Certification Report

Tatsuo Tomita, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application Date/ID	2018-07-09 (ITC-8679)
Certification Identification	JISEC-C0649
Sponsor	Maxell, Ltd.
TOE Name	ID&Trust IDentity-J with SAC (BAC+PACE) and AA version 1.0 on IFX M7892 G12 SLJ 52G
TOE Version	v1.0.7052
PP Conformance	Strict conformance to Protection Profile for ePassport IC with SAC (BAC+PACE) and Active Authentication version 1.0 (Certification Identification : JISEC-C0500)
Assurance Package	EAL4 augmented with ALC_DVS.2
Developer	ID&Trust Ltd.
Evaluation Facility	TÜV Informationstechnik GmbH, Evaluation Body for IT Security

This is to report that the evaluation result for the above TOE is certified as follows.
2019-08-28

Shinji Sato, Technical Manager
IT Security Evaluation Department
IT Security Center

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following standards prescribed in the "IT Security Evaluation and Certification Scheme Document."

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 5
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 5

Evaluation Result: Pass

" ID&Trust IDentity-J with SAC (BAC+PACE) and AA version 1.0 on IFX M7892 G12 SLJ 52G " has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" by Information-technology Promotion Agency, Japan, and has met

the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary 1
1.1 Product Overview 1
1.1.1 Protection Profile 1
1.1.2 TOE and Security Functionality 1
1.1.2.1 Threats and Security Objectives 6
1.1.2.2 Configuration and Assumptions 7
1.1.3 Disclaimers in Certification 7
1.1.3.1 Disclaimers originating from PP[12] 7
1.2 Conduct of Evaluation 8
1.3 Certification 8
2. Identification 9
3. Security Policy 10
3.1 Security Function Policies 10
3.1.1 Threats and Security Functions 10
3.1.1.1 Threats 10
3.1.1.2 Security Functions against Threats 13
3.1.2 Organisational Security Policies and Security Functions 16
3.1.2.1 Organisational Security Policies 16
3.1.2.2 Security Functions to Organisational Security Policies 19
4. Assumptions and Clarification of Scope 21
4.1 Usage Assumptions 21
4.2 Environmental Assumptions 21
4.3 Clarification of Scope 22
5. Architectural Information 23
5.1 TOE Boundary and Components 23
5.2 IT Environment 24
6. Documentation 25
7. Site security 25
8. Evaluation conducted by Evaluation Facility and Results 26
8.1 Evaluation Facility 26
8.2 Evaluation Approach 26
8.3 Overview of Evaluation Activity 26
8.4 IT Product Testing 27
8.4.1 Developer Testing 27
8.4.2 Evaluator Independent Testing 29
8.4.3 Evaluator Penetration Testing 32
8.5 Evaluated Configuration 34
8.6 Evaluation Results 34

8.7 Evaluator Comments/Recommendations 35
9. Certification 36
9.1 Certification Result 36
9.2 Recommendations 37
10. Annexes 38
11. Security Target 38
12. Glossary 39
13. Bibliography 42

1. Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of " ID&Trust IDentity-J with SAC (BAC+PACE) and AA version 1.0 on IFX M7892 G12 SLJ 52G v1.0.7052" (hereinafter referred to as the "TOE") developed by ID&Trust Ltd., and the evaluation of the TOE was finished on 2019-07-31 by TÜV Informationstechnik GmbH, Evaluation Body for IT Security (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, Maxell Ltd., and provide security information to procurement entities and consumers who are interested in this TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") described in Chapter 11. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

This Certification Report assumes "passport issuing authorities" to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee an individual IT product itself.

Reference should be made to Chapter 12 for the terms used in this Certification Report.

1.1 Product Overview

An overview of the TOE functions and operational conditions is described as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Protection Profile

The TOE claims strict conformance to the Protection Profile [12] (hereinafter referred to as the "PP").

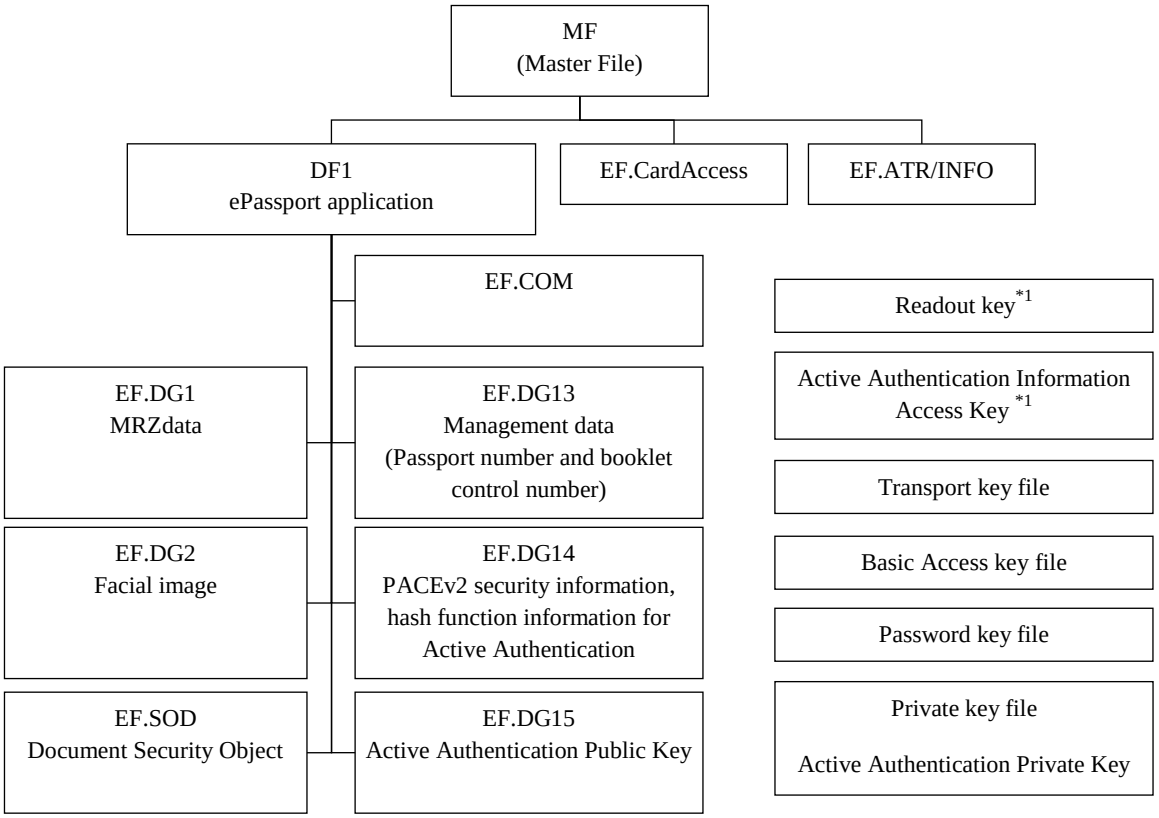
"Protection Profile for ePassport IC with SAC (BAC+PACE) and Active Authentication version 1.0 (Certification Identification: JISEC-C0500 - Official Japanese version, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan (MOFA), March 8, 2016.)".

1.1.2 TOE and Security Functionality

The TOE is an ePassport IC (including necessary software).

The ePassport IC including necessary software is the TOE. This ePassport IC is composed of IC chip hardware with a contactless communication interface, basic software (operating system) and an ePassport application program to be installed in the IC. An external antenna used for contactless communication is connected to the IC chip that will be embedded together with the antenna in a plastic sheet to constitute a portion of a passport booklet.
When a passport holder goes through an immigration process, the immigration official inspects the passport booklet using a passport inspection terminal (hereinafter a "terminal"). The whole Information, printed on the passport booklet in ordinary characters, will be encoded and printed in the machine readable zone (MRZ) of the passport booklet,

then read by the optical character reader of the terminal. Note that the information is digitized[1] and stored in the IC chip, the TOE. The digitized data is read out by the terminal via the contactless communication interface of the TOE. The digitized data also includes a facial image.
Figure 1-1 is a recomposed figure of Figure 2 in Part 10 of ePassport specifications [20] to explain the TOE.



*1 It is not stated as a file in PP [12].

Figure 1-1 File structure of ePassport IC

The PP [12] requires that, prior to reading of the files relating to the ePassport application, the terminal and the TOE to be mutually authenticated and the Secure Messaging to be applied to the communication between them. There are two mechanisms of mutual authentication and Secure Messaging specified in ePassport specifications [20]: Basic Access Control (BAC) and Password Authenticated Connection Establishment v2 (PACE v2). The latter utilises public key cryptography and increases security strength of the session key used in Secure Messaging.

