Xaica-alphaPLUS
ePassport Configuration
(BAC+AA)

Security Target Lite

Ver.1.4

Public ver.1.0

2 Oct, 2012

Revised by NTT DATA CORPORATION

Revision History

Date	Public Version	Change	Description of Change
2/10/2012	1.0	Newly created	

Table of Contents

1. ST introduction

This chapter describes ST reference, TOE reference and TOE overview.

1.1. ST reference

Title; Xaica-alphaPLUS ePassport configuration(BAC+AA) Security Target Lite
Version number: 1.4
Public version number: 1.0
Date of Issue: October 2, 2012
Sponsor: NTT DATA CORPORATION
Author: NTT DATA CORPORATION

1.2. TOE reference

TOE Name: Xaica-alpha PLUS ePassport configuration
TOE version: 0111(PQQ)
SPI version: SPI-001-01
Key Word: Smart Card, IC card, Smart card,e-Passport,e-passport
Developer: NTT DATA CORPORATION

1.3. TOE overview

This section defines the type of the Target of Evaluation (TOE) and describes its main security features and intended usages.

1.3.1. TOE Type

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

The TOE(ePassport IC) comprises:
1. IC chip hardware with the contactless communication interface, and basic software (operating system) and ePassport application program that are embedded on the identified hardware.
2. TOE guidance delivered to the User of the product.

1.3.2. TOE architecture

The diagram in Figure 1-1 shows the Extended TOE (native OS with separation mechanism and, potentially, with applicative behavior) in the framework of a Smart Secure Device composed of three layers: [PP-ESforSSD]

- The Security IC layer provides low-level security mechanisms and resources to upper layers, including CPU, memories, communication interfaces, Random Number Generator, sensors;
- The Native OS layer manages the IC resources, monitors IC detectors, implements cryptographic operation, boot at power-up, executin environment, memory management, I/O management, life cycle management, key management, random numbers, atomic operations, separation mechanism, provides security services to the Application Layer, and provides functionality to the product end users through the applicative behavior.
- The Application Layer uses native OS to access resources and services and implements specific functionalities provided to the end users.

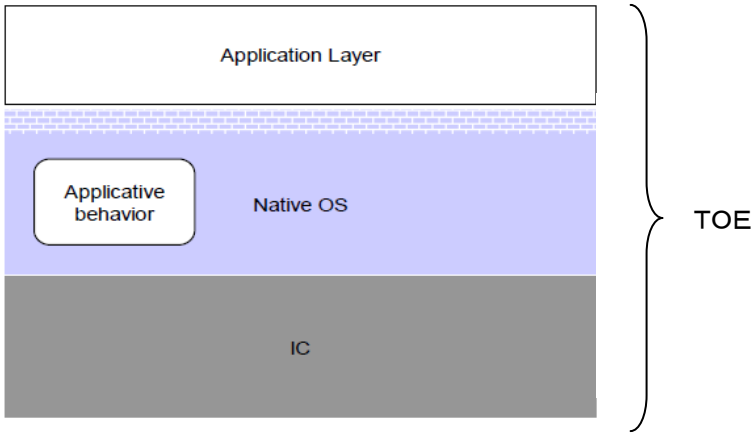


Figure 1-1: TOE Architecture

1.3.3. TOE Usage

A passport is an identification document, issued by government or public organization, whichcertifies, for the purpose of international travel, the identity of its holder, generally in a booklet (passport-booklet form). The International Civil Aviation Organization (ICAO) of the UnitedNations has provided the Passport Booklet Guidelines. For conventional passports, all information necessary as the certificate of identity was printed on a paper booklet, and thereby this could cause these passports to be forged for illicit purposes. In order to prevent forgery, an IC chip containing personal information with digital signature has been incorporated in a passport booklet. Since valid digital signature can be granted only by the passport issuing authority, a high level of forgery prevention effect can be achieved. However, digital signature is not enough to counter forgery by reproducing personal information with authorized signature to store such information on a different IC chip. This type of forgery attack can be countered by adding the active authentication function to the IC chip and verifying the authenticity of the IC chip with the use of the said function.

The TOE is embedded in the plastic sheet and then interfiled in the passport booklet. At immigration, the immigration official inspects the passport booklet using a passport inspection terminal (hereinafter referred to as the "terminal"). Information printed on the passport booklet in ordinary characters are encoded in the same contents, printed in the machine readable zone (MRZ) of the passport booklet, and read by the optical character reader of the terminal. In addition, the information is digitized1 and stored on the IC chip, i.e., the TOE. These digitalized data are read from the terminal through the contactless communication interface of the TOE. The digitalized data include facial images.

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

1.3.4. TOE Security Features

The main security functions of the TOE are designed to protect data stored in the TOE from illicit reading or writing. The operation of the security functions applying to contactless communication with the terminal shall comply with the Basic Access Control and Active Authentication Standards defined by the [ICAO Doc].

Attacks against protection data in the TOE include those through the contactless communication interface of the TOE and those attempting to disclose internal confidential information (Active Authentication Private Key) through a physical attack against the TOE. Attacks against the Active Authentication Private Key are assumed to be those performed by an attacker having a high attack potential.

