SHARP Passport Booklet module

Security Target – lite –

ST Version 1.13-1

November 17th, 2006

SHARP CORPORATION
IC CARD DEVELOPMENT DEPT.
SYSTEM-FLASH DIVISION
LARGE-SCALE IC GROUP

MASATOSHI KOBOTA, HIROSHI YAMAMORI
With support by TNO ITSEF BV

This document is the Security Target – lite – of the SHARP Passport Booklet module. This Security Target – lite – is the public version of the Security Target for the SHARP Passport Booklet module, version 1.13 of August 25, 2006.

TABLE OF CONTENTS

1 ST Introduction 5
1.1 ST Identification 5
1.2 ST Overview 5
1.3 CC Conformance 5
1.4 References 6
1.4.1 Relating Standards and Documents 6
1.4.2 Relating Protection Profile 7
1.5 Terminology and Abbreviation 8
1.5.1 Terminology 8
1.5.2 Abbreviation 11
2 TOE Description 12
2.1 TOE Components 12
2.2 TOE Scope 13
2.3 Procedure from Development to Final Use of the Passport Booklet Module 14
2.4 Security Functions of the Passport Booklet Module 15
2.4.1 Software functions 15
2.4.2 Hardware Functions 16
3 TOE Security Environment 17
3.1 Assumptions 17
3.2 Threats 17
3.2.1 Assets of Protection 17
3.2.2 Threats of Use Environment 18
3.3 Organizational Security Policies 18
4 Security Objectives 20
4.1 Security Objectives for the TOE 20
4.2 Security Objectives for the TOE Environment 21
5 IT Security Requirements 22
5.1 Subjects and Objects 22
5.2 Policies 22
5.2.1 The ePassPort Policy 22
5.2.2 The Secure Communication Policy 23
5.2.3 User Policy 23
5.2.4 TOE-Self Protection Policy 24

5.3 SPM Rationale 25
5.3.1 SPM- FSP correspondence 25
5.4 TOE Security Requirements 25
5.4.1 TOE Security Functional Requirements 25
5.4.2 Minimum Strength of Function 34
5.4.3 TOE Security Assurance Requirements 35
5.5 Security Requirements for the IT Environment 36
6 TOE Summary Specification 37
6.1 Security Functions 37
6.2 Strength of Security Functions 39
6.3 Assurance Measures 39
7 PP Claims 41
8 Rationale 42
8.1 Security Objectives Rationale 42
8.1.1 Threats and security objectives 43
8.1.2 Organisational security policies and security objectives 43
8.1.3 Assumptions and security objectives 43
8.2 Security Requirements Rationale 44
8.2.1 Security objectives and security functional requirements 44
8.2.2 Security objectives and security assurance requirements 45
8.2.3 Dependencies and mutual Support 45
8.2.4 Minimum strength of function 47
8.3 TOE Summary Specification Rationale 48
8.3.1 Security Functions Rationale 48
8.3.2 Security Functions Strength Rationale 53
8.3.3 Assurance Measures Rationale 54
8.3.4 The requirements are internally consistent 54
8.3.5 The requirements are mutually supportive 54

1 ST Introduction

1.1 ST Identification

ST Title:	SHARP Passport Booklet module Security Target – lite –
ST Version:	1.13-1
Issued Date:	November 17th, 2006
Author:	SHARP Corporation
	IC Card Development Dept.
	System-Flash Division
	Large-Scale IC Group
	Masatoshi Kobota, Hiroshi Yamamori
TOE Title:	SHARP Passport Booklet module
TOE Version:	1.1
Evaluation assurance level:	EAL4 augmented with AVA_VLA.4
Minimum strength of function:	SOF-high

1.2 ST Overview

The Target of Evaluation (TOE) is the SHARP passport booklet module (called the passport booklet). This is a composite TOE consisting of an application for the Passport Booklet ePassJP, a card operating system eP-APE and the SM4128(V3) module[1] (a packaged IC).

ePassJP is the application implementing e-passport functions as specified by ICAO [ICAO]. eP-APE supports that the ePassJP can run on the SM4128(V3) module. The SM4128(V3) module is described in the Security Target [ST-HW].

1.3 CC Conformance

- The functional requirement for the TOE conforms to ISO/IEC 15408-2:2005(E) (CC V2.3 part2).
- The assurance requirements for the TOE conform to ISO/IEC 15408-3:2005(E) (CC V2.3 part3): EAL4 augmented with AVA_VLA.4.

This Security Target uses the following Protection Profile (Conforming PP) is:

"*Protection profile for IC for the passport booklet, version1.0, 24 September 2004, Ministry of Foreign Affairs - Consular Affairs Bureau - Passport Division / JBMIA e-MRP/WG3*".

Regarding eavesdropping an additional objective for the environment is added in line with interna-

[1] The module is evaluated under BSI-DSZ-CC-0245 and available as A5 and A7 step. The A7 is a maintenance version of the A5 step.

tional developments regarding Machine Readable Travel Documents with „ICAO Application"[2].

The PP is not CC certified, but is the official requirements document of the Japanese government. This ST lite does not integrate the PP, however the official ST integrates the PP.

1.4 References

1.4.1 Relating Standards and Documents

- Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1:Introduction and general model, ISO/IEC 15408-1:2005
- Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2:Security functional requirements, ISO/IEC 15408-2:2005
- Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3:Security assurance requirements, ISO/IEC 15408-3:2005
- Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1:Introduction and general model, JIS X 5070-1:2000
- Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2:Security functional requirements, JIS X 5070-2:2000
- Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3:Security assurance requirements, JIS X 5070-3:2000
- Common Criteria for Information Technology Security Evaluation – part 1: Introduction and general model, August 1999 Ver.2.1, translation in January 2001 ver.1.2, Information-technology Promotion Agency, Japan – IT Security Center
- Common Criteria for Information Technology Security Evaluation – part 2: Security functional requirements, August 1999 Ver.2.1, translation in January 2001 ver.1.2, Information-technology Promotion Agency, Japan – IT Security Center
- Common Criteria for Information Technology Security Evaluation – part 3: Security assurance requirements, August 1999 Ver.2.1, translation in January 2001 ver.1.2, Information-technology Promotion Agency, Japan – IT Security Center
- Evaluation standard supplement document “supplement-0407”, August 2004, Information-technology Promotion Agency, Japan – IT Security Center
- Evaluation standard supplement document “supplement-0210 ver.2.0”, August 2004, Information-technology Promotion Agency, Japan – IT Security Center
- Evaluation standard supplement document “CCIMB Interpretations-0407”, August 2004, Information-technology Promotion Agency, Japan – IT Security Center

[2] These developments are for example compiled in Protection Profiles, see for a current version [ICAO2].

- [ST-HW] SM4128(V3) LSI FOR USE IN NATIONAL IDS AND PASSPORTS WITH SHARP SOFTWARE Version 1.8.5, 29 March 2005, SHARP Corporation - Integrated Circuits Group
- [ICAO] PKI for Machine Readable Travel Documents offering ICC read-only access V1.1, October 01, 2004, ICAO-NTWG
- [ICAO2] Common Criteria Protection Profile, Machine Readable Travel Document with „ICAO Application", Extended Access Control (BSI-PP-0026), Version 1.0, 7th June 2006.

1.4.2 Relating Protection Profile

- [PP-ePassport] Protection profile for IC for the passport booklet, version1.0, 24 September 2004, Ministry of Foreign Affairs - Consular Affairs Bureau - Passport Division / JBMIA e-MRP/WG3.
  Note: This PP is in Japanese and has not been CC evaluated. Therefore the official ST includes the PP translated to English which is authorized by the Japanese government as the official requirements document.
- [EuroPP] Smartcard IC Platform PP Ver.1.0, July 2001, EUROSMART(BSI-PP-0002)

1.5 Terminology and Abbreviation

1.5.1 Terminology

- APE

  Application execution Environment, the smartcard OS.

- Eavesdropper

  A threat agent reading the communication between the MRTD's chip and the End-User to gain the data on the MRTD's chip.

- ES

  Application dependent part of the software for passport booklet module.

- DS

  Part which controls hardware of passport booklet module directly, in this TOE: the APE.

- FROM

  Flash Memory (Flash EEPROM (Electrically Erasable and Programmable Read Only Memory))

- ICAO

  International Civil Aviation Organization. One of the specialized agencies of the United Nations established based on the international civil aviation treaty.

- OS

  APE

- R/W

  Reader writer for IC passport (passport booklet module).

- IC Passport

  Software running on contactless smartcard hardware, used to record digitalized passport data including biometric data (face image) of the passport booklet owner. The TOE is physically placed in one of the passport booklet pages.

- Printing Bureau

  Place where second issuance of the passport booklet is executed.

· Entity

Arbitrary organization, IT equipments, or personnel placed outside of TOE, which communicates with TOE.