Figure 1-2 shows how BAC and PACE are involved in the procedure for the terminal to access ePassport IC where either BAC or PACE is applied.

[1] In order to prevent the forgery of digital data, digital signature is applied to individual digital data by the passport issuing authorities. The verification process of the digital signature has been standardized by ICAO as Passive Authentication. PKI that provides interoperability for all member States of ICAO is used for the entire process from applying a digital signature through the verification thereof with the terminal, so as to support Passive Authentication. Since Passive Authentication is performed without involvement of the security functions of the TOE, from signing through its verification (including PKI as a background), it is not included in the security requirements for the TOE.

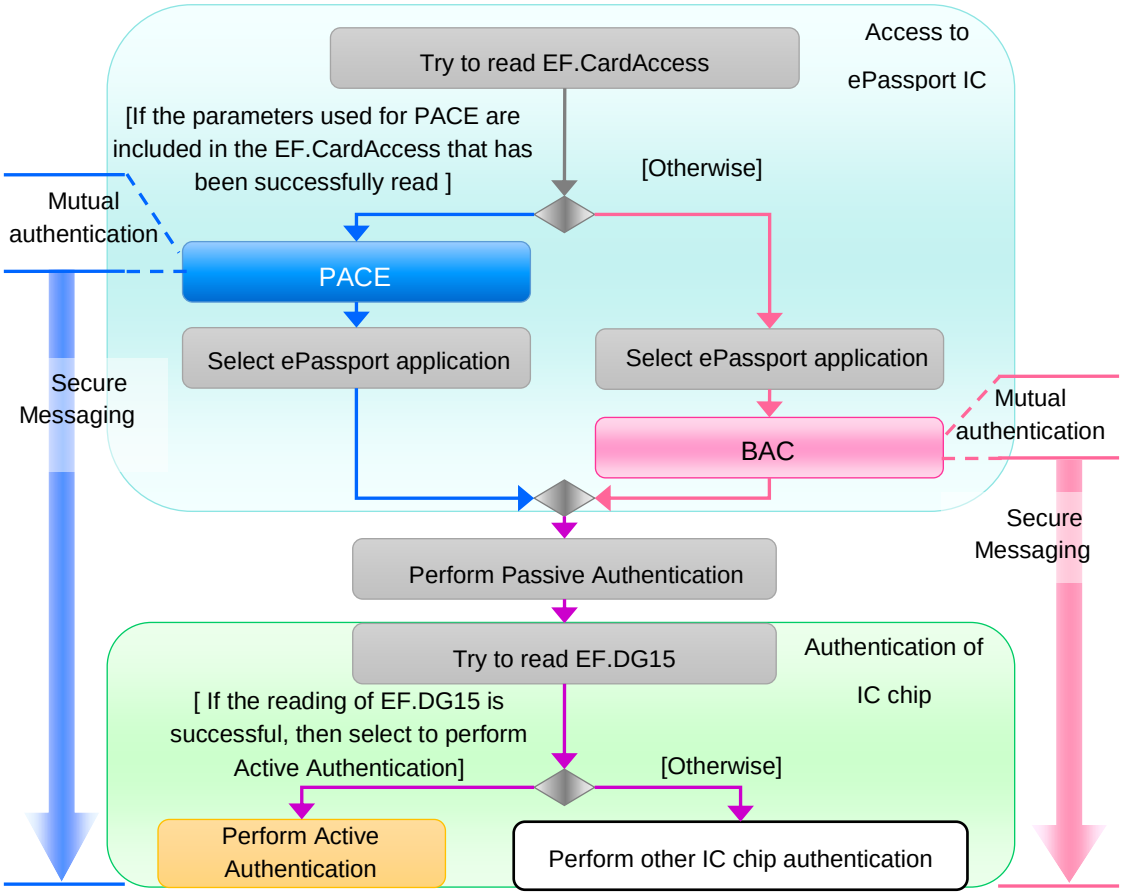


Figure 1-2 Procedure for a terminal to access an ePassport IC

Part 11 of ePassport Specifications [20] did not permit to implement only the PACE without BAC in an IC chip until the end of 2017 to ensure its compatibility.
The TOE is an IC chip which supports PACE and BAC, together with disabling function of BAC.
In order to prevent copying of ePassport IC, the PP [12] requires an Active Authentication function proving the authenticity of the IC chip by a challenge-response protocol using public key cryptography. The previously certified PP [30] also required the Active Authentication but the cipher used for the Active Authentication has been changed from RSA to ECDSA in the PP [12].

The TOE life-cycle is divided into four phases, as shown in Figure 1-3.

Though threats to the operational environment in Phases 1 and 2 have not been assumed, proper development security must be maintained to protect confidentiality and integrity of development data and the components of IC chips. In Phase 3, a security functionality is required so that only an authorised person will be allowed to process the TOE. Phase 4 requires a security functionality that can counter the attacks made by attackers possessing an Enhanced-Basic attack potential.

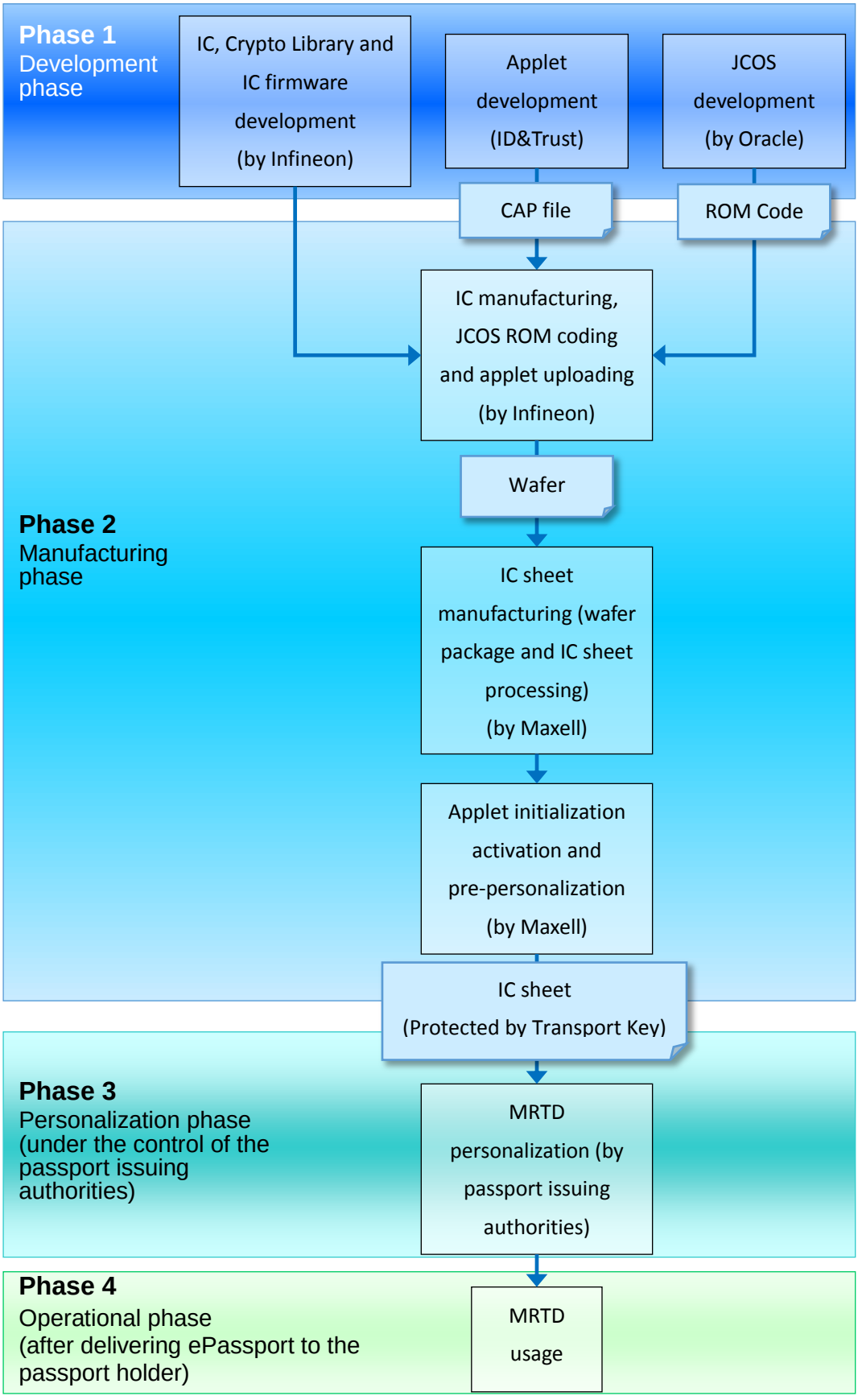


Figure 1-3 Life-cycle of the TOE

The TOE provides the following functions: a function to protect data stored in the TOE from unauthorised reading and writing, BAC and PACE functions specified in Part 11 of ePassport specifications [20], an Active Authentication, a BAC disable function, a protection function in transport, and tamper-resistance to physical attacks. The overviews of these functions are shown below.