The TOE provides the main security functions as follows.

・Basic Access Control

TOE provides Basic Access Control including Mutual authentication and secure messaging. Basic Access Control complies with [ICAO Doc].

・Active authentication support function.

TOE provides active authentication making the terminal authenticate the TOE. Active authentication complies with [ICAO Doc].

・Write inhibit function

TOE provides the function of inhibition of writing data after issuing a passport.

・Protection function in transport (Protection against attacks during transport before issuing the TOE)

TOE provides the function of protection against illicit issued stolen IC sheets during transport before issuing the TOE. To prevent illicit use during transport from shipping to delivery, the passport issuing authority configures the transport key which is decrypted by only the passport issuing authority.

・Tamper resistance

TOE provides the function of protection against confidential information leakage due to physical attacks.

1.3.5. TOE Life Cycle

It is described in terms of four life cycle phases.

- Phase 1 (Development): Development of IC chip hardware, basic software (operating system) and application software
- Phase 2 (Manufacturing): Manufacturing of the IC chip (with software installed), embedding it with antenna in the plastic sheet and Production of a passport booklet
- Phase 3 (Personalization): Writing of personal data
- Phase 4 (Operational Use): Use of the TOE by the passport holder in operational environment

Figure: 1-4 shows the workflow of the phases.

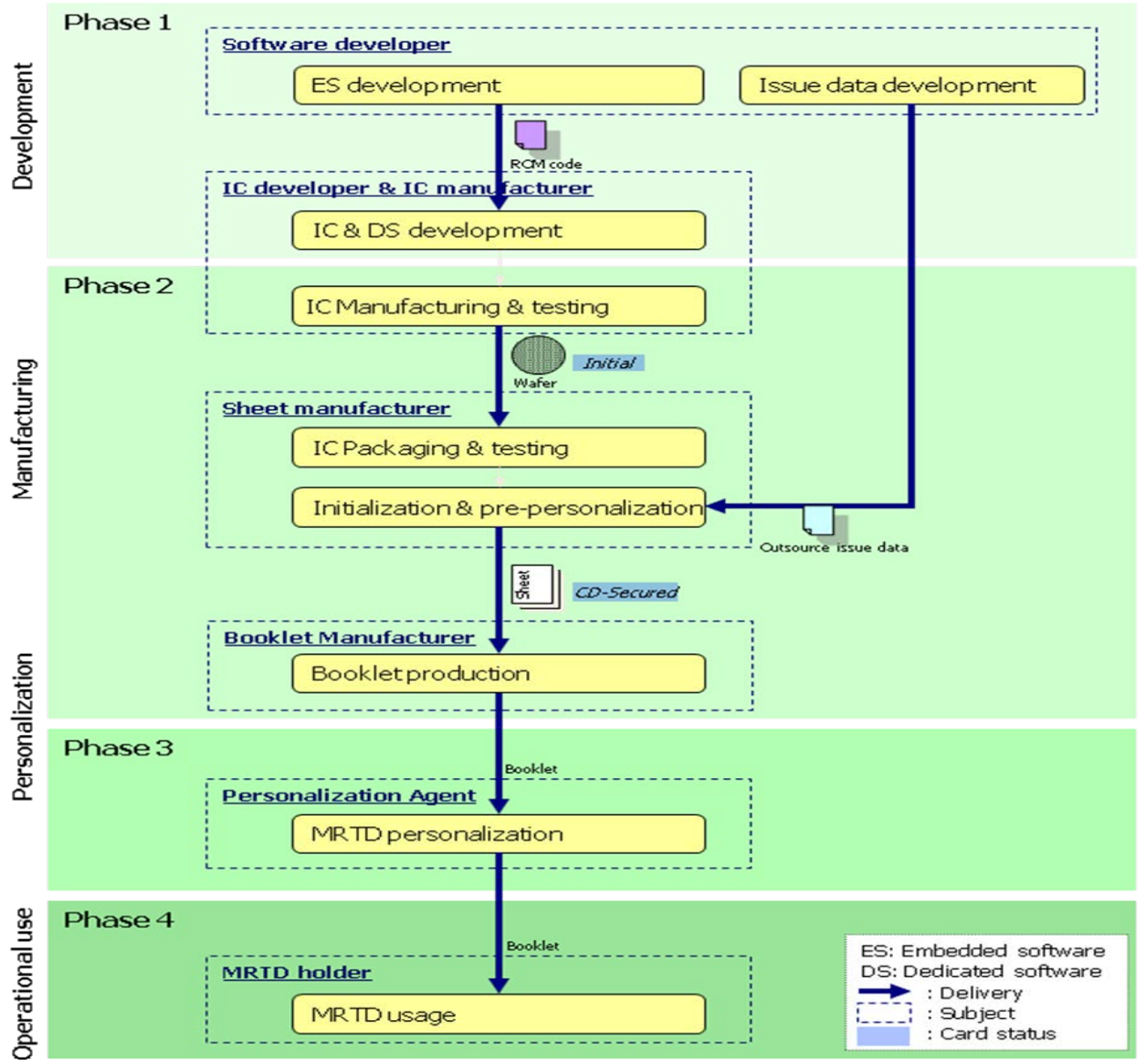


Figure: 1-2 Workflow

Table: 1-1 shows the assignment of term.