· Command Flag

Flag which controls execution rights of system management commands.

· Manufacturer

Generic name of entity related to development or manufacturing stage of passport booklet module.

· Biometric Data

Data obtained from human characteristics.

· Secure Messaging

Data communication method protected by encryption, and equipped with data concealment and integrity check feature for data transmitted during command execution.

· Session Key

Key generated during mutual recognition. Information read from the passport booklet module is encrypted with this key, preventing tapping of the information.

· Mutual Authentication

Authentication implemented mutually, between the terminal unit and the passport booklet module, for reading information of the face image.

· Tamper Resistance Function

Security function which complicates analysis (illegal access to data, tamper of data or functions) of stored data or internal structure, of the software or the hardware.

· Terminal Unit

Equipment composed of reader device to communicate with passport booklet module and display device to display data received from the passport booklet module.

· Second Issue

Write basic information (passport number, booklet number) as a passport booklet and update transport key for transporting to the next entity.

· Administrator

General name for entity related to second and third order issuance.

· Passport Booklet Owner

The owner of the passport booklet.

· Passport Booklet

SHARP passport booklet module equipped with tamper resistance function, complies with IC passport, which stores digitalized facial image of the passport booklet owner to the IC (integrated circuit), scheduled to be adopted in Japan from March 2006. The module is equipped with CPU, RAM, ROM, Flash Memory, and Co-processor, and is plastic encapsulated.

· Passport office

Place where the third order issue of the passport booklet module is executed.

· Logical block ID

ID to identify data in the FROM by each logical block (Application/Data/etc).

· End-user

Border patrol station. This is an external IT entity that interacts with the sharp passport booklet module according to the ICAO specification.

· Administrator

The external IT entity (used by manufacturer and National Printing Bureau) used to communicate TSF data (e.g. the digitalized passport data including biometric data (face image) of the passport booklet owner.) with the sharp passport booklet module.

1.5.2 Abbreviation

APE : Application execution Environment

CC : Common Criteria

C-APDU : Command Application Protocol Data Unit

CM : Configuration Management

DES : Data Encryption Standard

DS : Dedicated Software

EAL : Evaluation Assurance Level

ECC : Elliptic Curve Cryptosystem

ES : Embedded Software

FROM : Flash Memory (Flash EEPROM)

IC : Integrated Circuit

ICAO : International Civil Aviation Organization

MRTD : Machine Readable Travel Document

OS : Operating System

PIN : Personal Identification Number

PP : Protection Profile

RSA : Riverst Shamir Adleman

R-APDU : Response Application Protocol Data Unit

SFP : Security Function Policy

SOF : Strength Of Function

TOE : Target Of Evaluation

TSC : TSF Scope of Control

TSF : TOE Security Functions

TSP : TOE Security Policy

2 TOE Description

2.1 TOE Components

The Target of Evaluation (TOE) is the SHARP passport booklet module (called the passport booklet). This is a composite TOE consisting of an application for the Passport Booklet ePassJP, a card operating system eP-APE and the SM4128(V3) module (a packaged IC).

ePassJP is the application implementing e-passport functions as specified by ICAO [ICAO]. eP-APE supports that the ePassJP can run on the SM4128(V3) module. The SM4128(V3) module is described in the Security Target [ST-HW]. Figure 2-1 shows the TOE composition of hardware (SM4128(V3) module), operating system (eP-APE) and e-passport application (ePassJP).

The basic function of the TOE is as follows.

- Function of selecting file which stores data
- Function of reading data
- Function of writing data
- Enforcing access control rules on the access to data, including use of secure messaging

The hardware supports the software by providing separation between applications, and between applications and operating system. The hardware also provides protection against physical attacks. Note that the software does not require the hardware to provide protection of the Triple-DES keys used in the secure messaging, as these keys are derived from data printed on the passport booklet itself, and therefore do not need to be protected against side channel attacks that require physical access to the booklet module.

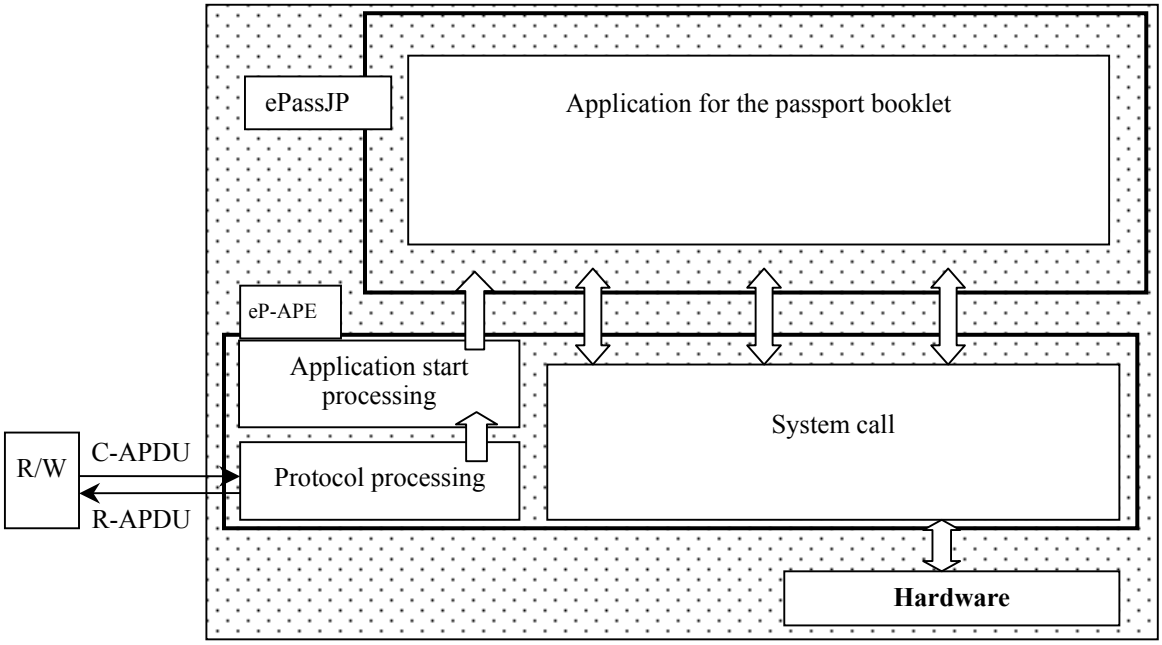

Figure 2-1: TOE Composition (TOE is the grey area)

2.2 TOE Scope

The TOE physically consists of a packaged module containing the following (based on [ST-HW]):

- A packaged module containing:
  - The circuitry of an IC (hardware, including the physical memories RAM, ROM and Flash ROM (FROM))
  - The following IC dedicated software:
    - BootROM (including DRNG function)
    - TestROM (test functionality is disabled before TOE delivery)

- The following Guidance documents:
  - Outline of the manufacture process command of eP-APE 1.100, version 1.2.0
  - SHARP e-Passport Module Users Manual, revision 1.01
  - Sharp Passport Booklet User guidance, version 1.0

The logical scope of the TOE is:

- APE version eP-APE 1.100 (the Operating System)
- Application for the Passport Booklet ePassJP version 1.0 (the application implementing the e-passport functions)
- Data.

The logical interface of the TOE consists of proprietary APDUs and the APDUs defined in [ICAO] which follow the format of ISO/IEC 7816, and the method of the communication of ISO/IEC 14443.

Explicitly excluded from the TOE (logical) scope:

- The (encrypted) value of the administrator authentication PIN[3]. This is necessary because (for additional security) the administrator authentication PIN is changed regularly.
- The value of the CPLD data[4], which contains information about when and where the TOE was manufactured. This is necessary because this data is variable (it contains e.g. a date of manufacturing).

Figure 2-2 shows the TOE in its environment (the passport reader at a border control station).