(1) Basic Access Control (BAC)

The TOE performs mutual authentication with a terminal and applies Secure Messaging to communication with the terminal having succeeded in mutual authentication to permit the terminal to read access-controlled files in the TOE.

Ciphers used in mutual authentication and Secure Messaging for BAC are symmetric key ciphers (2-key Triple DES and Single DES) and a hash function (SHA-1).

(2) Password Authenticated Connection Establishment (PACE)

The TOE performs mutual authentication with a terminal and applies Secure Messaging to communication with the terminal having succeeded in mutual authentication to permit the terminal to read access-controlled files in the TOE.
Ciphers used in mutual authentication and Secure Messaging for PACE are key establishment scheme using public key cryptography (ECDH[2]), a symmetric key cipher (AES[3]) and a hash function (SHA-1[4] or SHA-256[5])

(3) Active Authentication

In order to prevent copying of ePassport IC, the TOE provides an Active Authentication function to prove the authenticity of the IC chip by a challenge-response using public key cryptography.
Ciphers used in the Active Authentication are a digital signature algorithm (ECDSA[6]) and a hash function (SHA-256 or SHA-384).

(4) BAC disable function

The TOE provides a BAC disable function in order to support the policy by the passport issuing authorities such that ePassport ICs to be issued after a given time in the future shall not accept the BAC protocol.

(5) Write protection function

A function that prevents any writing to the files in the TOE once a passport has been issued.

(6) Protection function in transport

The TOE provides a function allowing access to the given files in the TOE only after the authentication is successfully completed using a transport key, in order to protect IC chips from unauthorised use during transport.

---

2 Although the option of using DH is also described in ePassport specifications [20], ECDH is selected in the PP [12].
3 Although the option of using Triple DES is also mentioned in ePassport specifications [20], AES is selected in the PP [12]. In the PP [12], it is required to support both 128-bit AES key and 256-bit AES key.
4 SHA-1 is used when using 128-bit AES key.
5 SHA-256 is used when using 256-bit AES key.
6 Although the option of using RSA is also described in the ePassport specifications [20], ECDSA is selected in the PP [12]. Taking it into account, the signature shall be generated using 256-bit or 384-bit private key. SHA-256 is used in case of 256-bit private key, and SHA-384 is used for 384-bit.

(7) Tamper-resistance to physical attacks

The TOE security functionality (TSF) also counters physical attacks against its hardware and software that constitutes the TSF. Assumed attacks for the TOE are the same as for IC cards in general. There exists various attacks using physical means, such as physical manipulation of the IC chip, disclosure and/or modification of information by probing, disclosure of the cryptographic key by monitoring and/or analysing electromagnetic emanation of the TOE.

For these security functions, the validity of the design policy and the accuracy of the implementation were evaluated within the scope of the assurance package requested by the Conformance PP [12].

The following section describes the threats and assumptions that the TOE assumes.

1.1.2.1 Threats and Security Objectives

This TOE counters the various threats by using the security functions as follows.

A conventional passport as an ID including all necessary information printed on a paper booklet could have been forged and used by an unauthorised person. In order to solve this problem, an ePassport IC has a digital signature issued by the official passport issuing authorities applied to digital data stored in the IC chip, and adopts Passive Authentication so as to confirm authenticity of the data read out from the IC chip by using PKI system, in which interoperability between the passport issuing end and receiving end is guaranteed.

Passive Authentication is, however, not enough to counter a forgery made by copying personal information with the official signature and then storing it in another IC chip. Therefore, the PP [12] adopts a challenge-response protocol using public key cryptography called Active Authentication specified in the ePassport specifications [20] so that it can restrict the reading of a private key used for the Active Authentication (hereinafter “Active Authentication Private Key”) from the IC chip to counter the forgery.

The ePassport specifications [20] have adopted the file system specified in ISO/IEC 7816-4. Assuming that the Active Authentication Private Key is also stored in this file system, it might be read out using commands specified in ISO/IEC 7816-4. The PP [12] requires the TOE to reject read access to the key in order to counter such threats.

Data available to be read out from an ePassport IC contains a facial image and information for Passive Authentication. It is assumed that there will be some attempts to disclose and/or modify communication data between the ePassport IC and the terminal at the immigration inspection counter. This threat can be countered by applying mutual authentication as well as Secure Messaging between the TOE and the terminal.

Because of the nature of its physical embodiment, an IC chip mounted on an IC card may leak internally processed information through power consumption and electromagnetic emanation. Disclosure of the data in the IC chip by physical probing, physical manipulation

of the IC chip circuit, and malfunction due to environmental stress also need to be considered. Thus the TOE is required to provide the functionality to protect TSF against such physical attacks. Note that the resistance to the above mentioned threats are addressed by the platform explained in 5.1.

1.1.2.2 Configuration and Assumptions

The evaluated product is assumed to be operated under the following configuration and assumptions.

The TOE is interfiled in the ePassport booklet and information necessary for ePassport is written therein. The ePassport booklet is carried along with the holder thereof and used to certify the identity of the holder in various situations, including immigration procedures.

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

In order for the passport inspection authorities of the receiving state or organisation to verify 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 organisations of the passport shall be maintained by passport issuing authorities.

1.1.3 Disclaimers in Certification

1.1.3.1 Disclaimers originating from PP[12]

The PP [12] declares that the BAC and PACE are mutual authentication and secure messaging functions. The BAC and PACE, as specified in the ePassport specifications [20], are mechanisms to counter only an attack made by an attacker who does not know MRZ data, in which the attacker interrupts wireless communication to try to eavesdrop and tamper information read out from an ePassport IC to a terminal.

According to the ePassport specifications [20], MRZ data is the information necessary to break into the BAC[7] and PACE, and therefore it is possible to read out information for Passive Authentication eventually by masquerading as a legitimate terminal if the attacker can obtain the MRZ data. Thus, the authentication cannot counter the threat from the attacker who knows MRZ data trying to break in the BAC or PACE to read out data from the ePassport IC. However, even if the attacker can obtain the MRZ data, attackers cannot logically read out an Active Authentication Private Key as long as the TOE conforms to the PP [12].

Although the PP [12] requires the TOE to have Active Authentication support function for protecting the ePassport IC from being copied, the TOE function by itself cannot prevent abuse of the forged passport. In order for the Active Authentication mechanism to properly function as a system, it must have confidentiality of the Active Authentication Private Key

[7] It is documented in the page of cryptographic protocol verification of the BAC (http://crypto-protocol.nict.go.jp/AKE_zoo/11770-2-6-epass/11770-2-6-epass_Main.html) conducted by CPVP operated by National Institute of Information and Communications Technology (NICT).

as well as integrity and authenticity of the Active Authentication public key. In accordance with assumption A.Administrative_Env discussed later, users authorised by the passport issuing authorities need to securely perform the following:

- Generate an Active Authentication key pair
- Apply the digital signature to the Active Authentication public key
- Store the Active Authentication key pair on the ePassport IC

In addition, users authorised by the passport issuing authorities need to securely manage the key pair(s) to be used to generate a digital signature for data stored on the ePassport IC and maintain the PKI environment appropriately, in accordance with assumption A.PKI described later.

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed on 2019-07, based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme Document" [1], "Requirements for IT Security Certification" [2], and "Requirements for Approval of IT Security Evaluation Facility" [3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [15] and the Observation Reports prepared by the Evaluation Facility as well as evaluation documentation, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The certification oversight reviews were also prepared for those concerns found in the certification process. Those concerns pointed out by the Certification Body were fully resolved, and the Certification Body confirmed that the TOE evaluation had been appropriately conducted in accordance with the CC ([4][5][6]) and the CEM ([7]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

TOE Name:	ID&Trust IDentity-J with SAC (BAC+PACE) and AA version 1.0 on IFX M7892 G12 SLJ 52G
TOE Version:	v1.0.7052
Developer:	ID&Trust Ltd.

Users can verify that a product is the evaluated and certified TOE by the described method in the User's Guide [22].
In Personalization Phase and Operational Phase, IDentity-J-v1.0 applet is identifiable with GET DATA. It can be checked whether the product is the TOE or not, by comparing the result of GET DATA command with the following information as per 12.1 of User's Guide [22].