Table: 1-1 terms

Term	Assignment
IC developer	STMicroelectronics
Software developer	NTT DATA
IC manufacturer	STMicroelectronics
IC Embedded Software	YR80

Phase 1 "Development"

Phase 1 is a development phase.

In phase 1, STMicroelectronics developes the IC chip hardware, NTTDATA developes basic software (operating system) and application software.

Next, security of phase 1 is described.

In phase 1, threats to the operational environment are not considered, but proper development security shall be maintained to protect the confidentiality and integrity of data developed.
Where the TOE configuration items are developed across a number of sites, secure development environment is required for all configuration items.
Security related to the TOE in the development phase is evaluated as the development security for assurance requirements. The TOE security functions are still not validly operational in the development phase.

NTTDATA maintains secure development environment at the same level as that of ALC_DVS.2 by countermeasures including compliance with a regulation and vulnerability analysis (entering and leaving management, proof reading management and server duplexing etc.) to protect the confidentiality and integrity.

Similarly, STMicroelectronics maintains secure development environment according to ALC_DVS.2.

In phase 1, the follows is performed.

NTTDATA developes basic software (operating system) and application software, STMicroelectronics developes the IC chip hardware. NTTDATA designs and produces the issue data for the Initialization and the pre-personalization in manufacturing sites. The initialization data and the pre-personalization data are encrypted with **Outsource** mechanism.

Phase 2 "Manufacturing"

Phase 2 is a manufacturing phase.

In phase 2, STMicroelectronics produces the IC chip, sheet manufacturer produces IC sheet and Booklet manufacturer

produces passport booklet.

Next, security of phase2 is described.

In this phase, threats to the operational environment are not considered, but proper development security shall be maintained to protect the confidentiality and integrity of the configuration items of the IC chip.

STMicroelectronics maintains secure manufacturing environment according to ALC_DVS.2 by counter measures to protect the confidentiality and integrity.

Sheet manufacturer maintains secure manufacturing environment according to ALC_DVS.2 by issuing Issue data produced by NTTDATA with outsource mechanism to protect the confidentiality and integrity.

Manufacturing environment of booklet manufacturer is secure environment and put under the control of the passport issuing authorities, no explicit attack against the TOE is assumed.

But, as the organizational security policy, security functionality that allows only an individual having authority to process the TOE is required for the TOE. Therefore, all other authenticated user (persons who succeeded in transport key, readout key, and active authentication information access key PIN verification) can't access to the internal TOE data by access control.

To prevent illicit issued stolen IC sheets during transport from manufacturer to the passport issuing authorities, TOE is protected by active authentication information access key and transport key.

In phase 2, the follows is performed.

At first STMicroelectronics produces IC chip, next sheet manufacturer embeds basic software (operating system) and application software, finally The TOE inlay is manufactured.

A file object necessary for an ePassport is created in the TOE and an IC chip identification serial number is written in the file object. The functional tests for the internal circuit of IC chip are conducted before the IC chip is sealed. After that, only the contactless communication interface becomes available as an external interface.

The manufactured IC chip is embedded in the plastic sheet together with the contactless communication antenna and the transport key, readout key, and active authentication information access key are configured.

The TOE is interfiled in the ePassport booklet and The Passport number, Booklet management number and active authentication keys are configured by booklet manufacture.

After this information is configured, the TOE is delivered to the personalization agent.

Phase 3 "Personalization"

Phase3 is Persnalization phase under the control of the passport issuing authorities.

In phase 3, personalization agent personalizes the TOE.

Next, security of phase3 is described

This phase is put under the control of the passport issuing authorities, no explicit attack against the TOE is expected there.
But, as the organizational security policy, security functionality that allows only an individual having authority to process the TOE is required for the TOE. Therefore, all other authenticated user (persons who succeeded in transport key and readout key PIN verification) can't access to the internal TOE data by access control.

In phase 3, the follows is performed.

Information necessary for e-passport includes the personal information of the passport holder (e.g.name, information on birth and so on) and cryptographic key used by the security function is written in the TOE.

After the completion of personalization of all information, the e-passport is issued to the holder thereof.

Phase 4 "Operational Use"

Phase 4 is a phase subsequent to the handover of passport booklet to the final user, i.e., the holder thereof.

In phase4, the passport booklet is carried along with the holder thereof and used as a means to certify the identity of the holder in various situations, including immigration procedures.

Next, security of phase 4 is described.

In phase 4, no information stored in the TOE is altered or deleted. Information necessary for immigration procedures is protected against illicit reading by the TOE security function, except in the case where the information is read by the authorized terminal.

Passive authentication using Digital signature for ePassport data protects against tampering of ePassport data.
Under the circumstances, performing active authentication protects against copying ePassport data to other ePassport. The private key for active authentication is only used for the internal processing of the TOE and will never be readout to anywhere other than TOE. The information assets in the TOE are protected against external unauthorized access by the TOE security function.