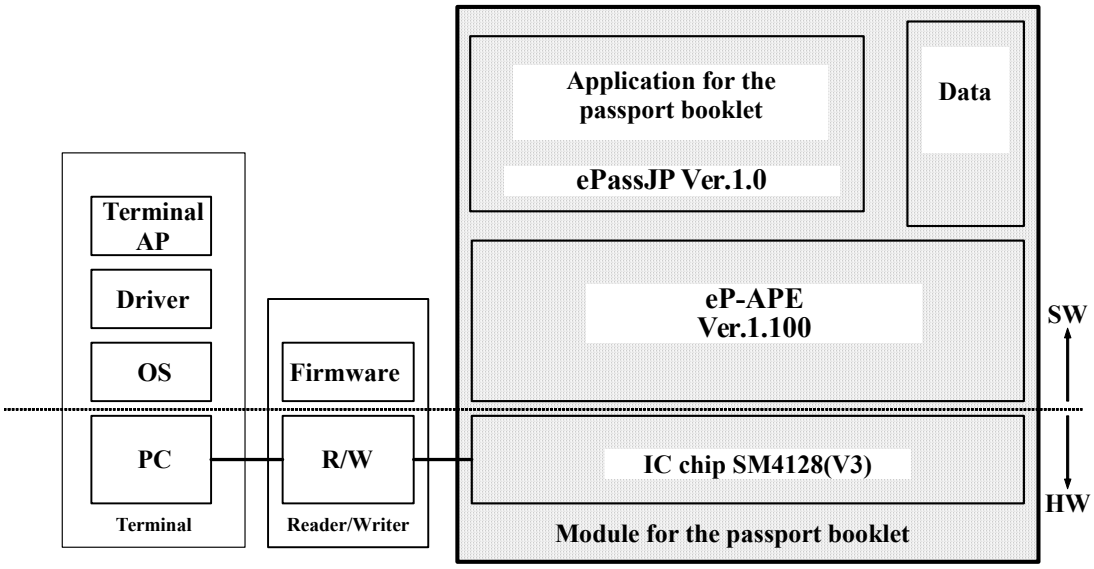

Figure 2-2: System Configuration (TOE physical scope is denoted by grey area)

2.3 Procedure from Development to Final Use of the Passport Booklet Module

The passport booklet module lifecycle consists of various phases. In this section, the relation of entities and the range of the responsibilities are clarified. Figure 2-3 shows the flow from the development to the final use of the passport booklet module.

[3] The existence and handling of the data is NOT outside the TOE scope, only its value.

[4] The existence and handling of the data is NOT outside the TOE scope, only its value.

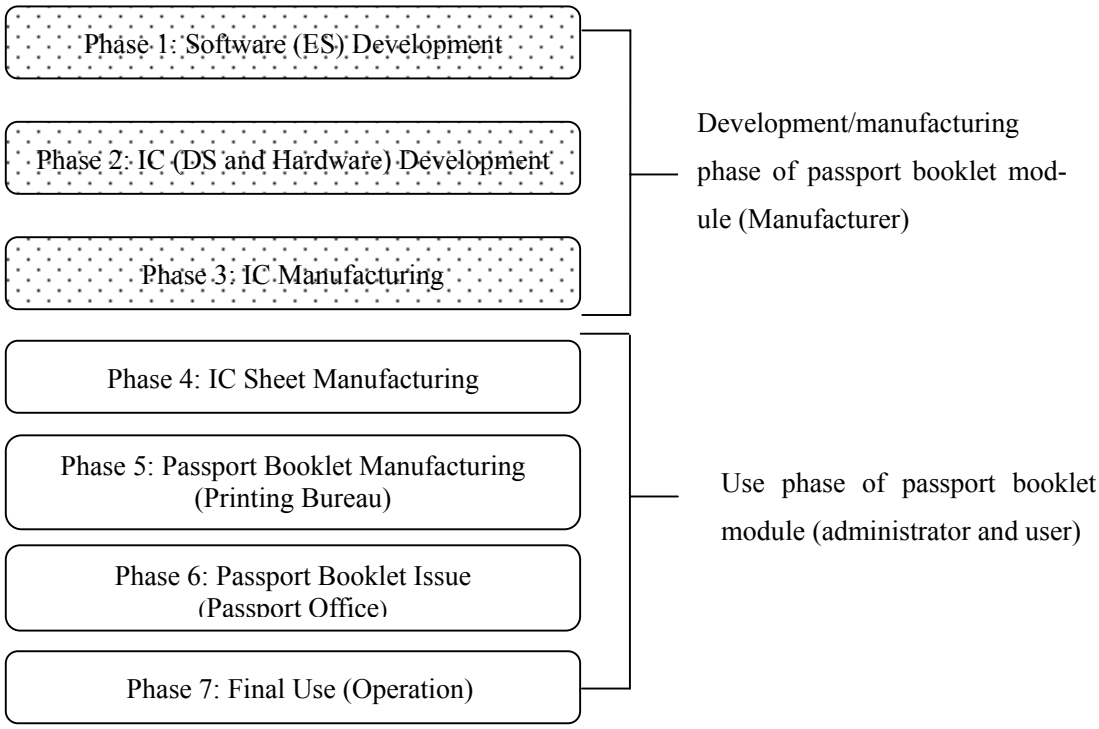

Figure 2-3: Flow of Passport Booklet Module (TOE is grey area)

The TOE is delivered in module form. This means that it is delivered at the end of phase 3, therefore the relevant phases of the lifecycle model for this TOE are Phases 1, 2, and 3. Phases 2, 3 were covered by the hardware evaluation [ST-HW].

2.4 Security Functions of the Passport Booklet Module

2.4.1 Software functions

The TOE software provides the following APDU's:

- CHANGE_REFERENCE_DATA
- CREATE MF
- CREATE_FILE
- FORMAT
- GET_CHALLENGE
- LOCK FORMAT
- MANAGE_ATTRIBUTE
- MANAGE_SECURITY_ENVIRONMENT
- MUTUAL_AUTHENTICATE
- READ BINARY
- SELECT FILE
- VERIFY

- WRITE BINARY
- ReadTestData
- WriteTestData

This will realise the security functionality, i.e. access control, deactivation of writing files on operation phase, mutual authentication, secure messaging and protection of physical tampering.

2.4.2 Hardware Functions

The functions of the (SM4128(V3) module, the hardware of the TOE, are described in the hardware Security Target [ST-HW].

Informational Note

- The physical interfaces[5] of the TOE[6]:
  - The physical interface of the TOE to the environment is the entire surface of the module. The physical interface to an attacker consists of the entire surface of the module, the passivation layer, the shielding layer, the flat layout, the narrow wiring and the scrambled data bus.
- The environmental interface[5] of the TOE[6] is the temperature.

  The electrical interface of the TOE to the environment are the ISO7816 contacts (RST, CLK, and I/O), the ISO14443 contacts (CL2 and CL3), the backside pins (IOR0, IOR1, RFTEST, T_SO and MRGRD), the power pins (VCC, GND, VFF, VDD, VPPO, VPP and VNN), the covered and blocked pins (A[18:0], DQ[15:0], RPB, CEB, WEB, WPB, CK1IO, CK2IO, CPRCKIO and OEB) and the covered pins (RBB, REGDIS, T_DEMIN, T_CLK, T_RSTB, MRGRD and T_SI).

[5] It is taken from [ST-HW]. Note that the internal software interface removed as it is no longer an externally accessible interface.

[6] Note that only the ISO 14443 interface is used in normal interaction with the TOE. Backside pins are not accessible.

3 TOE Security Environment

This ST doesn't introduce any new Assets of Protection, Threats of Use Environment, Organizational Security Policies, Security Objectives for the TOE, Security Objectives for the Environment and Security Objectives Rationale.

3.1 Assumptions

A.1 (TOE Management):

The TOE, which is embedded in a passport booklet, is assumed to be protected from any physical attacks in the Printing Bureau and the passport offices.

A.2 (Issuing environment):

The Printing Bureau and the passport offices are assumed to issue passport booklets in secure manner.

A.3.1 (Secure delivery 1):

The delivery processes after the TOE has been once delivered to manufacturer from the developer are assumed to be protected from any physical attacks.

A.3.2 (Secure delivery 2):

The delivery processes from manufacturer to the National Printing Bureau are assumed to be protected from any physical attacks.

A.4 (Anti-eavesdropping measures):

The End-User will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the authentication protocol of the module.

3.2 Threats

3.2.1 Assets of Protection

Asset to be protected by the TOE are the user data as follows:

- Personal information: face image, name etc.
- Passport information: passport number, hash values, digital signatures etc.

The following data are included in the assets.

- IC Serial Number
- TSF Data

3.2.2 Threats of Use Environment

The user environment of the TOE, as mentioned in section 2.3, are assumed as the phase from [4] to [7]. Before the TOE is delivered to the end user (the owner of the passport booklet), it is assumed that the TOE is managed securely and there is no threat for the assets as mentioned in section 3.1. Therefore, the threats to be countered arise from the environment of the end use (operational) phase.

Although the user information written in the TOE is not secret, it should be protected from unintended reading out. For example, an attacker could skim the personal information off illegally from the TOE via its contactless communication interface. It should be prohibited that the personal information in the TOE is read out without being acknowledged.

T.1 (Illegal read out):

An attacker reads out the user data from the TOE via the contactless interface by using an illegal terminal device to abuse the information.

T.2 (Physical tampering):

An attacker tampers parts, elements or data within the TOE physically to forge a passport booklet.

T.3 (Illegal modification):

An attacker modifies or adds user data of the TOE via interfaces of the TOE.

Application note

Threat T1 includes skimming threat.

3.3 Organizational Security Policies

P.1 (ID Read out):

The TOE maintains integrity of the IC serial number of the TOE and the administrator is able to read out the number.

P.2 (Mutual authentication):

The TOE can perform mutual authentication with a terminal device.