The return value of GET DATA : IDentity-J-v1.0.7052

3. Security Policy

This chapter describes security function policies that the TOE adopts to counter threats, and organisational security policies.
The TOE is an ePassport IC on which necessary information as a Passport is written, such as name, date of birth, facial image data.

The TOE provides the following security functions which fulfil the requirements in PP [12]:

- Basic Access Control (BAC) function (mutual authentication and secure messaging)
- Password Authenticated Connection Establishment (PACE) function (mutual authentication and secure messaging)
- Active Authentication support function (prevention of forgery of an ePassport IC chip)
- BAC disable function (in response to the policy by the Passport Issuing Authorities for TOEs not to accept the BAC protocol after a certain point of time)
- Write protection function (protection on writing data after an issuance of a passport)
- Protection function in transport (protection against attacks during transport before its issuance)
- Tamper resistance (protection against leakage of confidential information caused by physical attacks)

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Section 3.1.1 and to satisfy the organisational security policies shown in Section 3.1.2.

3.1.1 Threats and Security Functions

3.1.1.1 Threats

The TOE assumes the threats shown in Table 3-1 and provides the security functions to counter them.

Table 3-1 Assumed Threats

Identifier	Threat
T.Copy[8]	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.

[8] The threat T.Copy points out the limitation of the ePassport IC which only supports the Passive Authentication.

Identifier	Threat
	[Note] 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[9]	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. [Note] 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[10]	In the operational environment after issuing a TOE embedded passport booklet, an attacker who does not know about MRZ data may interfere with the

[9] The threat T.Logical_Attack indicates a possibility that the Active Authentication Private Key may be readout using commands defined in the ISO/IEC 7816-4 considering that TOEs adopt the file system defined in the ISO/IEC 7816-4.

10 The threat T.Communcation_Attack indicates the concerns of attacker's disclosure and tampering of readable data, including facial images. The threats T.Logical_Attack and T.Communication_Attack are stated independently, as the data under attack is distinct.

Identifier	Threat
	communication between the TOE and a terminal to disclose and/or alter communication data that should be concealed. [Note] 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 its 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[11]	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 nondestructive 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. [Note] 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 nondestructive attacks includes measurements on leaked electromagnetic wave associated with the TOE operation and induction of malfunctions of security functions by applying environmental stress (e.g.

11 Using a physical means for TOE, the threat T.Physical_Attack is contrasted with the threat T.Logical_Attack, whose available means are limited to the logical means. However, the threat T.Physical_Attack includes attacks combining physical means with logical means (data output via the contactless communication interface), such as the Differential Fault Analysis (DFA).

Identifier	Threat
	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.

3.1.1.2 Security Functions against Threats

The TOE counters the threats shown in Table 3-1 by the following security function policies.

(1) Countering the threat T.Copy

The Passive Authentication is an inspection system using PKI system to verify personal information stored in an ePassport IC with a digital signature, which then will be read out through a terminal. The threat T.Copy is assumed to break through an inspection with Passive Authentication, in which an attacker presents a forged ePassport IC having an IC with duplicated personal information, including a digital signature, taken from a different IC.
The ePassport specifications [20] define the following procedure using the Active Authentication to counter this threat.

(a) A terminal sends nonce (8-byte) to an ePassport IC.

(b) An ePassport IC generates a signature to the received nonce with the Active Authentication Private Key stored in the ePassport IC to send it to the terminal.

(c) The terminal tries to verify a signature using the Active Authentication Public Key read out separately from the ePassport IC and if the signature is successfully verified, the ePassport IC will be confirmed authentic. Note that a digital signature is applied to Active Authentication Public Key, which allows terminals to verify integrity and authenticity of the Active Authentication Public Key using the PKI system.

As for the digital signature algorithms of Active Authentication, the PP [12] defines ECDSA (using a 256-bit or 384-bit private key), which was defined in [21] referred by the ePassport specifications [20].
As for the confidentiality of a related Active Authentication Private Key and integrity of an Active Authentication Public Key and an Active Authentication Private Key, the PP [12]

requires a mechanism to issue an ePassport to a passport applicant while preventing the following two actions according to the organisational security policies P.Data_Lock described in 3.1.2.1.

- Reading and/or writing the Active Authentication Private Key
- Writing the Active Authentication Public Key

(2) Countering the threat T.Logical_Attack

The threat T.Logical_Attack assumes a possibility that via a contactless communication interface the Active Authentication Private Key is logically read in an operational environment where a passport booklet with an embedded TOE has been issued.

The TOE counters the above threat by preventing logical reading of the Active Authentication Private Key in the operational environment after the issuance of the passport booklet.

(3) Countering the threat T.Communication_Attack

The threat T.Communication_Attack assumes attacks to disclose and/or tamper readable data including facial images.
This threat can be countered by applying mutual authentication and Secure Messaging between the TOE and terminals.
The ePassport specifications [20] define the following two applicable mechanisms for the mutual authentication and Secure Messaging
a) BAC
b) PACE
The PP [12] requires TOEs to support both BAC and PACE mechanisms. It depends on a terminal which mechanism is actually used in the mutual authentication and Secure Messaging between the TOE and the terminal, as shown in Figure 1-2.

a) Table 3-2 shows cryptographic algorithms used for BAC defined in the ePassport specifications [20], which will be combined with ISO/IEC 11770-2 Key Establishment Mechanism 6.

Table 3-2 Cryptographic algorithms used for BAC

Cryptographic algorithm	Cryptographic operation	Cryptographic key size (bit)	Usage
SHA-1	Derivation of a session key for BAC	_*1	Secure Messaging
CBC mode Triple DES	Message encryption and decryption	112	Mutual authentication
	Generation and verification of authentication codes(final block of message) *2	112	
	Message encryption and decryption	112	Secure Messaging
	Generation and verification of authentication codes(final block of message) *2	112	
CBC mode Single DES	Generation and verification of authentication codes(excluding the final block of message) *2	56	Mutual authentication
	Generation and verification of authentication codes(excluding the final block of message) *2	56	Secure Messaging

*1 Assuming the function as a key derivation function, it takes the 128-bit data established by the mutual authentication concatenated with 32 bits of the counter.

*2 It describes ISO/IEC 9797-1 MAC Algorithm 3.

b) Table 3-3 shows cryptographic algorithms used for PACE.

Table 3-3 Cryptographic algorithms used for PACE

Cryptographic algorithm	Cryptographic operation	Cryptographic key size (bit)	Usage
SHA-1*1	Derivation of a session key for PACE	_*3	Mutual authentication and Secure Messaging
SHA-256*2	Derivation of a session key for PACE	_*3	Mutual authentication and Secure Messaging
ECDH	Key agreement	256 or 384	Mutual authentication and Secure Messaging
CMAC mode AES	Generation and verification of authentication tokens	128 or 256	Mutual authentication
	Generation and verification of authentication codes	128 or 256	Secure Messaging
CBC mode AES	Nonce*4 encryption	128 or 256	Mutual authentication
	Message encryption and decryption	128 or 256	Secure Messaging

*1 Used to derive a 128-bit AES session key.

*2 Used to derive a 256-bit AES session key.

*3 A hash function does not take a cryptographic key. However, assuming it as a key derivation function, it takes a shared secret established by ECDH concatenated with 32 bits of the counter.

*4 This nonce, generated by the TOE itself with a random number generator, differs from the nonce seen in Active Authentication.

(4) Countering the threat T. Physical_Attack

A TOE conforming to the PP [12] is exposed to physical tampering (observation, analysis, and modification) due to its nature of an IC as a physical embodiment. Behaviour of a TOE is also affected by operating conditions such as voltage, frequency and temperature.
The TOE conforming to the PP [12] provides protection function for TSF in order to resist the attacks described in the mandatory technical document regarding IC cards and similar devices [9].
Examples of these attacks include:

- Attacks that attempt to extract internal signals of a TOE.
- Attacks that attempt to manipulate internal signals of a TOE.
- Fault Injection Attacks (including DFA)
- Side channel attacks (including DEMA)
- Exploitation of the test features of IC chips.
- Reactivation of disabled access control mechanisms
- Attacks that predict random numbers generated by a random number generator and/or decrease the entropy of output random numbers.

3.1.2 Organisational Security Policies and Security Functions

3.1.2.1 Organisational Security Policies

Organisational security policies required in use of the TOE are shown in Table 3-4.