2. TOE conformance claim

In this chapter, CC conformance claim, PP claim and Package claim and their rationales are described.

2.1. CC conformance claim

This ST conforms to the standards including:

- Common Criteria for Information Technology Security Evaluation Version 3.1, Part 1: Introduction and general model Revision 3 (CCMB-2009-07-001);
- Common Criteria for Information Technology Security Evaluation Version 3.1, Part 2: Introduction and general model Revision 3 (CCMB-2009-07-002);
- Common Criteria for Information Technology Security Evaluation Version 3.1, Part 3: Introduction and general model Revision 3 (CCMB-2009-07-003);
- CC Part 2 extended;
- CC Part 3;
- Composite product evaluation for Smart Cards and similar devices, September 2007, Version 1.0 Revision 1 (CCDB-2007-09-001).

2.2. PP claim

This ST refers to [PP-AA] as presented below.

- Protection Profile for Passport Booklet IC with Active Authentication,Version 1.00 February 15, 2010

2.3. Package claim

The assurance level for the evaluation of this ST is EAL4+ augmented with ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2 and ATE_DPT.3 components.

3. Security problem definition

In this chapter, users, assets, threats, organizational security policies and assumptions are set out.

3.1. Users

The users are The entities that interact with the product through the physical or logical external interfaces of the TOE.

Table 3-1: definition of User

Users	Definition
Booklet Manufacture	Manufacturing booklet
Personalization Agent	Personalizing
Passport reading person	Reading ePassport
Passport holder	Holding ePassport

Application note: For the TOE, Subjects are defined as follows.

Table 3-2: definition of Subject

Subjects	*Definition*
Issuing Authority Process	*Process on behalf of Issuing Authority Process*
Terminal Process	*Process on behalf of Terminal*

The Table 3-3 shows the correlation between the Subject and User.

Table 3-3: Relationship between Subject and User

Subject	*User*
Issuing Authority Process	*Booklet Manufacture, Personalization Agent*
Terminal Process	*Passport reading person*

3.2. Assets

The assets in the TOE include the personal information of the passport holder (e.g. name, information on birth and so on), management data and cryptographic key used by the security function.

Attacks against the Active Authentication Private Key in cryptographic key are assumed to be those performed by an attacker having a high attack potential. The Active Authentication Private Key are protected against external unauthorized access by the TOE security function.

Application note: For the TOE, Assets of AP layer are defined as follows.

Table 3-4: Assets of AP layer

Assets	*Protection level*
Active Authentication private key	*AVA_VAN.3*
Readout key	
Transport key	
Active Authentication information access key	
Basic access control cryptographic key	
Authenticator generation key	
MRZ data	
Facial image	
IC chip serial number	
Management data	
Active Authentication public key	
Common information on basic coding rules	
Security data related to passive authentication	

3.3. Threats

This section describes threats to be countered by the TOE. These threats shall be countered by the TOE or its operational environment independently or in combination with them.

T.Copy

An attacker trying to forge the ePassport may forge the ePassport by reading personal information with digital signature from the TOE and writing the reproduced data in an IC chip having the same functionality as that of the TOE. This attack results in damage to credit for the whole Passport Booklet including the TOE.

Application Note: Where information retrieved from the authorized TOE is reproduced in an illicit IC chip, information stored in the TOE will be reproduced together with the digital signature, forgery protection by means of digital signature verification become disable. 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 discriminating the facial image.

T.Logical_Attack

In the operational environment after TOE embedded Passport Booklet is issued, an attacker being in a situation to read the MRZ data of the Passport Booklet may try to read confidential information (active authentication private key) stored in the TOE through the contactless communication interface of the TOE.

Application Note: Where an attacker has physical access to the Passport Booklet, the attacker will be able to visually read personal information printed on the Passport Booklet or optically read the printed MRZ data. Since the security functions of the TOE cannot prevent reading such data, the information and data stated above are not included in the threat-related assets to be protected by the TOE. In other words, the purpose of this threat 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 by the use of data that the attacker has read from the MRZ.

T.Physical_Attack

In the operational environment after TOE embedded Passport Booklet is issued, an attacker may try to disclose confidential information (active authentication private key) stored in the TOE by physical means. This physical means includes both of nondestructive attacks made without impairing the TOE functions and destructive attacks made by destructing part of the TOE to have mechanical access to the inside of the TOE.

Application Note: An attack made by an attacker trying to read confidential information (active authentication private key) stored in the TOE through physical access to the TOE. Making such a physical attack will disable the security function operated according to the TOE program to demonstrate the original performance thereof, resulting in potential violation of SFR. The example of nondestructive attacks shows those measurements of leakage electromagnetic wave associated with the TOE operation and inducing malfunctions of security functions by applying environmental stress (e.g. changes in temperature or clock, or application of high-energy electric and magnetic 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 could be used to make the said attacks. The TOE having got attacked may not be reused as a ePassport IC. Even in such case, however, the disclosed private key may be abused to forge the TOE.