P.3 (Secure messaging):

Communication between the TOE and a terminal device is protected from eavesdropping.

P.4 (Transport key invalidation):

The TOE has verification error counters of transport keys and invalidates a transport key when the error counter for the transport key exceeds the specified limit.

P.5 (High attack potential):

The TOE shall be resistant to attacks performed by an attacker possessing a high attack potential.

Application notes

- Policy P.3 (Secure messaging) indicates that communication between TOE and the terminal device is protected from eavesdropping. The secure messaging mechanisms complies with the ICAO standard. This is defined by the Japanese government and implies that the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal.. Note that eavesdropping is not considered a threat.
- The rationale for policy P.5 (high attack potential) is as follows: A passport is considered to be a valuable document and the unauthorized copy and modification of user data are considerable threats. Therefore resistance to an attack potential “high” is considered to be appropriate.

4 Security Objectives

4.1 Security Objectives for the TOE

O.1 (Identification and authentication, access control):

The TOE must assure that only authorized users are granted to access user data.

O.2 (ID read out):

The TOE must maintain its individual IC serial number and present it according to request.

O.3 (Modification prohibition):

The TOE must prohibit modification of the stored data or adding any new data.

O.4 (Mutual authentication):

The TOE must provide mutual authentication function with a terminal device.

O.5 (Secure messaging):

The TOE must protect communication data with a terminal device from unauthorized disclosure.

O.6 (Physical tampering):

The TOE must counter physical tampering.

O.7 (Transport key invalidation):

The TOE must invalidate the transport key when verification errors exceed the specified limit.

O.8 (High attack potential):

The security functional requirements and the assurance requirements of the TOE correspond to attacks performed by an attacker possessing a high attack potential.

PP application note

"O.3 (Modification Prohibition)", "TSF must prohibit writing of the new data.", is not relevant since this TOE does not provide the function of rewriting data once written.

4.2 Security Objectives for the TOE Environment

OE.1 (TOE Management):

The Printing Bureau and the passport offices must protect the TOE from any physical attacks during the issuing phases.

OE.2 (Issuing environment):

The Printing Bureau and the passport offices must issue passport booklets in secure manner.

OE.3a (Secure Delivery 1):

The delivery processes after the TOE has been once delivered to manufacturer from the developer must be protected from any physical attacks.

OE.3b (Secure Delivery 2):

The delivery processes from manufacturer to the National Printing Bureau must be protected from any physical attacks

OE.4 (Anti-eavesdropping measures):

The End-User will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the authentication protocol of the module.

5 IT Security Requirements

5.1 Subjects and Objects

This section defines the subjects and objects used within the SFRs:

- Subjects:
  - Administrator
  - End-user
- Objects:
  - ePassPort data: (consisting of the files DG1, DG2, DG13, DG.SOD and DG.COM)
  - The CPLD data
  - Keys: Transport Key, Reading Out Key, CPLD Key, End User Authentication Key

5.2 Policies

This section defines the various security policies. Each security policy model:

- Describes the rules and characteristics of the policy.
- Includes a policy to SFR mapping.

The Security Policy Model is integrated in the ST to enhance understandability of the SFRs and to assist in meeting the ADV_SPM.1 Informal Security Policy Model requirements.

5.2.1 The ePassPort Policy

This ePassPort policy describes who can read and write what in the TOE. The rules and characteristics of this policy are:

1. The TOE shall:
   - Provide access to objects (specified through FDP_ACC.2 and FDP_ACF.1)
   - Export and import data (specified through FDP_ETC.1 and FDP_ITC.1)

   in accordance with the following rules:

Administrators authenticated by the Transport Key can: • Modify the Transport Key • Modify the End User Authentication Key • Write DG1, DG2, DG13, DG.SOD and DG.COM once • Read DG1, DG2, DG13, DG.SOD and DG.COM Administrators authenticated by the Reading Out Key can: • Read DG13

Administrators authenticated through the CPLD Key can:

- Read CPLD
- Write CPLD (only if the write functionality has not been deleted, see FIA_AFL.1 in the User Policy)

Authenticated end-users can:

- Read DG1, DG2, DG13, DG.SOD and DG.COM

2. All security attributes are restrictive and cannot be changed (specified through FMT_MSA.3 and FMT_MSA.1)
3. No security functions can be managed in any way (specified through FMT_MOF.1)
4. The TSF data that can be modified (by the administrator): transport key and end-user authentication key. (Specified through FMT_MTD.1)

5.2.2 The Secure Communication Policy

The Secure Communication Policy arranges the secure communication between the End-User and the TOE. The rules and characteristics of this policy are:

- Triple DES using a Session Key encrypts communication of data between End-User and TOE. This is specified by FCS_COP.1
- This Session Key is generated when a MUTUAL AUTHENTICATE command is successfully completed. This is specified by FCS_CKM.1.
- This Session Key is set to invalid when:
  - Another MUTUAL AUTHENTICATE command is received. This invalidates the old Session Key whether it is successful or not. If the command is successfully completed it will generate a new Session Key.
  - The TOE finds an abnormality while processing an encrypted message

  Invalid keys are no longer used. This is specified by FCS_CKM.4
- This Session Key is overwritten whenever the TOE is initialized or reset. This is specified by FCS_CKM.4.
- Nobody can access the Session Key, or, in other words, any value for its security attributes (which it doesn't have) is therefore secure. This is specified by FMT_MSA.2.

5.2.3 User Policy

The User Policy defines the various users of the TOE, and how they identify and authenticate. The rules and characteristics of this policy are as follows:

- The different roles are Administrator and End-user. This is specified in FMT_SMR.1.
- These roles are associated with subjects. This is specified with FIA_ATD.1 and FIA_USB.1
- Before a user is successfully identified and authenticated to the TOE he can only perform

these commands:

- Execute ReadTestData
- SELECT FILE
- GET CHALLENGE
- VERIFY
- MUTUAL AUTHENTICATE

This is specified with FIA_UAU.1 and FIA_UID.1

- The MUTUAL AUTHENTICATE command is used to authenticate end-users. This is specified through FIA_UAU.5
- The VERIFY command is used to authenticate administrators. This is specified through FIA_UAU.5
- Administrators can authenticate using different keys. If they use a different keys they obtain different access rights. This is specified through FDP_ACF.1 (see the ePassPort policy).
- When authenticating, a maximum number of tries is allowed, depending on the key that is used. This is specified through FIA_AFL.1

List of authentication events	*Positive integer number*
Authentication by the transport key	3
Authentication by Reading out key	3
CPLD key	∞
End-user Mutual Authentication key[7]	∞

- When this number is exceeded (only relevant for the transport key and reading out key, one can never authenticate again using that key. This is specified through FIA_AFL.1
- If authentication has been disallowed against both the transport key and the reading out key, the write functionality of the TOE shall be permanently deleted. This is specified through FIA_AFL.1

5.2.4 TOE-Self Protection Policy

The TOE Self-Protection Policy arranges the way the TOE protects itself and some of the User Data. Its rules and characteristics are as follows:

- The TOE and its subjects cannot be logically interfered or tampered with. This is specified by FPT_SEP.1
- The TOE cannot be successfully physically attacked. This is specified by FPT_RVM.1
- The TSP cannot be bypassed. This is specified by FPT_RVM.1
- The TOE detects when user data is corrupted through failure of the TOE. This is specified by FDP_SDI.1

[7] The key used for Mutual Authentication by the end-user is included here for completeness only.

5.3 SPM Rationale

The mapping of each individual policy to the SFRs has been clearly described in the description of each policy. Given the fact that the mapping between SFRs and policies is very straightforward, no further rationale has been included.

5.3.1 SPM- FSP correspondence

This correspondence has been included in the Functional Specification.

5.4 TOE Security Requirements

5.4.1 TOE Security Functional Requirements

This chapter defines the functional requirements to TOE.

5.4.1.1 FCS_CKM.1 Cryptographic key management

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

- [assignment: list of standards]:As defined in [ICAO]
- [assignment: cryptographic key generation algorithm]:As defined in [ICAO], Annex E.1.
- [assignment: cryptographic key sizes]:112bit

Dependencies: FCS_COP.1 Cryptographic operation
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.4.1.2 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction method] that meets the following: [assignment: list of standards].

- [assignment: list of standards]:None
- [assignment: cryptographic key destruction method]:SHARP passport booklet module cryptographic key destruction algorithm

  <SHARP passport booklet module cryptographic key destruction algorithm>

  Method to destruct cryptographic key used in TOE, as shown below.

Method 1: The RAM area is initialized by overwriting it at the power up or reset.

Method 2: Session key validity flag in the RAM area is invalidated, when MUTUAL AUTHENTICATE command is executed, or when abnormality is detected during processing secured message.

