

The security objective O.Authority is sufficiently achieved by the said SFRs.

O.Data_Lock

In the event of an authentication failure with the transport key, readout key or Active Authentication Information Access Key, authentication corresponding to the relevant key is permanently prohibited, and as the result, the security objective of permanently prohibiting readout and write of the internal data of the TOE is sufficiently achieved by the three SFRs:

FIA_AFL.1a, FIA_AFL.1d, and FIA_AFL.1r.

7.3.1.3.Dependencies for Security Functional Requirements

Table 14 shows dependencies and support for the dependencies defined for SFRs.

In the table, the Dependencies column describes dependencies defined for SFRs, and the Support for the Dependencies column describes by what SFRs the defined dependencies are satisfied or rationales indicating the justification for non-satisfied dependencies.

SFR	Dependencies	Support for the Dependencies
FCS_CKM.1p	FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1sp, FCS_COP.1mp, and FCS_CKM.4 support to satisfy the dependencies.
FCS_CKM.1e	FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1e and FCS_CKM.4 support to satisfy the dependencies.
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1, FCS_CKM.1p, FCS_CKM.1e, and FCS_CKM.1p support to satisfy the dependency. FDP_ITC.1 supports keys only on volatile memory.
FCS_COP.1a	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 supports. FCS_CKM.4 supports keys on volatile memory. Since the modification and destruction of keys on non-volatile memory are prohibited, FCS_CKM.4 does not apply to.
FCS_COP.1h	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Since keys do not exist, any requirements do not apply to.
FCS_COP.1n	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 supports. FCS.CKM.4 supports on keys on volatile memory. Since the modification and destruction of keys on non-volatile memory are prohibited, FCS_CKM.4 does not apply to.
FCS_COP.1e	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1e and FCS_CKM.4 support to satisfy the dependencies.
FCS_COP.1hp	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Since keys do not exist, any requirements do not apply to.
FCS_COP.1mp	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1p and FCS_CKM.4 support to satisfy the dependencies.
FCS_COP.1sp	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1p and FCS_CKM.4 support to satisfy the dependencies.
FCS_RND.1	No dependencies	N/A
FDP_ACC.1a	FDP_ACF.1	FDP_ACF.1a supports to satisfy the dependency.
FDP_ACC.1p	FDP_ACF.1	FDP_ACF.1p supports to satisfy the dependency.
FDP_ACF.1a	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1a supports. Objects are created at initial configuration, but not created in the operational environment of the TOE. Therefore, FMT_MSA.3 related to file creation does not apply to.
FDP_ACF.1p	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1p supports. Objects are created at initial configuration, but not created in the operational environment of the TOE. Therefore, FMT_MSA.3 related to file creation does not apply to.
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1a supports. Objects are created at initial configuration, but not created in the operational environment of the TOE. Therefore, FMT_MSA.3 related to file creation does not apply to
FDP_UCT.1p	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1or FDP_IFC.1]	FDP_ITC.1 and FDP_ACC.1p support to satisfy the dependencies
FDP_UIT.1p	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	FDP_ITC.1 and FDP_ACC.1p support to satisfy the dependencies.
FIA_AFL.1a	FIA_UAU.1	FIA_UAU.1 supports to satisfy the dependency.

SFR	Dependencies	Support for the Dependencies
FIA_AFL.1d	FIA_UAU.1	FIA_UAU.1 supports to satisfy the dependency
FIA_AFL.1r	FIA_UAU.1	FIA_UAU.1supports to satisfy the dependency
FIA_UAU.1	FIA_UID.1	FIA_UID.1 supports to satisfy the dependency.
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	FMT_SMR.1 and FMT_SMF.1 support to satisfy the dependencies.
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.1 supports to satisfy the dependency
FPT_PHP.3	No dependencies	N/A
FTP_ITC.1	No dependencies	N/A

Table 14 Dependencies for SFRs

7.3.2. Security Assurance Requirements Rationale

The security functionality of the TOE is featured by difficulty of TOE (IC chip) forgeries realized by adoption of the Active Authentication function and strengthening Secure Messaging with PACE. The security characteristics of the Active Authentication function are achieved by protecting the internal confidential information (private key) in the TOE. And, the security characteristics of the strengthened Secure Messaging functionality are achieved by the use of the session key which possesses sufficient entropy.

Reading out the information kept secret in an IC chip requires advanced means of physical attacks, and it costs a certain amount of facilities and takes some time to decipher the strengthened Secure Messaging.

Assuming attackers possessing a high attack potential who are capable of such attacks, AVA_VAN.5 is required as the security assurance requirement for the vulnerability assessment. In addition, ALC_DVS.2 is adopted as the development security assurance requirement to provide stricter protection of development information used for an attack means.

When using the IC chip as the TOE, state of the art technologies are required for SFRs and design methods to realize such SFRs. However, there are no significant variations in the security functionality of product, and points to be checked for the vulnerability assessment are also well-defined. Consequently, EAL4, which is the top level for commercial product but does not require stringency as high as that for EAL5 whose target application is military use, is adopted as the development and manufacturing assurance requirements except development security and vulnerability assessment.