3.4. Organizational security policies

This section describes organizational security policies that apply to the TOE or operational environment. This PP includes conformance to the standards provided by ICAO and conditions required by the passport issuing authorities in Japan in the organizational security policies.

P.BAC

In the operational environment after TOE embedded Passport Booklet is issued, the TOE allows the terminal to read the given information from the TOE in accordance with the basic access control procedure defined by ICAO Doc 9303 Part 1. This basic access control procedure includes mutual authentication between the TOE and the terminals and secure messaging between the same. TOE files to be read are EF.DG1, EF.DG2, EF.DG13, EF.DG15, EF.COM, and EF.SOD under the rules stated above. For any files that are not listed in this PP out of those stated above under the same rules, the handling thereof is not defined. Any users other than the TOE are unable to have access to the basic access key file and the private key file that have stored internal TOE data.

Application Note: To meet global interoperability necessary for ePassport, the basic access control (BAC) procedure should be addressed. The mutual authentication function and the secure messaging function included in the BAC procedure are not intended to counter a high level of attacks, but have certain effect in preventing access to the internal TOE data through illicit devices. Accurately implementing the BAC procedure makes it possible to prevent a

skimming attack (acquisition of part of passport-specific information without opening the ePassport) and eavesdropping attack (acquisition of information contained in data by capturing communication data with terminals). The BAC procedure is regarded as a possible means to counter the reinforced basic attack capability. This PP has been prepared on the assumption of a high level of attack capability on the active authentication private key. However, the skimming attack and the eavesdropping attack countered by the BAC procedure do not fall under the category of such a high level of attack capability.

P.Authority

The TOE under the control of the passport issuing authorities allows only authorized users (persons who succeeded in readout key, transport key, or active authentication information access key verification) to have access to the internal TOE data, as shown in Table 3-1.

Table 3-4: Internal TOE data access management by passport issuing authorities

Authentication status*1	File subject to access control	Operation permitted	Reference: Data subject to operation
Successful verification with readout key	EF.DG13*2	Read	IC chip serial number (entered by manufacturer)
	EF.DG15		Active authentication public key
Successful verification with transport key	Transport key file	Write	Transport key data (update of old data)
	Basic access key file		Basic access control cryptographic key Authenticator generation key
	EF.DG1*3		MRZ data
	EF.DG2*3		Facial image
	EF.DG13*2/*3		Management data (Passport number and Booklet management number)
	EF.COM*3		Common information on basic coding rules
	EF.SOD*3		Security data related to passive authentication defined by ICAO Doc 9303 Part 1, Section IV, NORMATIVE APPENDIX 3
Successful verification with active authentication information access key	EF.DG15*3	Write	Active authentication public key
	Private key file		Active authentication private key

*1 The readout key, transport key, and active authentication information access key are configured by the manufacturer. The transport key can be changed (updated) by authorized user. With regard to the file subject to access control included in this table and files storing the read key and active authentication information access key, user access not stated in this table or Notes is inhibited. (Control of access to terminals after issuing to the passport holder, i.e., <Basic

access control>, is separately specified.)

*2 EF.DG13 has an IC chip serial number entered by the manufacturer and management data added by the passport issuing authorities.

*3 Read (Permitted/Not permitted) in case of successful key verification is not specified.

Application Note: All files stated in the table above store user data or TSF data. The transport key file stores TSF data, and all other files store user data (the management of cryptographic key is treated as user data). The TSF data file is not included in files subject to access control stated in Chapter 6, Section "Security Functional Requirements" and treated in FMT_MTD.1.

Application Note: 'Read' operation means readout from the TOE.

P.Data_Lock

When the TOE detects a failure in authentication with the transport key, readout key or active authentication information access key, it will permanently invalidate authentication related to each key, thereby inhibiting reading or writing the file based on successful authentication thereof. Table 3-1 shows the relationship between the key used for authentication and its corresponding file in the TOE.

P.Prohibit

Any and all writing to the files in the TOE and reading from the files in the TOE based on successful authentication with readout key are inhibited after issuing to the passport holder. As the means, authentication invalidation through authentication failure with the transport key, readout key, and active authentication information access key (see P.Data_Lock) shall be used.

3.5. Assumptions

This section describes assumptions to be addressed in the operational environment of the TOE. These assumptions are needed for the TOE to validate security functionality.

A.Administrative_Env

The TOE that was delivered from the TOE manufacturer to the passport issuing authorities and is under the control of the authorities is subjected to secure management and issuing procedures until it is issued to the passport holder.

A.PKI

In order for the passport inspection authorities of the receiving state or organization to verify the authenticity of information that has been digitally signed by the passport Issuer and stored in the TOE (including the active authentication public key), the interoperability of the PKI environment both of the issuing and receiving states or organizations of the passport is maintained.

4. Security objectives

In this chapter, Security Objectives for the TOE, Security Objectives for the operational environment and Security Objectives rationale are described.