Dependencies: FCS_CKM.1 Cryptographic key management

FMT_MSA.2 Secure security attributes

5.4.1.3 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

- Above assignment shown in the table below.

List of standards	Cryptographic algorithm	Mode of operation	Cryptographic key sizes	List of cryptographic operations	Subject of cryptographic operations
FIPS PUB46-3	Triple-DES	CBC with zero IV	112bit	Encryption	Communication data for the secured command after the session key is shared.
					Data in the response message during mutual authentication.
				Decryption	Secured communication data after the session key is shared.
					Command data during mutual authentication.

Dependencies: FCS_CKM.1 Cryptographic key management

5.4.1.4 FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1

FDP_ACC.2.1 The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.

- [assignment: access control SFP]: ePassPort policy
- [assignment: list of subjects]: All subjects
- [assignment: list of objects]:All objects

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Dependencies: FDP_ACF.1 Security attribute based access control

5.4.1.5 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the [assignment: access control SFP] to objects based on the following:[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

- [assignment: access control SFP]: ePassPort policy
- [assignment: list of subjects]:Administrator and end user
- [assignment: list of objects]: All objects
- [assignment: security attributes, named groups of security attributes]: the identity: administrator or end user

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

- [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]:

  Administrators authenticated by the Transport Key can:
  - Modify the Transport Key
  - Modify the End User Authentication Key
  - Write DG1, DG2, DG13, DG.SOD and DG.COM once
  - Read DG1, DG2, DG13, DG.SOD and DG.COM

  Administrators authenticated by the Reading Key can:
  - Read DG13

  Administrators authenticated through the CPLD Key can:
  - Read CPLD area
  - Write CPLD area (only if the write functionality has not been deleted, see FIA_AFL.1 in the User Policy)

  Authenticated end-users can:

  Read DG1, DG2, DG13, DG.SOD and DG.COM

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

- [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]:None

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

- [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]:None

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

5.4.1.6 FDP_ETC.1 Export of user data without security attributes

Hierarchical to: No other components.

FDP_ETC.1.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] when exporting user data, controlled under the SFP(s), outside of the TSC.

- [assignment: access control SFP(s) and/or information flow control SFP(s)]: ePassPort policy

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

Dependencies: FDP_ACC.1 Subset access control

5.4.1.7 FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other components.

FDP_ITC.1.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] when importing user data, controlled under the SFP, from outside of the TSC.

- [assignment: access control SFP and/or information flow control SFP]: ePassPort policy.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: additional importation control rules].

- [assignment: additional importation control rules]:None

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

5.4.1.8 FDP_SDI.1 Stored data integrity monitoring

Hierarchical to: No other components.

FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for [assignment: integrity errors] on all objects, based on the following attributes: [assignment: user data attributes].

- [assignment: integrity errors]:In case of physical failure occurrence
- [assignment: user data attributes]: All user data

Dependencies: No dependencies

5.4.1.9 FIA_AFL.1 Authentication failure handling [8]

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: positive integer number], "an administrator configurable positive integer within [assignment: range of acceptable values]"] unsuccessful authentication attempts occur related to [assignment: list of authentication events].

- [selection: [assignment: positive integer number], "an administrator configurable positive integer within [assignment: range of acceptable values]"]: refer to table below
- [assignment: list of authentication events]: refer to table below.

List of authentication events	Positive integer number
Authentication by the transport key	3
Authentication by Reading out key	3
CPLD key	∞
End-user Mutual Authentication key[9]	∞

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: list of actions].

- [assignment: list of actions]:

[8] Informative note: This blocking is used by the administrators to permanently block the administrator interface before issuing the TOE to its holder (transition to phase 7).

[9] The key used for Mutual Authentication by the end-user is included here for completeness only.

- disallow further authentication against that key.
- If authentication has been disallowed against both the transport key and the reading out key, the write functionality of the TOE shall be permanently deleted

Dependencies: FIA_UAU.1 Timing of authentication

5.4.1.10 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: list of security attributes].

- [assignment: list of security attributes]: administrator or end user identifier. The administrator is identified by use of the VERIFY command, and the end user is identified by use of the MUTUAL AUTHENTICATION command.

Dependencies: No dependencies

5.4.1.11 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

- [assignment: list of TSF mediated actions]:Execute ReadTestData, SELECT FILE, VERIFY, MUTUAL AUTHENTICATE and GET CHALLENGE command.

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.

Dependencies: FIA_UID.1 Timing of identification

5.4.1.12 FIA_UAU.5 Multiple authentication mechanisms10

Hierarchical to: No other components.

FIA_UAU.5.1 The TSF shall provide [assignment: list of multiple authentication mechanisms] to support user authentication.

- [assignment: list of multiple authentication mechanisms]: the VERIFY , MUTUAL AUTHENTICATION commands.

[10] Informative note: these two controls are provided to conform the ICAO and the Japanese Government (Passport booklet IC) requirements.

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

- [assignment: rules describing how the multiple authentication mechanisms provide authentication]: The administrator uses the VERIFY command as defined in ISO 7816 and the end user uses the MUTUAL AUTHENTICATION commands as defined in [ICAO].

Dependencies: No dependencies

5.4.1.13 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow [assignment: list of TSF-mediated actions] on behalf of the user to be performed before the user is identified.

- [assignment: list of TSF-mediated actions]:Execute ReadTestData, SELECT FILE, GET CHALLENGE, VERIFY and MUTUAL AUTHENTICATE commands.

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.

Dependencies: No dependencies

5.4.1.14 FIA_USB.1 User-subject binding

Hierarchical to: No other components.

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user:[assignment: list of user security attributes].

- [assignment: list of user security attributes]: Identity

Dependencies: FIA_ATD.1 User attribute definition

5.4.1.15 FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: determine the behaviour of, disable, enable, modify the behaviour of] the functions [assignment: list of functions] to [assignment: the authorized identified roles].

- [assignment: list of functions]:All TOE security functions
- [selection: determine the behaviour of, disable, enable, modify the behaviour of]: modify the behaviour of

- [assignment: the authorized identified roles]: Nobody.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

5.4.1.16 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorized identified roles].

- [assignment: list of security attributes]: Any
- [selection: change_default, query, modify, delete, [assignment: other operations]]:modify
- [assignment: access control SFP, information flow control SFP]: ePassPort policy.
- [assignment: the authorized identified role]:Nobody

Dependencies: FDP_ACC.1 Subset access control

FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

5.4.1.17 FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV_SPM.1 Informal TOE security policy model

FDP_ACC.1 Subset access control

FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

5.4.1.18 FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to provide [selection: choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.

- [selection: choose one of: restrictive, permissive, [assignment: other property]]: restrictive
- [assignment: access control SFP, information flow control SFP]: ePassPort policy.

FMT_MSA.3.2 The TSF shall allow the [assignment: the authorized identified roles] to specify alter-

native initial values to override the default values when an object or information is created.

- [assignment: the authorized identified roles]:Nobody.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

5.4.1.19 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorized identified roles].

- [assignment: list of TSF data]: 'Transport Key' and 'End user authentication key'.
- [selection: change_default, query, modify, delete, clear, [assignment: other operations]]:modify
- [assignment: the authorized identified roles]:Administrator

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

5.4.1.20 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: list of security management functions to be provided by the TSF].

- [assignment: list of security management functions to be provided by the TSF]: None

Dependencies: No dependencies

5.4.1.21 FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: the authorized identified roles].

- [assignment: the authorized identified roles]: All subjects

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.4.1.22 FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

FPT_PHP.3.1 The TSF shall resist [assignment: physical tampering scenarios] to the [assignment: list of TSF devices/elements] by responding automatically such that the TSP is not violated.

- [assignment: list of TSF devices/elements]:TSF
- [assignment: physical tampering scenarios]:physical manipulation and physical probing[11]

Dependencies: No dependencies

5.4.1.23 FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

5.4.1.24 FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

5.4.2 Minimum Strength of Function

The minimum function strength level of this TOE is a SOF-high. The functional requirements that use probabilistic or permutation mechanism are FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FIA_UAU.1 and FIA_UID.1, mentioned above. Among these functional requirements, functional requirements that relate to minimum function strength level are UAU.1 and FIA_UID.1. FCS_CKM.1, FCS_CKM.4 and FCS_COP.1 are the functional requirements that use cryptographic algorithm, therefore, they are not target of this strength of function requirement.

[11] This assignment is quoted from [EuroPP], Chapter 5

5.4.3 TOE Security Assurance Requirements

The evaluation assurance level of TOE is EAL4 augmented with AVA_VLA.4.

The table 5-1 shows list of TOE security assurance requirements.

Table 5-1: List of TOE Security Assurance Requirements

Assurance class	Assurance component ID	Assurance component introduction
Configuration management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security functional evaluation
	AVA_VLA.4	Highly resistant

5.5 Security Requirements for the IT Environment

There are no security requirement for the IT environment.