Table 3-4 Organisational Security Policies

Identifier	Organisational Security Policy
P.BAC	In the operational environment after issuing a TOE embedded passport booklet, the TOE shall allow a terminal to read certain information from the TOE in accordance with BAC defined by Part 11 of [20]. 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 [15] is not defined. Note that this organisational security policy will not be applied after disabling BAC with P.Disable_BAC.
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 [20]. 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 [15] is not defined.
P.Authority[12]	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 3-5.
P.Data_Lock[13]	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

[12] Corresponding to protection function in transport
[13] Corresponding to write protection function

Identifier	Organisational Security Policy
	successful authentication thereof. Table 3-5 shows the relationship between the key used for authentication and its corresponding file in the TOE.
P.Prohibit[14]	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 applicant. 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.
P.Disable_BAC[15]	In accordance with the passport issuing authorities' policies against compromise of BAC, TOEs issued after a certain time shall not accept the BAC procedure. As a means to achieve it, a TOE provides the procedure of disabling the BAC function, and a user authorised by the passport issuing authorities disables the BAC function by implementing the procedure. [Note] This organisational security policy shall be applied only if the passport issuing authorities demand to terminate issuing IC chip equipped with the BAC function.

Table 3-5 Access control of internal data of the TOE by passport issuing authorities

Authentication status	File subject to access control	Permitted operation	Reference: Data subject to operation
Successful verification with readout key*1	EF.DG13	Read	IC chip serial number (entered by manufacturer)
Successful verification with transport key*1	Transport key file	Write	Transport key data (update of the previous data)
	Basic access key file		Basic access key (Encryption key) Basic access key (Message Authentication Code key)
	Password key file		Password key
	EF.DG1	Read or Write	MRZ data
	EF.DG2		Facial image

[14] Corresponding to write protection function
[15] Corresponding to the BAC disable function

Authentication status	File subject to access control	Permitted operation	Reference: Data subject to operation
	EF.DG13[*2]		Management data (Passport number and Booklet management number)
	EF.DG14		PACEv2 security information Hash function information for Active Authentication
	EF.COM[*3]		Common data
	EF.SOD		Security data related to Passive Authentication defined in Part 10 of ePassport specifications [20]
	EF.CardAccess	Write	PACEv2 security information
	EF.DG15	Read	Active Authentication Public key
Successful verification with Active Authentication Information Access Key[*1]	EF.DG15	Write	Active Authentication Public Key
	Private key file		Active Authentication Private Key

[*1] A readout key, a transport key, and an Active Authentication Information Access Key are configured by the manufacturer. A transport key can be modified (updated) by a user. User accesses not stated in this table or note is denied: access to files subject to access control specified in this table, access to files storing a readout key which may change authentication status or files storing an Active Authentication Information Access Key. (Access to information in the TOE through a terminal after the issuance of a TOE embedded passport booklet is controlled by either BAC or PACE, which will be separately specified.)

[*2] An IC chip serial number has already been recorded in EF.DG13 by the manufacturer and its management data will be appended to the file by the passport issuing authorities.

[*3] EF.COM file may not be created depending on the passport issuing authorities' instructions.

Table 3-6 shows the relationship between organisational security policies shown in Table 3-4 and applicable phases.

Table 3-6 Organisational security policies and applicable phases

Organisational security policies	Phase			
	Phase 1	Phase 2	Phase 3	Phase 4
P.BAC				X*1
P.PACE				X
P.Authority			X	
P.Data_Lock			X	
P.Prohibit			X	X
P.Disable_BAC			X	

*1 P.BAC will not be applied to Phase 4 if BAC function is disabled in Phase 3.

[Note] "X" indicates that organisational security policies shall be applied.

3.1.2.2 Security Functions to Organisational Security Policies

The TOE provides the security functions to satisfy the organisational security policies shown in Table 3-4.

(1) Supporting the organisational security policy P.BAC (Basic Access Control (BAC))

In the operational environment after an issuance of a TOE embedded passport booklet, the organisational security policy defines that a terminal reads the given information from the TOE in accordance with the BAC protocol defined in the ePassport specifications [20].

The TOE provides the function supporting the BAC protocol defined by Part 11 of ePassport specifications [20], which enables that the given information be securely read out from the TOE at the intended level of the BAC protocol.

(2) Supporting the organisational security policy P.PACE (Password Authenticated Connection Establishment (PACE))

In the operational environment after an issuance of a TOE embedded passport booklet, the organisational security policy defines that a terminal reads the given information from the TOE in accordance with the PACE protocol defined in the ePassport specifications [20].

The TOE provides the function supporting the PACE protocol defined by Part 11 of ePassport specifications [20], which enables that the given information be securely read out from TOE at the intended level of the PACE protocol.

(3) Supporting the organisational security policy P.Authority (protection function in transport)

The organisational security policy defines that access to files in the TOE under the control of the passport issuing authorities to be controlled in accordance with Table 3-5.

In order to access files in the TOE, the TOE requires a user authentication with a transport key, a readout key, or an Active Authentication Information Access Key, and only when the authentication is successful, the access to files in the TOE shall be allowed based on the authentication status for each key.

(4) Supporting the organisational security policy P.Data_Lock (write protection function)

The organisational security policy defines that if the TOE detects a failure in

authentication with a transport key, a readout key or an Active Authentication Information Access Key, the TOE permanently disables authentication related to the said key and thereby prevents reading or writing files that require successful authentication shown in Table 3-5.

When detecting a failure in authentication with a readout key, a transport key, or an Active Authentication Information Access Key, the TOE disables authentication mechanism that uses the said key, which prevents access to the files with these keys.

(5) Supporting the organisational security policy P.Prohibit (write protection function)
The organisational security policy defines that any writing to files in the TOE and/or reading those files after successful authentication of a readout key must be prevented once a passport has been issued to a passport applicant.

By causing authentication failures with a transport key, a readout key, or an Active Authentication Information Access Key before the issuance of a passport to a passport applicant, writing to files in the TOE and reading those files after authentication of a readout key is prevented by using the function provided by the TOE described above (4).

(6) Supporting the organisational security policy P.Disable_BAC (BAC disable function)
The organisational security policy defines that the BAC function of the TOE shall be disabled by following two means in order to realise the policy of the passport issuing authorities that TOEs issued after a given time shall not support the BAC.

a). The TOE provides a means to disable the BAC function of itself.
b). Users authorised by the passport issuing authorities conduct a procedure to disable the BAC function.

Item a) is realised by the TOE providing the function to disable the BAC.

Item b) is realised by users authorised by the passport issuing authorities conducting the procedure to disable the BAC of the TOE following instructions of the passport issuing authorities.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate the TOE as useful information for the assumed readers to determine the use of the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE.

The effective performances of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions in Use of the TOE

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

4.2 Environmental Assumptions

The TOE form is an IC chip and has a contactless interface. When using this TOE, the passport inspection terminal devices that supports Type-B transmission protocol defined in ISO / IEC 14443 with an optical character reader are used.

4.3 Clarification of Scope

As described in 1.1.3, it cannot be countered against the threat that an attacker who knows the MRZ data breaks through the key sharing access control and reads out the data of the passport booklet IC.

Although the PP [12] requires the TOE to have Active Authentication support function for protecting the ePassport IC from being copied, the TOE function by itself cannot prevent abuse of the forged passport. In order for the Active Authentication mechanism to properly function as a system, it must have confidentiality of the Active Authentication Private Key as well as integrity and authenticity of the Active Authentication public key. In accordance with assumption A.Administrative_Env discussed later, users authorised by the passport issuing authorities need to securely perform the following:

- Generate an Active Authentication key pair
- Apply the digital signature to the Active Authentication public key
- Store the Active Authentication key pair on the ePassport IC

In addition, users authorised by the passport issuing authorities need to securely manage the key pair(s) to be used to generate a digital signature for data stored on the ePassport IC and maintain the PKI environment appropriately, in accordance with assumption A.PKI described later.

5. Architectural Information

This chapter explains the scope and the main components (subsystems) of the TOE.

5.1 TOE Boundary and Components

Figure 5-1 shows the composition of the TOE.