4.1. Security objectives for the TOE

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

O.AA

The TOE shall provide a means to verify the authenticity of the IC chip itself composing the TOE in order to prevent the reproduction of personal information including the digital signature on an illicit IC chip and the forgery of the passport. This means shall be standardized so as to ensure the global interoperability of ePassport and, for this purpose, address active authentication defined by ICAO Doc 9303 Part 1.

O.Logical_Attack

The TOE shall, under any circumstances, prevent confidential information in the TOE (active authentication private key) from being read outside the TOE through the contactless communication interface of the TOE.

O.Physical_Attack

The TOE shall, by a physical means, avert attacks trying to disclose confidential information in the TOE (active authentication private key) not through the contactless communication interface of the TOE. The physical means shall counter attacks applicable to the TOE out of known attacks against the IC chip taking into account nondestructive attacks and also destructive attacks.

O.BAC

This security objective applies to the operational environment after issuing the Passport Booklet. The basic access control procedure defined by [ICAO Doc] shall be used to ensure the global interoperability of the ePassport. This procedure includes mutual authentication between the TOE and the terminals and secure messaging between the same. Communication between the TOE and the terminals performed by the use of the said procedure shall only be permitted. Information the terminal reads from the TOE is stored in the EF.DG1, EF.DG2, EF.DG13, EF.DG15, EF.COM, and EF.SOD files out of the files contained in the rules stated above. The TOE shall permit only the terminal that has succeeded in mutual authentication to read the files stated above. For any files that are not listed in this PP out of those stated above under the same rules, the handling thereof is not defined. Any users other than the TOE shall not be able to have access to the basic access key file and the private key file that have stored internal TOE data.

According to the provisions of ICAO Doc, the common cryptographic key used by the basic access control procedure shall be generated from information printed on the data page of the Passport Booklet, and the contents of the information and the format to describe them shall also comply with the provisions stated above. Thus, the entropy of the said cryptographic key cannot in principle be increased above that specific to the information printed on the data page of

the Passport Booklet. For this reason, with regard to the security functionality of the TOE provided by the basic access control procedure, in the case where a brute-force attack is assumed, the entropy specific to the information printed on the data page of the Passport Booklet becomes the upper limit of resistance force to the attack. The TOE shall meet the security requirements by accurately implementing the basic access control procedure.

Application Note: The basic access control procedure uses a cryptographic key generated from the data printed in the MRZ of ePassport to perform mutual authentication and secure messaging. This cryptographic key can be generated from the printed data when the data page of the ePassport is opened, and does not require a high confidentiality level. The entropy of the key generated is also not as large as it can counter a high level of attacks. However, the security functionality of the basic access control procedure will not affect the protection of the active authentication private key. This security objective is not intended to counter a high level of attacks, but intended to accurately implement the basic access control procedure for the protection of the TOE against limited attacks including skimming and eavesdropping.

O.Authority

The TOE shall limit users and operation methods that have access to the internal TOE information, in the environment under the control of the passport issuing authorities according to the organizational security policy P. Authority, Table 3-5.

O.Data_Lock

The operation of the internal TOE information shall be limited only to the authorized user (i.e., authorized personnel under the control of the passport issuing authorities or the terminal after issuing the passport) to prevent illicit reading and writing by any users other than those stated above. As a means for this purpose, in the case where the TOE detects an authentication failure with the readout key, transport key, or active authentication information access key, this security objective shall permanently inhibit reading and writing the internal TOE information permitted according to authentication related to each of the said keys. The security objective shall also apply to invalidate the readout key, transport key, or active authentication information access key in the case where the passport issuing authorities causes an intentional authentication failure before the TOE is issued to the passport holder. The relationship between the readout key, transport key, and active authentication information access key and their corresponding internal TOE information are as listed in Table 3-5 of the organizational security policy P.Authority. After the security objective O.Data_Lock is implemented, only the access to TOE stated in the security objective O.BAC is permitted.

4.2. Security objectives for the operational environment

This section describes security objectives that the TOE should address in the operational environment to solve problems with regard to the threats and organizational security policies defined as the security problems. In addition, the security objectives stated herein shall all be derived from the assumptions.

OE.Administrative_Env

The TOE being under the control of the authorities is subjected to secure management and treatment until it is delivered to the passport holder through the issuing procedures.

OE.PKI

In order for the ePassport inspection authorities of the receiving state or organization to verify the authenticity of information that has been digitally signed by the passport issuing state or organization and stored in the TOE (i.e., information on the passport holder and the active authentication public key), the TOE shall be used in a situation in which the interoperability of the PKI environment is maintained in both the passport issuing state or organization and receiving state or organization.

4.3. Security Objectives Rationale

In this section, the measures presented in the Security Objectives are verified for their effectiveness against the threats defined in the security challenge definition, organizational security policies and assumptions.

4.3.1. Security Problem Definition and Security Objectives

The following tables Table 4-1 to Table 4-3 show the relationship between the SPD and the Security Objectives.