6 TOE Summary Specification

6.1 Security Functions[12]

SF.Sec_Messaging (Cryptographic operation by secure messaging)

The TOE protects the communication with end-users and controls access using secure messaging with Triple-DES cryptography according to [ICAO] specifications.

SF.Sec_Stat_Key (Data protection by cryptographic key)

The TOE performs authentication by SF.Mutual_Authand maintains the result of this authentication in the security status. This security status is used for access control.

Note: The TOE is constructed such that on start-up the maintained security statuses express that no successful authentication (by SF.Verify) has been performed.

SF.Sec_Stat_PIN (Data protection by personal identification number)

The TOE performs authentication by SF.Verify and maintains the result of authentication in the security status. This security status is used for access control.

Note: The TOE is constructed such that on start-up the maintained security statuses express that no successful authentication (by SF.Verify) has been performed.

SF.Access_Con (Access control)

The TOE permits access to the user data only when the present security status matches the access control conditions for the user data.

SF.Stores (security attributes of data)

The TOE stores security attributes for each ISO7816 DF and EF that stores user data or authentication data. SF.Stores allows access (read-only due to pre-loaded initial data, see below) to these security attributes. The TOE has pre-loaded initial data that determines its access control:

- The administrator is allowed to (after successful authentication using the Transport Key):
  - Modify his own Transport key.
  - Modify keys for mutual authentication.
  - Fill in passport data **once**.
  - Read passport data.
- The administrator is allowed to (after successful authentication using the Reading Out Key):
  - Read one specific part of the passport data: DG13.

[12] Refer to the table 8.3 'Security Function and corresponding Security Functional Requirements'.

- The administrator is allowed to (after successful authentication using the CPLD Key):
  - Read/Write[13] CPLD data.
- The administrator can lock (disabling further authentication attempts) the transport and reading out key by the repeated (3x) use of an invalid key.
- The end-user can (after successful authentication):
  - Read passport data.

SF.Construction (Security structure)

The TOE is securely constructed. This SF covers security functionality of the hardware platform that protects against tampering.

SF.Verify (Administrator identification and authentication)

The TOE identifies the administrator by use of the VERIFY command. The TOE authenticates the administrator by successful use of the VERIFY command. The number of consecutive failed authentication attempts is limited.

Note: SELECT FILE is used to be able to select the key against which authentication is to be performed.

SF.Mutual_Auth (Mutual authentication)

The TOE identifies the end-user by use of the MUTUAL AUTHENTICATE command. The TOE authenticates the end-user by successful use of the MUTUAL AUTHENTICATE command (according to [ICAO] specifications).

SF.Integrity_Check (Safety check)

The TOE functionality that allows for reading stored user data includes integrity checking of the data.

SF.Protection (no-bypass, self protection)

The TOE mediates all requests from the administrator and end-user, and maintains a security domain for itself protected from logical and physical tampering.

SF.Key_Destruction

The TOE invalidates cryptographic session keys in the following situations:

- When a subsequent MUTUAL AUTHENTICATE command is started by invalidating the session key validity flag.
- When an abnormality is detected during processing of a secured message by invalidating the ses-

[13] Once the TOE is in personalized mode CPLD data can only be read as in personalized mode all write functionality is no longer available.

sion key validity flag.

· On power-up by overwriting all RAM.

6.2 Strength of Security Functions

TOE security functions that are based on probabilistic or permutation mechanism are SF.Sec_Messaging, SF.Verify and SF.Mutual_Auth. SF.Verify and SF.Mutual_Auth in security functions have a strength level of SOF-high, and SF.Sec_Messaging is not the target of this strength of function level since it is the security function which uses cryptographic algorithm.

6.3 Assurance Measures

The table 6-1 shows security assurance requirements that correspond to assurance measures.

Table 6-1: Security Assurance Requirements corresponding to Assurance Measures

Assurance requirement class	Assurance requirement component	Assurance measures
Configuration management	ACM_AUT.1	· For source code and documents of application part of the TOE, developers have implemented automated configuration management system. · Developers set up the transport key and IC serial number to ensure secure delivery. · Developers have implemented access control policies and measures to assure development security. · Developers use well-known compiler tools for creation of TOE. · The life cycle of the TOE is defined in a lifecycle definition document.
	ACM_CAP.4	
	ACM_SCP.2	
Delivery and operation	ADO_DEL.2	
Life cycle support	ALC_DVS.1	
	ALC_LCD.1	
	ALC_TAT.1	
Delivery and operation	ADO_IGS.1	· Developer provides 'Module delivery management document for the passport booklet' to the customers describing how to securely injecting passport number and booklet number.

Assurance requirement class	Assurance requirement component	Assurance measures
Development	ADV_FSP.2	· Functional specification document for the passport booklet module describing external interface of the TOE.
	ADV_IMP.1	· Source code
	ADV_HLD.2	Design documents for the passport booklet module. These documents include the security correspondence.
	ADV_LLD.1	
	ADV_RCR.1	
	ADV_SPM.1	
Guidance documents	AGD_ADM.1	· Instruction manual for the passport booklet module provides instructions how to securely personalize the passports.
	AGD_USR.1	
Tests	ATE_COV.2	· Test manual for the passport booklet module · Test item analysis document for the passport booklet module · Test report for the passport booklet module · These documents describe all test method and actual testing done on the TOE.
	ATE_DPT.1	
	ATE_FUN.1	
	ATE_IND.2	· Test material for the passport booklet module
Vulnerability assessment	AVA_MSU.2	· Evaluation report for the passport booklet module The following evaluation results are included in the report. - Effects on miss-use analysis results - Security function strength - Vulnerability analysis results
	AVA_SOF.1	
	AVA_VLA.4	

7 PP Claims

This Security Target uses the following Protection Profile (PP):
"*Protection profile for IC for the passport booklet, version1.0, 24 September 2004, Ministry of Foreign Affairs - Consular Affairs Bureau - Passport Division / JBMIA e-MRP/WG3*". Regarding eavesdropping an additional objective for the environment is added in line with international developments regarding Machine Readable Travel Documents with „ICAO Application"[14].

The PP is not CC certified, but is the official requirements document of the Japanese government. This ST lite does not integrate the PP, however the official ST integrates the PP.

[14] These developments are for example compiled in Protection Profiles, see for a current version [ICAO2].

8 Rationale

8.1 Security Objectives Rationale

The following table 8-1 shows that the stated security objectives are traceable to all of the aspects identified in the security environments.

Table 8-1: Mapping between the TOE security environment and the Security objectives

	O.1 Identification authentication	O.2 ID Read out	O.3 Modification Prohibition	O.4 Mutual authentication	O.5 Secure messaging	O.6 Physical tampering	O.7 Transport key invalidation	O.8 High attack potential	OE.1 TOE Management	OE.2 Issuing environment	OE.3a, OE3b Secure delivery1, 2	OE.4 Anti-eavesdropping measures
T.1 Illegal read out	√											
T.2 Physical tampering						√						
T.3 Illegal modification			√									
P.1 ID read out		√										
P.2 Mutual authentication				√								
P.3 Secure messaging					√							
P.4 Transport key invalidation							√					
P.5 High attack potential								√				
A.1 TOE management									√			
A.2 Issuing environment										√		
A.3 Secure delivery											√	
A.4 Anti-eavesdropping measures												√

8.1.1 Threats and security objectives

The identified threats are covered by the security objectives as follows.

T.1 is covered by O.1. O.1 provides that only granted user can access user data so that data within the TOE is protected from illegal read out through the contactless interface of the TOE.

T.2 is covered by O.6. O.6 provides that the TOE can resist physical tampering so that data within the TOE or internal structure of the TOE can not be modified without using legitimate interface of the TOE.

T.3 is covered by O.3. O.3 prohibits modification of the stored data or additional writing of new data via legitimate interface of the TOE.

8.1.2 Organisational security policies and security objectives

The identified organisation security policies are covered by the security objectives as follows.

P.1 is covered by O.2. O.2 provides that the TOE maintains the IC serial number within the TOE and provides it when requested.

P.2, P.3, P.4, and P.5 are covered by O.4, O.5, O.7, and O.8 respectively. It is obvious that O.4, O.5, O.7, and O.8 meet corresponding organisational security policies.

8.1.3 Assumptions and security objectives

The identified assumptions are covered by the security objectives as follows.

A.1, A.2, A.3, and A.4 are covered by OE.1, OE.2, OE.3(a, b), and OE.4 respectively. It is obvious that OE.1, OE.2, OE.3(a, b), and OE.4 meet corresponding assumptions.

8.2 Security Requirements Rationale

8.2.1 Security objectives and security functional requirements

The following table 8-2 shows that all TOE security requirements are traceable to the security objectives.