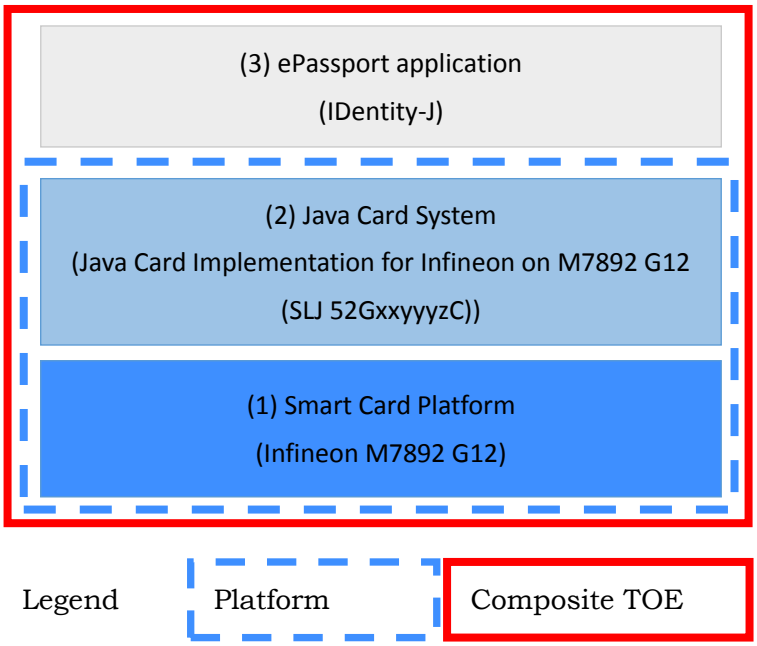


Figure 5-1 TOE boundary

Components of the TOE are explained below.

Table 5-1 Components of TOE and their overview

	Component	Overview
(1)	Smart Card Platform	IC chip and cryptographic library manufactured by Infineon Technology. This uses the M7892 G12 identified by the platform ST [17].
(2)	Java Card System	Provides Java Card APIs, Virtual Machine, and Runtime Environment. (1) and (2) are integrated and certified as Java Card Platform (see ST[16]). It provides cryptographic algorithms and secure messaging function used for the passport booklet IC, making use of (1).
(3)	ePassport application (IDentity-J)	An applet that provides ePassport functionality that runs on the Java Card System.

5.2 IT Environment

The TOE is an IC chip embedded software required for the passport booklet IC and hardware platform on which the software operates.
The TOE operates with wireless signal power sent from the terminal.

6. Documentation

The identification of documents attached to the TOE is listed below.

TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

User's Guide [22]
ID&Trust Ltd., ID&Trust IDentity-J-v1.0 Applet for Japanese ePassport - User's Guide v1.0.12.

7. Site security

In the evaluation of this TOE, Minimum Site Security Requirements [11] were applied in the evaluation of ALC_DVS.2. Concerns found in evaluation activities were all issued as the Observation Reports, and those were reported to the developer and the sponsor. Those concerns were reviewed by the developer and the sponsor, and all the concerns were solved eventually.

8. Evaluation conducted by Evaluation Facility and Results

8.1 Evaluation Facility

TÜV Informationstechnik GmbH, Evaluation Body for IT Security that conducted the evaluation as the Evaluation Facility is approved under JISEC and is accredited by NITE (National Institute of Technology and Evaluation), the Accreditation Body, which joins Mutual Recognition Arrangement of ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

8.2 Evaluation Approach

The evaluation was conducted by using the evaluation methods prescribed in the CEM and CC supporting documents ([8][9][10][11]) in accordance with the assurance components in the CC Part 3.

Details for evaluation activities were reported in the Evaluation Technical Report.

The Evaluation Technical Report explains the summary of the TOE as well as the content of the evaluation and the verdict of each work unit in the CEM and CC supporting documents ([8][9][10][11]).

8.3 Overview of Evaluation Activity

The history of the evaluation conducted is described in the Evaluation Technical Report as follows.

The evaluation has started on 2018-07 and concluded upon completion of the Evaluation Technical Report dated 2019-07.

The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted.

Additionally, the evaluator directly visited the development and manufacturing sites on 2018-10 and on 2018-11 and examined procedural status conducted in relation to each work unit for configuration management, delivery and development security by investigating records and interviewing staff.

Furthermore, the evaluator conducted the sampling check of the developer testing and the evaluator testing by using the developer testing environment at the developer site on 2018-10.

Concerns found in evaluation activities for each work unit were all issued as the Observation Reports, and those were reported to the developer.

Those concerns were reviewed by the developer, and all the concerns were solved eventually.

For evaluation, composite evaluation based on CC supporting documents ([8][9][10]) is

applied, and the certification report of the referenced platform is BSI-DSZ-CC-0869-V2-2019 [18][16].

8.4 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had performed.

As a result of the evidence shown in the process of the evaluation and those confirmed validity, the evaluator performed the reproducibility testing, additional testing and penetration testing based on vulnerability assessments judged to be necessary.

8.4.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer performed and the documentation of actual testing results.

The content of the developer testing evaluated by the evaluator is explained as follows.

1) Summary of the Developer Testing

A summary of the developer testing is as follows.

a. Developer Testing Outline

An outline of the developer testing is as follows.

Developer testing is broadly divided into (i) functional testing and (ii) issuance testing. The functional test is a common test for machine-readable passports according to the test specification [31] defined by ICAO. The issuance test is a test related to the issuance procedure of the passport booklet IC which is not covered by ICAO.

<Developer test method>

When the TOE test was performed, the behaviour of the TOE was confirmed by transmitting APDU commands and receiving their responses via the contactless IF of the TOE using an IC card reader.

<Developer test tool>

The tools used for functional testing by ID&Trust Ltd. are shown in Table 8-1 and the tools used for issuance test by Maxell Ltd. are shown in Table 8-2.

Table 8-1 Developer test tools (functional testing)

[16] Regarding the part beyond the platform's mutual recognition scope of CCRA, the platform evaluation was conducted by the Evaluation Facility that is under the umbrella of JISEC, and based on the fact that the same Evaluation Facility is in charge of composite evaluation, it has been confirmed that it can be reused in composite evaluation.

Tool name	Overview, purpose of use
Gemalto Prox-DU Contactless_12400279	The IC card reader equipped with the contactless IF. It transmits command APDU to TOE and receives response APDU.
GlobalTester TestManager Release 2.9.0v20160509	Test tool for passport booklet IC used by ID & Trust Ltd. The test tool make enable execution test based on test specifications of passport booklet ICs issued by German BSI and ICAO.
Windows PC	PC with which the above IC card reader cooperates and on which the above software operates

Table 8-2 Developer test tools (issuance test)

Tool name	Overview, purpose of use
DUALi DE-620	The IC card reader equipped with the contactless IF. It transmits command APDU to TOE and receives response APDU.
ePassport Committee member of JBMIA test tool version 1.0.0.1	Test tool used by Maxell, Ltd.
IDnT perso tool 3.7.1476	The tool used for TOE initialization and personal information setting.
Windows PC	PC with which the above IC card reader cooperates and on which the above software operates

<Content of the performed developer testing>

As for functional tests, test scenarios and expected values are specified in the test specifications provided by ICAO [31], and the expected values and actual values were compared according to the scenarios.

Regarding the issuance test, the test procedure and the expected value were specified after the test preconditions were specified, and the expected value and the actual value were compared in accordance with the test procedure.

b. Scope of the Performed Developer Testing

The developer testing was performed on 302 items by the developer.

By the coverage analysis, it was verified that all security functions and external interfaces described in the functional specification had been tested.

Under the condition that the platform has been evaluated and certified, by the depth analysis, it was verified that all the subsystems and subsystem interfaces described in the TOE design had been sufficiently tested.

c. Result

The evaluator confirmed the approach of the performed developer testing and the legitimacy of tested items, and confirmed consistencies between the testing approach described in the testing plan and the actual testing approach.

The evaluator confirmed consistencies between the testing results expected by the developer and the actual testing results performed by the developer.

8.4.2 Evaluator Independent Testing

The evaluator performed the sample testing to reconfirm the execution of security functions by the test items extracted from the developer testing. In addition, the evaluator performed the evaluator independent testing (hereinafter referred to as the "independent testing") to gain further assurance that security functions are certainly implemented, based on the evidence shown in the process of the evaluation.

The independent testing performed by the evaluator is explained as follows.

1) Configurations in the Independent Testing

In this TOE, two variations of Table 8-3 exist depending on the information embedded in EF.CardAccess, EF.DG14 and EF.DG15, and in the independent testing performed by the evaluator, tests were performed on both.

Table 8-3 Variations of TOE

Identifier	PACE OID[17]	Elliptic curve Domain Parameters[18]	Hash functions used in ECDSA for active authentication[19]
Config_A	id_PACE_ECDH_GM_AES_CBC_CMAC-128[20]	NIST P-256	SHA-256
Config_B	id_PACE_ECDH_GM_AES_CBC_CMAC-256[21]	NIST P-384	SHA-384

<Independent testing tools>

[17] Information is recorded in EF.CardAccess and EF.DG14.
[18] Applicable to ECDH in PACE and ECDSA for active authentication.
Information is recorded in EF.CardAccess, EF. DG14 and EF.DG15. .
[19] Information is recorded in DG14.
[20] OID is defined in TR-03111[21].
[21] OID is explained in TR-03111[21].

The tools used in the independent test are shown in Table 8-4.