Table 4-1: Security Problem Definition and Security Objectives

Security Objectives / Security Problem Definition	O.AA	O.Physical_Attack	O.Logical_Attack	O.BAC	O.Authority	O.Data_Lock	O.E.Administrative_Env	O.E.PKI
T.Copy	x							
T.Physical_Attack		x						
T.Logical_Attack			x					
P.BAC				x				
P.Authority					x			
P.Data_Lock						x		
P.Prohibit						x		
A.Administrative_Env							x	
A.PKI								x

Table 4-2: Security Problem Definition and Security Objectives

Threats	Security Objectives	Rationale
T.Copy	O.AA	Section 4.3.2
T.Physical_Attack	O.Physical_Attack	Section 4.3.2
T.Logical_Attack	O.Logical_Attack	Section 4.3.2
P.BAC	O.BAC	Section 4.3.3

Threats	Security Objectives	Rationale
P.Authority	O.Authority	Section 4.3.3
P.Data_Lock	O.Data_Lock	Section 4.3.3
P.Prohibit	O.Data_Lock	Section 4.3.3
A.Administrative_Env	OE.Administrative_Env	Section 4.3.4
A.PKI	OE.PKI	Section 4.3.4

Table 4-3: Security Objectives and Security Problem Definition

Security Objectives	Threats
O.AA	T.Copy
O.Physical_Attack	T.Physical_Attack
O.Logical_Attack	T.Logical_Attack
O.BAC	P.BAC
O.Authority	P.Authority
O.Data_Lock	P.Data_Lock, P.Prohibit
OE.Administrative_Env	A.Administrative_Env
OE.PKI	A.PKI

4.3.2. Threats

This section describes rationales for the security objectives for the TOE and the operational environment to thoroughly counter all identified threats.

T.Copy

In the case where an attacker uses the reproduction of personal information (with digital signature) read from the TOE with the IC chip having the same functionality as that of the TOE, the forged passport cannot be detected through verification by the digital signature. To prevent this attack, the security objective for the TOE: O.AA addresses embedding of data that can verify the authenticity of the IC chip itself in the TOE. This allows the TOE to detect illicit IC chips and prevent the forgery of passports, thus eliminating the threat T.Copy.

T.Logical_Attack

The security objective for the TOE: O.Logical_Attack makes it possible to inhibit reading confidential information (active authentication private key) in the TOE through the contactless communication interface of the TOE, under any circumstances. Thus the threat T.Logical_Attack is eliminated.

T.Physical_Attack

The security objective for the TOE: O.Physical_Attack makes it possible to counter an attack to disclose confidential information (active authentication private key) in the TOE by physical means not through the contactless communication interface of the TOE. For the physical means, both nondestructive attacks and destructive attacks are considered, and countermeasures by which the TOE can counter known attacks against the IC chip. Thus the threat can be reduced to an adequate extent for the practical use.

4.3.3. Organizational Security Policies

This section describes rationales for the security objectives for the TOE and the operational environment to implement organizational security policies.

P.BAC

The security objective for the TOE: O.BAC allows only the authorized personnel (terminal) to read the internal TOE information through a secure communication path by applying the basic access control procedure defined by ICAO Doc 9303 Part 1. O.BAC covers all contents of P.BAC, thus the organizational security policy P.BAC is properly implemented.

P.Authority

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

P.Data_Lock

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

P.Prohibit

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

4.3.4. Assumptions

This section describes rationales for the security objectives for the TOE and the operational environment to further properly meet the assumptions.

A.Administrative_Env

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

A.PKI

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

5. Extended components definition

5.1. Definition of the Family FPT_EMSEC

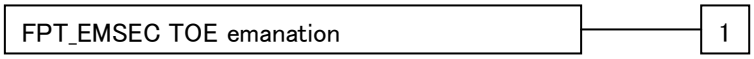
The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [CC2].

The family "TOE Emanation (FPT_EMSEC)" is specified as follows.

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMSEC.1 TOE emanation has two constituents:

FPT_EMSEC.1.1 Limit of Emissions requires not to emit intelligible emissions enabling access to TSF data or user data.

FPT_EMSEC.1.2 Interface Emanation requires not to emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to:	No other components.
Dependencies:	No other components.
FPT_EMSEC.1.1	The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].
FPT_EMSEC.1.2	The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

6. Security requirements

This chapter describes Security functional requirements, Security assurance requirements and Security requirements rationale of TOE.

6.1. Definitions

6.1.1. Access control policy

Issuer processing access control SFP

- This policy refers to access control for the personal information of the passport holder (e.g. name, information on birth and so on), management data and cryptographic key used by the security function in issuing by Booklet manufacture and personalization agent.

Basic access control SFP

- This policy refers to access control for the personal information of the passport holder (e.g. name, information on birth and so on), management data and cryptographic key used by the security function after issuing to the passport holder.

6.1.2. Key distribution method for secure messaging

MET.MUTUAL_AUTHENTICATE

- The TOE exchanges seed data of session key and distributes the session keys by 'MUTUAL_AUTHENTICATE' command of Basic Access Control according to [ICAO Doc] in mutual authentication.