Table 8-2: Mapping of the TOE Security Objectives and the TOE Security Functional Requirements

	FCS_CKM.1	FCS_CKM.4	FCS_COP.1	FDP_ACC.2	FDP_ACF.1	FDP_ETC.1	FDP_ITC.1	FDP_SDI.1	FIA_AFL.1	FIA_ATD.1	FIA_UAU.1	FIA_UAU.5	FIA_UID.1	FIA_USB.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FMT_PHP.3	FMT_RVM.1	FPR_SEP.1	EAL4+AVA_VLA.4
O.1 Identification /Authentication,Access Control				√	√	√	√		√	√	√	√	√	√		–		–	√	–	√		√	√	
O.2 ID read out				√	√	√		√																	
O.3 Modification Prohibition															√					–	–				
O.4 Mutual authentication			√				√										–	–							
O.5 Secure messaging	√	√	√														–								
O.6 Physical tampering																						√			
O.7 Transport key invalidation									√																
O.8 High attack potential																									√

In the table, "√" indicates the direct requirements which derive from the security objectives, and "–" indicates the indirect requirements which derive from mutual supportiveness.

O.1 is met by FDP_ACC.2, FDP_ACF.1, FDP_ETC.1, FDP_ITC.1, FDP_SDI.1, FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FAI_UAU.5, FIA_UID.1, FIA_USB.1, FMT_MTD.1, FMT_SMR.1, FPT_RVM.1, and FPT_SEP.1. FDP_ACC.1 and FDP_ACF.1 control access to the user data based on the access control rules to protect the user data. FPT_RVM.1 and FPT_SEP.1 protect the TSF itself from untrusted subjects. FDP_ETC.1 and FDP_ITC.1 export and import the user data from/to the TOE. FIA_UAU.1, FIA_USB.1 and FIA_UID.1, FIA_AFL.1, FIA_ATD.1 and FIA_UAU.5 provide conditions to identify and authenticate the legitimate users (administrator and end user). FMT_MTD.1, FMT_SMR.1, FMT_MSA.1, FMT_MSA.3, and FMT_SMF.1 provide administrative functions to maintain the TSF secure.

O.2 is met by FDP_ACC.2, FDP_ACF.1, FDP_ETC.1, and FDP_SDI.1. FDP_SDI.1 assures integrity of the IC serial number. FDP_ACC.2, FDP_ACF.1, and FDP_ETC.1 control access to the IC serial number when it is exported.

O.3 is met by FMT_MOF.1, FMT_SMF.1, and FMT_SMR.1. Only granted user can manage the security functions of the TOE.

O.4 is met by FCS_COP.1 and FDP_ITC.1. FDP_ITC.1 imports a key from the external device securely. FCS_COP.1 requires cryptographic processing for mutual authentication. Also, FMT_MSA.2 and FMT_MSA.3 assure that security attributes are introduced securely.

O.5 is met by FCS_CKM.1, FCS_CKM.4, and FCS_COP.1. FCS_CKM.1 provides generation of keys for secure messaging. FCS_CKM.4 provides secure destruction means for the cryptographic keys. FCS_COP.1 provides cryptographic operation of secure messaging. Moreover, FMT_MSA.2 assures that security attribute is secure, and supports the functional requirements above.

O.6 is met by FPT_PHP.3. It provides the requirements to resist physical tempering of the hardware.

O.7 is met by FIA_AFL.1. It provides the behaviour of the authentication function on authentication failure.

O.8 is met by security assurance requirement of EAL4 augmented (+AVA_VLA.4). AVA_VLA.4 requires that the TOE can resist an attacker possessing high attack potential.

8.2.2 Security objectives and security assurance requirements

The procurement office of passport booklet requires that the TOE can resist attackers possessing high attack potential, because it is likely that the TOE becomes a target of various illegalities. Then, EAL4 augmented (+AVA_VLA.4) is appropriate.

8.2.3 Dependencies and mutual Support

Dependencies for the security functional requirements and the assurance requirements are satisfied as follows.

Dependencies for augmented security assurance requirement AVA_VLA.4 are satisfied because ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, and AGD_USR.1 are all included in the package of ELA4.

Dependencies for the security functional requirements are shown in the following table. "H(#)" of the right hand column shows that the dependency is satisfied by a component being hierarchical to. "EAL4" shows that the dependency is satisfied, because it is contained in EAL4.

Table 8-3: Dependencies of the security function requirements

#	Security Functional Requirements	Dependencies	# which copes
1	FCS_CKM.1: Cryptographic key management	FCS_COP.1, FCS_CKM.4, FMT_MSA.2	3 2 17
2	FCS_CKM.4: Cryptographic key destruction	FCS_ITC.1, FCS_CKM.1, FMT_MSA.2	7 1 17
3	FCS_COP.1: Cryptographic operation	FCS_ITC.1, FCS_CKM.1	7 1
4	FDP_ACC.2 Complete access control	FDP_ACF.1	5
5	FDP_ACF.1: Security attribute based access control	FDP_ACC.1, FMT_MSA.3	H (4) 18
6	FDP_ETC.1: Export of user data without security attributes	FDP_ACC.1	H (4)
7	FDP_ITC.1: Import of user data without security attributes	FDP_ACC.1, FMT_MSA.3	H (4) 18
8	FDP_SDI.1: Stored data integrity monitoring	No dependencies	-
9	FIA_AFL.1: Authentication failure handling	FIA_UAU.1	11
10	FIA_ATD.1: User attribute definition	No dependencies	-
11	FIA_UAU.1: Timing of authentication	FIA_UID.1	13
12	FIA_UAU.5: Multiple authentication mechanisms	No dependencies	-
13	FIA_UID.1: Timing of identification	No dependencies	-
14	FIA_USB.1: User-subject binding	FIA_ATD.1	10
15	FMT_MOF.1: Management of security functions behaviour	FMT_SMF.1, FMT_SMR.1	20 21
16	FMT_MSA.1: Management of security attributes	FDP_ACC.1, FMT_SMF.1, FMT_SMR.1	H (4) 20 21
17	FMT_MSA.2: Secure security attributes	ADV_SPM.1, FDP_ACC.1, FMT_MSA.1, FMT_SMR.1	EAL4 H (4) 16 21
18	FMT_MSA.3: Static attribute initialization	FMT_MSA.1,	16

#	Security Functional Requirements	Dependencies	# which copes
		FMT_SMR.1	21
19	FMT_MTD.1: Management of TSF data	FMT_SMF.1, FMT_SMR.1	20 21
20	FMT_SMF.1: Specification of Management Functions	No dependencies	-
21	FMT_SMR.1: Security roles	FIA_UID.1	13
22	FPT_PHP.3: Resistance to physical attack	No dependencies	-
23	FPT_RVM.1: Non-bypassability of the TSP	No dependencies	-
24	FPT_SEP.1: TSF domain separation	No dependencies	-

All dependencies are satisfied as shown in the table 8-3.

Each security objective is met by the security requirements as shown in 8.2.1. There is no conflict between security requirements corresponding with each security objective. O.1 is also addressed by FPT_RVM.1 and FPT_SEP.1, which make up mutual supportiveness.

8.2.4 Minimum strength of function

The TOE is required to resist an attacker possessing high attack potential. Therefore, the minimum function strength of SOF-high is appropriate.

8.3 TOE Summary Specification Rationale

8.3.1 Security Functions Rationale

Security functions and corresponding security functional requirements are shown in table 8-4, and rationale that fulfils this is shown in table 8-5 as sufficiency of security functional requirements by security functions.

Table 8-4: Security Functions and corresponding Security Functional Requirements

	SF.Sec_Messaging	SF.Sec_Stat_Key	SF.Sec_Stat_PIN	SF.Access_Con	SF.Stores	SF.Construction	SF.Verify	SF.Mutual_Auth	SF.Integrity_Check	SF.Protection	SF.Key_Desctruction
FCS_CKM.1.1								√			
FCS_CKM.4.1											√
FCS_COP.1.1	√										
FDP_ACC.2.1		√	√	√	√		√	√			
FDP_ACC.2.2		√	√	√	√		√	√			
FDP_ACF.1.1		√	√	√	√		√	√			
FDP_ACF.1.2				√	√						
FDP_ACF.1.3		√	√	√	√						
FDP_ACF.1.4		√	√	√	√						
FDP_ETC.1.1				√	√						
FDP_ETC.1.2				√	√						
FDP_ITC.1.1				√	√						
FDP_ITC.1.2				√	√						
FDP_ITC.1.3				√	√						

	SF.Sec_Messaging	SF.Sec_Stat_Key	SF.Sec_Stat_PIN	SF.Access_Con	SF.Stores	SF.Construction	SF.Verify	SF.Mutual_Auth	SF.Integrity_Check	SF.Protection	SF.Key_Desctruction
FDP_SDI.1.1									√		
FIA_AFL.1.1							√				
FIA_AFL.1.2				√	√						
FIA_ATD.1.1							√	√			
FIA_UAU.1.1							√	√			
FIA_UAU.1.2				√	√						
FIA_UAU.5.1							√	√			
FIA_UAU.5.2							√	√			
FIA_UID.1.1							√	√			
FIA_UID.1.2				√	√						
FIA_USB.1.1		√	√				√	√			
FMT_MOF.1.1				√	√	√					
FMT_MSA.1.1				√	√						
FMT_MSA.2.1				√	√						
FMT_MSA.3.1				√	√						
FMT_MSA.3.2				√	√						
FMT_MTD.1.1			√	√	√						
FMT_SMF.1.1				√	√						
FMT_SMR.1.1		√	√	√	√		√	√			
FMT_SMR.1.2		√	√	√	√		√	√			

	SF.Sec_Messaging	SF.Sec_Stat_Key	SF.Sec_Stat_PIN	SF.Access_Con	SF.Stores	SF.Construction	SF.Verify	SF.Mutual_Auth	SF.Integrity_Check	SF.Protection	SF.Key_Destruction
FPT_PHP.3.1						√				√	
FPT_RVM.1.1				√	√					√	
FPT_SEP.1.1										√	
FPT_SEP.1.2										√	

Table 8-5: Sufficiency of Security Functional Requirements by Security Functions.