Table 8-4 Tools used in the independent tests

Tool Name	Outline and purpose of use
SDI011	Contactless IC card reader
WOLF v1.84 / Python v2.7	Tool for APDU scripting.
Windows PC	Windows PC with which the above IC card reader cooperates and on which the above software operates

2) Summary of the Independent Testing

A summary of the independent testing is as follows.

a. Viewpoints of the Independent Testing

Viewpoints of the independent testing that the evaluator designed from the developer testing and the provided evaluation documentation are shown below.

The evaluator devised independent tests based on the idea of augmenting the developer tests on the interface and supplementing the developer's test policy.

In addition to augmenting developer testing, the following aspects are also considered: the complexity and the susceptibility to vulnerabilities of interfaces and related functionality.

Furthermore, it was specifically chosen to cover the TSFIs related to the followings:

-Identification and Authentication
-Protection against interference, logical tampering and bypass
-Secure messaging
-Preparation procedure according to the guidance

The selection process is based on evaluator experience, so that all TOE security functionality is included in within the subset. All cryptographic functionality is provided by the platform and was sufficiently tested during the platform evaluation.

<Viewpoints of Independent tests>

1 Negative tests
2 Confirming that BAC disabling function does not work for TOEs which issuing procedures applied to.
3 Correct behaviour of the write protection function.

b. Independent Testing Outline

The evaluator devised the additional testing from the developer testing and the provided

evaluation documentation from the above viewpoints.

An outline of the independent testing that the evaluator performed is as follows.

<Independent Testing Approach>

For this TOE, the APDU interface is essential and focused and tested.

<Content of the Performed Independent Testing>

The independent testing was performed on 20 items by the evaluator.

Table 8-5 shows viewpoints of the independent testing and the content of the testing corresponding to them.

Table 8-5 Content of the Performed Independent Testing

Viewpoint	Overview
Negative tests	- Before reading files, confirm that files that require PACE authentication cannot be selected or read without completing PACE authentication. - Make sure that not writeable files cannot be written even after PACE authentication. - For files that are not described in the specifications provided by the supplier, confirm that file selection cannot be performed, assuming an ISO / IEC 7816-4 file system. - Confirm that command replay attacks are detected by secure messaging after authentication by PACE. - Confirm that the Active Authentication cannot be performed without successful authenticated through BAC procedure. - Perform the negative tests exercising BAC authentication without generating challenge data of correct length (8-byte) specified in ePassport specifications [20].
Confirmation that BAC disabling function is not processed	Send the TERMINATE BAC command to the TOE which issuing procedures have been applied to and confirm that the command is not processed.
Correct behaviour of the write protection function	Check the VERIFY command is properly blocked for the TOE after the passport booklet is issued.

c. Result

All the independent testing performed by the evaluator was correctly completed, and the

evaluator confirmed the behaviour of the TOE.

The evaluator confirmed consistencies between the expected behaviour and all the testing results.

8.4.3 Evaluator Penetration Testing

The evaluator devised and performed the necessary evaluator penetration testing (hereinafter referred to as the "penetration testing") on the potentially exploitable vulnerabilities of concern under the assumed environment of use and attack level from the evidence shown in the process of the evaluation.

The penetration testing performed by the evaluator is explained as follows.

1) Summary of the Penetration Testing

A summary of the penetration testing performed by the evaluator is as follows.

a. Vulnerability of Concern

The evaluator searched into the provided documentation and the publicly available information for the potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing based on the CC supporting documents ([9][10]).

1 First, as a result of searching potential vulnerabilities common to the TOE, there is a concern that the implementation of the secure messaging protocol could, from its behaviour, enable to restore plaintexts or cryptographic keys.

2 Next, taking into account the fact that the platform has been evaluated and certified, tests were performed to confirm the countermeasures implemented based on the guidance of the platform.

In addition, the following penetration tests are considered and it is finally concluded that relevant vulnerabilities of concern cannot be exploited, which are categorised as software attacks mentioned in CC supporting document [9]. However the tests were performed to make sure of the evaluation.

3 Editing commands
4 Direct protocol attacks
5 Replay attacks
6 Bypass authentication or access control

b. Penetration Testing Outline

The evaluator performed the following penetration testing to identify potentially exploitable vulnerabilities.

<Penetration Testing Environment>

Table 8-6 shows details of components of the penetration testing environment and tools used in the penetration testing.

Table 8-6 Configuration of the Penetration Testing

Components	Outline and Purpose of Use
TOE	ID&Trust IDentity-J with SAC (PACE) and AA version 1.0 on IFX M7892 G12 SLJ 52G v1.0.7052 All of the variations listed in Table 8-3 were targeted for penetration testing.
SDI011	Contactless IC card reader
WOLF v1.84 / Python v2.7	Tool for APDU scripting.
Windows PC	Windows PC with which the above IC card reader cooperates, and on which the above software operate.

<Penetration Testing Approach>

Table 8-7 shows vulnerabilities of concern and the content of the penetration testing corresponding to them.

Table 8-7 Content of the Performed Penetration Testing

Viewpoints of Vulnerabilities	Penetration Testing Outline
1. Secure Messaging Protocol Implementation	Check the behaviour of the TOE whether it doesn't give overly specific internal information of the TOE, even when input commands are modified/manipulated.
2.Implementation of countermeasures based on platform guidance	Attempt the PACE mutual authentication procedure and observe the behaviour of the TOE to verify that the documented countermeasures have been implemented.
3.Editing commands 4.Direct protocol attacks	Confirm that the behaviour of the TOE is in accordance with the documented specification with respect to the Active Authentication command with various parameter values. During the PACE authentication procedure, confirm

	that the behaviour of the TOE is secure when the public key sent from the terminal to the TOE is not on the elliptic curve.
5. Replay attacks	After secure messaging is applied, replaying commands is detected and handled, invalid commands are not processed, or the TOE resets.
6. Bypass authentication or access control	After completing PACE authentication for a personalized TOE, files cannot be created where secure messaging is applied. By changing the order of commands in PACE authentication procedure, make sure that the PACE state machine is properly implemented.

c. Result

In the penetration testing performed by the evaluator, the evaluator did not find any exploitable vulnerabilities that attackers who have the assumed attack potential could exploit.

8.5 Evaluated Configuration

In the TOE evaluation, two configurations required by the procurement entity for the passport booklet IC and shown in Table 8-3 were used.
In the TOE evaluation, the evaluation was performed in the configuration shown in "8.4.2 Evaluator Independent Test".
An IC card reader without an optical character reader was used, and evaluation was carried out by setting information of MRZ data on the tool. In actual operation, a terminal equipped with an optical character reader is used, but based on the fact that the interface of the TOE is a contactless IF, the evaluator determined that the evaluation configuration is appropriate.

8.6 Evaluation Results

The evaluator had concluded that the TOE satisfies all work units prescribed in the CEM by submitting the Evaluation Technical Report.

In the evaluation, the following were confirmed.

- PP Conformance: Protection Profile for ePassport IC with SAC (BAC+PACE) and Active Authentication, Version 1.00, (March 8, 2016), Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan (Certification Identification: JISEC-C0500)

- Security functional requirements: Common Criteria Part 2 Extended

- Security assurance requirements: Common Criteria Part 3 Conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.

・All assurance components of EAL4 package

・Additional assurance component ALC_DVS.2

The result of the evaluation is only applied to those which are composed by the TOE corresponding to the identification described in Chapter 2.

8.7 Evaluator Comments/Recommendations

There is no evaluator recommendation to be addressed to consumers.

9. Certification

The Certification Body conducted the following certification based on the materials submitted by the Evaluation Facility during the evaluation process.

1. Contents pointed out in the Observation Reports shall be adequate.

2. Contents pointed out in the Observation Reports shall properly be solved.

3. The submitted documentation was sampled, the content was examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.

4. Rationale of the evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.

5. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

9.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report, Observation Reports and related evaluation documentation, the Certification Body determined that the TOE satisfies all assurance requirements for EAL4 augmented by ALC_DVS.2 in the CC Part 3.

9.2 Recommendations

There is no note.

10. Annexes

There is no annex.

11. Security Target

The ST-Lite [15] of the TOE is provided as a separate document from this Certification Report.

Security Target Lite ID&Trust IDentity-J with SAC (BAC+PACE) and AA, v1.4, 26.07.2019, ID&Trust Ltd.

This ST-Lite is the sanitized version of the evaluated full ST [14] based on the CC supporting document, ST sanitising for publication [13].

12. Glossary

The abbreviations relating to the CC used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

The definitions of terms and abbreviations relating to the TOE used in this report are listed below.