Note that ALC_DVS.2 does not have dependencies on other components, and the dependencies defined in AVA_VAN.5 are identical to those in AVA_VAN.3 (EAL4). Therefore, being identical to the

EAL4 assurance package in terms of dependencies, dependencies among the security assurance components shown in Table 12 are all satisfied.

8. TOE Summary Specification

8.1.1. TSF.AccessControl

The TSF.AccessControl defines access control over all User and TSF data. There are two security function policy in the TOE:

- PACE SFP (active in operational phase);
- Issuance procedure access control SFP (active in personalisation phase).

In Phase 4 (Operational phase):

This TSF ensures the confidentiality of the user data and protect against unauthorized disclosure of them. It defines the necessary security status of the TOE (successful PACE) to read out user data in operational phase.

Furthermore, it prohibits the modification or reading out transport key file, password key file, and private key file.

In Phase 3 (Personalisation phase)

TSF.AccessControl defines other security status (successful verification of readout key, transport key or Active authentication Information Access Key) in personalisation phase to read out or to write user data (for details please see: Table 7 Internal data of the TOE access control by passport issuing authorities).

FDP_ACC.1a defines the Issuance procedure access control SFP during the personalization in Phase 3.

FDP_ACC.1p defines the PACE SFP during the personalization in Phase 4.

FDP_ACF.1a defines the security attributes for Issuance procedure access control SFP during the personalization in Phase 4.

FDP_ACF.1p defines the security attributes for PACE SFP during the personalization in Phase 3.

FIA_UAU.1 allows to readout of EF.CardAccess and EF.ATR/INFO before user authentication.

FIA_UID.1 allows to readout of EF.CardAccess and EF.ATR/INFO before user identification.

FMT_MTD.1 defines the conditions to modify the transport key.

8.1.2. TSF.Authenticate

The TOE provides several authentication mechanisms to authenticate the terminal and itself as described here:

- PACE ([6])
- GP Authentication ([5])
- Active Authentication ([6])
- Transport Key Verification
- Readout Key Verification

PACE is a password authenticated Diffie-Hellman key agreement protocol that provides secure communication and password-based authentication of the eMRTD chip and the inspection system and PACE ensures that only the authorized terminal is able to read out user data.

GP authentication provides authentication mechanism during the manufacturing. Phase 2 (initialization and pre-personalization of IDentity-J applet).

Active Authentication authenticates the TOE by signing a challenge sent by terminal with Active Authentication private key. Successful Active Authentication ensures that the data read from an genuine ePassport.

Transport key verification ensures that only the authorized passport issuing authorities are able to personalise (write user data) the TOE.

Readout Key verification ensures that only the authorized entity is able to read out the IC chip serial number and later management data.

FIA_UAU.4 ensures the fresh random number for PACE procedure.

FIA_UAU.5 provides the PACE procedure related functions.

FMT_MTD.1 provides the authentication mechanism (Transport Key Verification) to modify the Transport Key.

FMT_SMR.1 provides the authentication mechanism (Transport Key Verification) for the role of authorized personnel of the passport issuing authorities.

FTP_ITC.1 uses the PACE protocol for authentication.

8.1.3. TSF.SecureManagement

The TOE has own secure management function, which compares the authentication status of the TOE and the rules of the TSF.AccessControl (SFP PACE (in operational phase) and Issuance procedure access control SFP (in personalisation phase)) and decides about the executable function, furthermore it checks the life cycle state of the TOE

This TSF ensures that to read out EF.CardAccess and EF.ATR/INFO before user (in this case terminal) identification or authentication.

- FDP_ACF.1a responsible to check the authentication status regarding the objects.
- FDP_ACF.1p responsible to check the authentication status regarding the objects.
- FIA_AFL.1a responsible to detect the unsuccessful authentication attempt and to permanently stop the authentication.
- FIA_AFL.1d responsible to detect the unsuccessful authentication attempt and to permanently stop the authentication.
- FIA_AFL.1r responsible to detect the unsuccessful authentication attempt and to permanently stop the authentication.
- FIA_UAU.1 checks the authentication status of the TOE.
- FIA_UID.1 checks the authentication status of the TOE.
- FDP_ITC.1 responsible to check the authentication status for Issuance procedure access control SFP.
- FMT_MTD.1 responsible to change the authentication status of the TOE after successful authentication of the authorized personnel of the passport issuing authorities.
- FMT_SMF.1 responsible to check the necessary authentication status for the execution of the security management functions.
- FMT_SMR.1 responsible to check the authentication status for the authorized personnel of the passport issuing authorities.

8.1.4. TSF.Crypto

The following Table 15 presents the cryptographic functions of the TOE and the related SFRs,. While the TSF.Platform provides low-level cryptographic operations using the cryptographic library of the Platform, the TSF.Crypto responsible for applet level cryptographic functions, so it provides e.g. the necessary parameters for crypto functions of the Platform. Furthermore, this TSF handles the cryptographic data in applet level, and calls the proper Platform level function.