Security Functional Requirements	Sufficiency
FCS_CKM.1.1	SF.Mutual_Auth: As shown in the [ICAO] specification: The TOE uses the GET CHALLENGE and MUTUAL AUTHENTICATION commands to generate 112 bit cryptographic (session) keys. Generation of these session keys includes verification of a cryptographic key value stored in the TOE. Successful verification corresponds with end-user authentication.
FCS_CKM.4.1	SF.Key_Destruction One-two-one mapping to SF
FCS_COP.1.1	SF.Sec_Messaging: As shown in the [ICAO] specification: The TOE uses Triple-DES (Mode: CBC with zero Initialization Vector) to encrypt / decrypt secured messages

Security Functional Requirements	Sufficiency
FDP_ACC.2.1 FDP_ACC.2.2	SF.Verify, SF.Mutual_Auth, SF.Sec_Stat_Key, SF.Sec_Stat_PIN, SF.Access_Con, SF.Stores: SF.Verify and SF.Mutual_Auth identify and authenticate the administrator and end-user respectively. SF.Sec_Stat_Key and SF.Sec_Stat_PIN maintain result of these authentications. SF.Access_con compares the maintained authentication status with the security attributes associated with the data according to SF.Stores.
FDP_ACF.1.1	SF.Verify, SF.Mutual_Auth, SF.Sec_Stat_Key, SF.Sec_Stat_PIN, SF.Access_Con, SF.Stores: SF.Verify and SF.Mutual_Auth identify and authenticate the administrator and end-user respectively. SF.Sec_Stat_Key and SF.Sec_Stat_PIN maintain result of this authentication. SF.Access_con compares the maintained authentication status with the security attributes associated with the data according to SF.Stores.
FDP_ACF.1.2	SF.Access_Con, SF.Stores: SF.Access_con compares the maintained authentication status (see above for FDP_ACF.1.1) with the security attributes associated with the data according to SF.Stores.
FDP_ACF.1.3	SF.Sec_Stat_Key, SF.Sec_Stat_PIN, SF.Access_Con, SF.Stores: TOE is not equipped with the rule to authorize the access of the subject for object other than required by FDP_ACF.1.1.
FDP_ACF.1.4	SF.Sec_Stat_Key, SF.Sec_Stat_PIN, SF.Access_Con, SF.Stores: TOE is not equipped with the rule to deny the access of the subject for object other than required by FDP_ACF.1.1.
FDP_ETC.1.1 FDP_ETC.1.2	SF.Access_Con, SF.Stores: The security attributes do not allow export of security attributes by any user.
FDP_ITC.1.1 FDP_ITC.1.2	SF.Access_Con, SF.Stores: The security attributes do not allow changing/setting security attributes by any user. Therefore security attributes cannot be imported at all.
FDP_ITC.1.3	SF.Access_Con, SF.Stores: The TOE is not equipped with any security attribute related rules other than required by FDP_ITC.1.1
FDP_SDI.1.1	SF.Integrity_Check: The TOE provides the function to detect changes to the stored user data by an integrity check function.
FIA_AFL.1.1	SF.Verify: The TOE limits the number of consecutive failed authentication attempts.

Security Functional Requirements	Sufficiency
FIA_AFL.1.2	SF.Access_Con, SF.Stores The TOE denies further authentication attempts after the key has been locked. Locking a key occurs after 3 failed attempts.
FIA_ATD.1.1	SF.Verify, SF.Mutual_Auth: The TOE maintains the security status that corresponds with the last authentication attempt of the administrator and the end-user.
FIA_UAU.1.1 FIA_UID.1.1	SF.Verify, SF.Mutual_Auth: To authenticate the administrator the VERIFY command is used. To authenticate the end-user MUTUAL AUTHENTICATE and GET CHALLENGE is used. To be able to select the key against which authentication (by the VERIFY command) is performed SELECT FILE can be used.
FIA_UAU.1.2 FIA_UID.1.2	SF.Stores, SF.Access_Con,: SF.Stores and SF.AccessCon show that access to user data is allowed after successful authentication only
FIA_UAU.5.1 FIA_UAU.5.2	SF.Verify, SF.Mutual_Auth: The TOE provides the following authentication methods: - For the administrator: The VERIFY command as specified in ISO7816.. - For the end-user: The GET CHALLENGE and MUTUAL AUTENTICATE commands as specified in the [ICAO] specification.
FIA_USB.1.1	SF.Access_Con SF.Access_Con permits access only if the user data associated access control attributes match with those of the user.
FMT_MOF.1.1 FMT_SMF.1.1	SF.Construction, SF.Access_Con, SF.Stores: Physically: The TOE forbids modification against all TOE security functions. Logically: SF.Access_Con and SF.Stores do not allow any user to change any security attribute.
FMT_MSA.1.1 FMT_MSA.2.1 FMT_MSA.3.1 FMT_MSA.3.2	SF.Access_Con, SF.Stores The TOE does not accept setting any security attributes at all

Security Functional Requirements	Sufficiency
FMT_SMR.1.1 FMT_SMR.1.2	SF.Verify, SF.Sec_Stat_PIN, SF.Mutual_Auth and SF.Sec_Stat_Key, SF.Access_Con, SF.Stores SF.Verify, SF.Sec_Stat_PIN authenticate the administrator user and maintain this status. SF.Mutual_Auth and SF.Sec_Stat_Key authenticate the end-user and maintain this status. SF.Access_Con and SF.Stores permit access only if the user data associated access control attributes match with those of the user.
FMT_MTD.1.1	SF.Access_Con, SF.Stores: The administrator is allowed to change the Transport Key and the keys used for mutual authentication.
FPT_PHP.3.1	SF.Protection, SF.Construction The TOE hardware protects against physical tampering.
FPT_RVM.1.1	SF.Access_Con, SF.Protection, SF.Stores: The TOE hardware ensures that it is not possible to access or change the stored data without going through the software. The TOE hardware always starts the TOE software (APE part). The TOE software (APE part) always executes the electronic passport application at start-up. The TOE software (application part) always checks security attribute associated with user data, during user data reading and writing.
FPT_SEP.1.1	SF.Protection: The TOE software realizes the function to prevent installing other application on the TOE, or delete or tamper passport booklet application. The TOE hardware protects against physical tampering.
FPT_SEP.1.2	SF.Protection: The TOE maintains separate security domains for the subjects (end-user and the administrator) as it allows at most one security domain to be active at a time.

Note: In some cases the leftmost column contains more than one SFR. This should be interpreted as that the sufficiency text in the right column applies to each SFR individually (and not combined). For proper understanding however the sufficiency text might include text that does not apply to every SFR.

8.3.2 Security Functions Strength Rationale

TOE security functions that are based on probabilistic or permutation mechanism are SF.Sec_Messaging, SF.Verify and SF.Mutual_ Auth. Among these, SF.Sec_Messaging is not the target of this function strength level, since it is the security function which use cryptographic algorithm. As mentioned in section 6.2, other security strength specifies "SOF-high". This satisfies the minimum function strength level "SOF-high" specified in section 8.2.4.

8.3.3 Assurance Measures Rationale

Security assurance requirements that the TOE assures is AVA_VLA.4 added to EAL4. Refer to the table 6-1. By that table, it is shown that the assurance measures meet all security assurance.

Developers have good experience on development of this type product, good coding practices, development security measurement and commensurate EAL4+ under the secure development environment.

8.3.4 The requirements are internally consistent

The requirements handle the subjects, objects and operations consistently as the same access control policy applies for all subjects, objects and operations.

8.3.5 The requirements are mutually supportive

The requirements handle the subjects, objects and operations mutually supportively.