Active Authentication	A security mechanism in which a public key and private key pair using the public key cryptography system is stored to keep the private key secret in the IC chip constituting a part of the TOE. The public key is transmitted to an external device trying to authenticate the TOE and after that the TOE will be authenticated through cryptographic calculation by the challenge-response protocol using the private key, which has been kept secret in the TOE. The Active Authentication protocol has been standardized by ICAO.
Active Authentication Information	Authentication data for writing Active Authentication key pairs
Access Key	
Basic Access Control	A mechanism for the mutual authentication and Secure Messaging specified in the ePassport specifications [20], which is referred to as BAC.
Issuance	To make a passport legally valid. To create a passport itself to render it effective as a passport.
Passive Authentication	A security mechanism in which the digital signature of the passport issuing authority is put on personal data to be stored in the TOE and if the PKI system with assured interoperability is used by both the passport issuing and receiving ends, authenticity of the data read from the TOE will be verified. The Passive Authentication procedure has been standardized

	by ICAO.
Passport	An identification document issued by a national government or an equivalent public institution to an overseas traveler. In general, a passport is issued as a booklet (passport booklet).
Passport issuing authorities	The Ministry of Foreign Affairs, passport manufacturers and regional passport offices under the direction of the said Ministry. The passport manufacturers file plastic sheets with TOEs into passport booklets in which necessary information other than personal information (birthdate, facial image data, security-related data regarding the aforementioned data, etc.) are written. Personal information are to be written in the passports by passport officers.
Passport manufacturer	A manufacturer manufacturing passport booklets with TOEs in which basic data (management data such as a passport number, an active authentication public key and a private key pair, etc.) will be written.
Passport office	A passport issuing organisation at which personal information of a passport holder is written in a passport booklet including the TOE. Passport offices, located in various regions, serve as a point of contact for a passport applicant to which a passport will be delivered.
Password Authenticated Connection Establishment	A mechanism for the mutual authentication and Secure Messaging specified in the ePassport specifications [20], which is referred to as PACEv2.
Password key file	A file containing keys derived from MRZ data and used for the nonce encryption in the PACEv2 protocol
Readout key	Authentication data for reading IC chip serial numbers
Secure Messaging	A set of means for cryptographic protection of [parts of] command-response pairs (See 3.50 of ISO/IEC 7816-4:2013.)
Transport key	Authentication data for protecting an integrated circuit (IC) chip against unauthorised use during its transportation
AES	Advanced Encryption Standard
ATR	Answer-to-Reset
BAC	Basic Access Control
CBC	Cipher Block Chaining
CMAC	Cipher-based MAC
DEMA	Differential Electro-Magnetic Analysis

DES	Data Encryption Standard
DF	Dedicated file. Structure containing file control information and, optionally, memory available for allocation. (See the definition 3.19 in ISO/IEC 7816-4:2013.)
DFA	Differential Fault Analysis
DG	Data Group
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EF	Elementary file. Set of data units or records or data objects sharing the same file identifier. (See 3.23 of ISO/IEC 7816-4:2013.)
EF.ATR/INFO	Answer-to-Reset file or Information file (See Clause 4 of ISO/IEC 7816-4:2013.)
EF.CardAccess	EF deployed directly under MF and contains PACEv2 security information
EF.COM	EF that provides the list of DGs located under the DF containing the version information for the Logical Data Structure (LDS), which specifies the types of formats to be used for data storage in ICs for passport booklets, and an ePassport application
EF.DG1	EF containing the MRZ data
EF.DG2	EF containing a facial image
EF.DG13	EF containing management data (a passport number and booklet management number)
EF.DG14	EF containing PACEv2 security information and information on hash functions for Active Authentication
EF.DG15	EF containing an Active Authentication public key
EF.SOD	EF containing hash values of other data groups and the digital signature for Passive Authentication
ICAO	International Civil Aviation Organization
JCOS	Java Card Operating System
MAC	Message Authentication Code
MF	Master file. A unique DF representing the root in a card using a hierarchy of DFs. (See 3.33 of ISO/IEC 7816-4:2013.)
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone. A machine readable zone that consists of a digitized facial image printed on the personal data page of ePassports, and the area for 88 letters provided at

	the bottom of the personal data page, in which personal data such as a name, nationality, sex, date of birth, passport number and date of expiry are printed.
MRZ data	Information printed on the data page of ePassports, which can be read by a terminal
OID	Object Identifier
PACE	Password Authenticated Connection Establishment
PACEv2	Password Authenticated Connection Establishment v2
PACEv2 security information	Information such as cryptographic algorithms and domain parameters used in PACEv2
PKI	Public Key Infrastructure
SAC	Supplemental Access Control Subsection 1.1.3 titled "Supplemental Access Control" of the bibliography [32] gives the following explanations. "This Technical Report specifies PACE v2 as an access control mechanism that is supplemental to BAC. PACE MAY be implemented in addition to BAC, i.e. — States MUST NOT implement PACE without implementing BAC if global interoperability is required. — Inspection Systems SHOULD implement and use PACE if provided by the MRTD chip."
SHA	Secure Hash Algorithm
SOD	Document Security Object

13. Bibliography

[1] IT Security Evaluation and Certification Scheme Document, July 2018, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, September 2018, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, September 2018, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part2:

Security functional components Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[7] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[8] Application Notes and interpretation of the Scheme(AIS34), Version 3, September 2009, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[9] Joint Interpretation Library - Application of Attack Potential to Smartcards, Version 2.9, January 2013

[10] Joint Interpretation Library - Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018

[11] Joint Interpretation Library – Minimum Site Security Requirements, Version 2.1 (for trial use), December 2017

[12] Protection Profile for ePassport IC with SAC (BAC+PACE) and Active Authentication, Version 1.00, (March 8, 2016), Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan (Certification Identification : JISEC-C0500)

[13] ST sanitising for publication, April 2006, CCDB-2006-04-004

[14] Security Target ID&Trust IDENTITY-J with SAC (BAC＋PACE) and AA, v1.3, 26.07.2019, ID&Trust, Ltd.

[15] Security Target Lite ID&Trust IDENTITY-J with SAC (BAC＋PACE) and AA, v1.4, 26.07.2019, ID&Trust, Ltd.

[16] Security Target Lite for BSI-DSZ-CC-0869-V2-2019, “Security Target Lite Java Card Platform Implementation for Infineon on M7892 G12 (SLJ52GxxyyyzC) v2.0”, Version 3.6, May 2019, Oracle Corporation

[17] Security Target Lite for BSI-DSZ-CC-0891-V3-2018, “Security Target Lite Common Criteria EAL6 augmented / EAL6+ M7892 Design Steps D11 and G12”, Version 1.2, 2017-11-21, Infineon Technologies AG

[18] Certification Report BSI-DSZ-CC-0869-V2-209 for Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0, 13 June 2019, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[19] ID&Trust IDentity-J with SAC (BAC+PACE) and AA version 1.0 on IFX M7892 G12 SLJ 52G EVALUATION TECHNICAL REPORT SUMMARY, Version 5, 2019-07-29, TÜV Informationstechnik GmbH – Evaluation Body for IT Security

[20] DOC 9303 Machine Readable Travel Documents Seventh Edition, ICAO, 2015

[21] Technical Guideline TR-03111, Elliptic Curve Cryptography, Version 2.0, 2012, Bundesamt für Sicherheit in der Informationstechnik

[22] ID&Trust IDentity-J-v1.0 Applet for Japanese e-Passport User's Guide, Version 1.0.12, 2019-07-21

[23] OBSERVATION REPORT (OR) AGD and FSP, Version 7, 2019-06-11, Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (TÜViT)

[24] OBSERVATION REPORT (OR) ALC ID&T, Version 3, 2019-02-26, Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (TÜViT)

[25] OBSERVATION REPORT (OR) ASE, Version 9, 2019-07-19, Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (TÜViT)

[26] OBSERVATION REPORT (OR) ADV (TDS & ARC), Version 6, 2019-04-24, Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (TÜViT)

[27] OBSERVATION REPORT (OR) NPB, Version 3, 2018-11-20, Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (TÜViT)

[28] OBSERVATION REPORT (OR) ALC MAXELL, Version 4, 2019-03-04, Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (TÜViT)

[29] OBSERVATION REPORT (OR) ATE, Version 3, 2019-05-21, Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (TÜViT)

[30] Protection Profile for ePassport IC with Active Authentication, Version 1.00, (February 15, 2010), Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan (Certification Identification : JISEC-C0247)

[31] RF protocol and application test standard for eMRTD – part 3, tests for application protocol and logical data structure, Version: V2.07, October 10, 2014, ICAO.

[32] International Civil Aviation Organization, ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.1, 15 April 2014