Function	Algorithm and key length	Related SFRs
Confidentiality protection	AES-CBC-128	FCS_COP.1n

Function	Algorithm and key length	Related SFRs
	AES-CBC-256	FTP_ITC.1
Session key generation	AES-128 with SHA-1 AES-256 with SHA-256	FCS_CKM.1p FCS_COP.1hp FTP_ITC.1
Key generation	EC-256 EC-384	FCS_CKM.1e FTP_ITC.1
Digital signature creation	ECDSA-SHA-256 ECDSA-SHA-384	FCS_COP.1a FCS_COP.1h
Authentication	AES-CMAC-128 AES-CMAC-256	FCS_COP.1mp
Secure messaging	AES-CBC-CMAC-128 AES-CBC-CMAC-256	FCS_COP.1sp FDP_UCT.1p FDP_UIT.1p FTP_ITC.1
Key agreement	ECDH-256 ECDH-384	FCS_COP.1e FTP_ITC.1
Key destruction	-	FCS_CKM.4
Random number generation	-	FCS_RND.1

Table 15 Cryptographic functions of the TOE

8.1.5. TSF.Platform

The TOE has several SFRs, which are rely on the Platform Security Functions and Services as described below:

TSF.Platform provides low-level cryptographic functions such as:

- Key generation (EC) and agreement(ECDH);
- Digital signature creation (ECDH);
- Key destruction (physically overwriting the keys with zeros);
- Encryption and decryption (AES);
- Random number generation (DRG.4 according to BSI AIS20);

For supported and applied algorithm and key length please see Table 15 Cryptographic functions of the TOE.

TSF.Platform provides protection against several type of attack, e.g. Side Channel Attacks (SDA, DPA) or Perturbation attacks.

Following SFRs are collected in the TSF.Platform.

FCS_CKM.1p uses the Platform crypto functions to generate session keys for PACE.

FCS_CKM.1e uses the Platform crypto functions to generate Elliptic Curve Key Pair for PACE

FCS_CKM.4 uses the Platform crypto functions to destruct the PACE session keys, PACE ephemeral key pair.

FCS_COP.1a uses the Platform crypto functions to generate digital signature for Active Authentication.

FCS_COP.1h uses the Platform crypto functions to generate hash value.

FCS_COP.1n uses the Platform crypto function to encrypt nonce.

FCS_COP.1e uses the Platform crypto function for ECDH key agreement.

FCS_COP.1hp uses the Platform crypto functions to generate session keys used for PACE.

FCS_COP.1mp uses the Platform crypto functions for authentication token generation and verification during PACE.

FCS_COP.1sp uses the Platform crypto function to generate keys for message encryption and decryption and MAC generation and verification (PACE).

FCS_RND.1 uses the Platform crypto function to generate fresh random number.

FDP_UCT.1p uses the Platform Secure Channel function to protect data from unauthorised disclosure.

FDP_UIT.1p uses the Platform Secure Channel function to protect data from modification, deletion, insertion and replay errors.

FIA_AFL.1a uses the Platform functionality for Active Authentication Information Access Key verification.

FIA_AFL.1d uses the Platform functionality for Transport Key verification.

FIA_AFL.1r uses the Platform functionality for Readout Key verification.

FIA_UAU.4 uses the Platform functionality to generate fresh secure random.

FMT_MTD.1 uses the Platform functionality to modify the Transport Key.

FMT_SMF.1 uses the Platform functionality to modify the Transport Key.

FPT_PHP.3 uses the Platform functionality to protect the data from hardware or software attacks.

FTP_ITC.1 uses the Platform Secure Channel function to set up and maintain a trusted channel.

9. Glossary

For Glossary please refer to the corresponding chapter of [2].

10. References

[1] Doc 9303 Machine Readable Travel Documents Seventh Edition, ICAO, 2015.

[2] Protection Profile for ePassport IC with SAC (PACE) and Active Authentication version 1.0 - JISEC C0499 - English translation, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan (MOFA), March 8, 2016.

[3] ID&Trust Ltd., ID&Trust IDentity-J-v1.0 Applet for Japanese ePassport - User's Guide v1.0.12.

[4] Appendix E - Specification of Japan e-passport requirement -extraction version -30 November 2017 revision 3.

[5] "Security Target for Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) v2.0 - ST Lite version 3.6," May 2019.

[6] ICAO, Machine Readable Travel Documents, RF protocol and application test standards for eMRTD - part 3 version 2.07 - October 10, 2014.

[7] Protection Profile for ePassport IC with SAC (PACE) and Active Authentication version 1.0 - JISEC C0499 - Official Japanese version, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan (MOFA), March 8, 2016.

[8] Technical Guideline TR-03111: Elliptic Curve Cryptography, version 2.0, BSI, 2012.

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional components version 3.1 revision 5 CCMB-2017-04-002, 2017.