6.2. SFR

This section describes Security functional requirements,

6.2.1. FCS_CKM.1 Cryptographic key generation

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *MET.MUTUAL_AUTHENTICATE adopting cryptographic transport key and authenticator generation transport key generation algorithm which defined by the following*] and specified cryptographic key sizes [assignment: *16 byte*] that meet [assignment: *Rules for secure messaging included in the Basic Access Control specified by [ICAO Doc]*].

6.2.2. FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *method for deleting cryptographic keys on volatile memory by shutting down power supply and rewriting all zero data*] that meet the following: [assignment: *none*].

6.2.3. FCS_COP.1a Cryptographic operation (Active authentication)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1a The TSF shall perform [assignment:*cryptgraphic operation shown in Table 6-1*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm shown in Table 6-1*] and cryptographic key sizes [assignment: *cryptographic key sizes shown in Table 6-1*] that meet the following: [assignment: *the Digital Signature Standards (complying with ISO/IEC 9796-2:2002 Digital signature scheme 1(ISO/IEC 9796-2,Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part2:integer factorization based mechanisms,2002)) used for active authentication defined by [ICAO Doc]*].

Table 6-1 Cryptographic algorithm

Cryptographic algorithm	Key length(bit)	Cryptographic operations
RSA	1792	Signature Generation
SHA-256	256	Hash operation

6.2.4. FCS_COP.1m Cryptographic operation (Mutual authentication)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1m The TSF shall perform [assignment: *authentication data encryption or decryption for mutual authentication and authenticator generation and verification*] in accordance with a specified cryptographic algorithm [assignment: *Triple DES in CBC mode*] and specified cryptographic key sizes [assignment: *16 byte*] that meet the following: [assignment: *Standards for mutual authentication system included in the Basic Access Control defined by [ICAO Doc]*].

6.2.5. FCS_COP.1s Cryptographic operation (Secure messaging)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1s The TSF shall perform [assignment: *cryptographic operation shown in* Table 6-2] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm shown in* Table 6-2] and cryptographic key sizes [assignment: *cryptographic key sizes shown in* Table 6-2] that meet the following: [assignment: *Standards for secure messaging included in the Basic Access Control defined by [ICAO Doc]*].

Table 6-2: cryptographic operation for secure messaging

Cryptographic algorithm	Key length(bit)	Cryptographic operations
CBC modeSingle DES	64(56+CRC8)bits	Authenticator generation and verification (excluding the final block of message)
CBC mode Triple DES(2key)	128(112+CRC16)bits	・Message encryption and decryption ・Authenticator generation verification (final block of message)

6.2.6. FDP_ACC.1a Subset access control (Issuing process)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1a The TSF shall enforce [assignment: *Issue processing access control SFP*] on [assignment: Subject *[Subjects shown in Table 6-3], Object [Objects shown in Table 6-3] and List of operations among subjects and objects addressed by SFP [Operations shown in Table 6-3]*].

Table 6-3: Subset access control (Issuing process)

Subjects	Objects	Operations
Issuing Authority Process	EF.DG13,EF.DG15	Read
	Basic access key file(ENC+MAC), EF.DG1, EF.DG2, EF.DG13, EF.COM, EF.SOD, EF.DG15,Private key file(Active Authentication Private Key)	write

Application Note: The data "transport key" stored in the "transport key file" out of data files shown in Table 3-7 of P.Authority are TSF data used as user authentication data. This PP defines the management of the transport key with the management requirement FMT_MTD.1 and, therefore, does not include the transport key file in the access control subjects. However, this reflects the discrimination between the user data and the TSF data for CC, but does not mean a difference in mechanisms in terms of implementation.

6.2.7. FDP_ACC.1b Subset access control (Basic access control)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1b The TSF shall enforce [assignment: *Basic access control SFP*] on [assignment: *Subject [Process on behalf of terminal], Object [Files EF.DG1, EF.DG2, EF.DG13, EF.DG15, EF.COM , EF.SOD, Basic access key file, and Private key file] and List of operations among subjects and objects addressed by SFP[Reading data from object]*].

Application Note: [ICAO Doc] defines the files EF.DG3 to 12, EF.DG14, and EF.DG16 in addition to the files listed above. These files are not used by this TOE, therefore this ST does not define addressing thereof.

6.2.8. FDP_ACF.1a Security attribute based access control (Issuing process)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT.MSA.3 Static attribute initialization

FDP_ACF.1.1a The TSF shall enforce [assignment: *Issue processing access control SFP*] to objects based on the following: [assignment: *Subject controlled under the indicated SFP [Subjects shown in* Table 6-4*], object [Objects shown in* Table 6-4*], and, for each, the SFP-relevant security attribute [Authentication status shown in* Table 6-4*]*].

FDP_ACF.1.2a The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *Where the authentication status shown in* Table 6-4 *is met, an operation to the file connected to the said authentication status is allowed*].

FDP_ACF.1.3a The TSF shall explicitly authorize access of subjects to objects based on the following additional

rules: [assignment: *none*].

FDP_ACF.1.4a The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *none*].

Table 6-4 Security attribute based access control (Issuing process)

Subjects	Objects	Authentication status	Operations
Issuing Authority process	EF.DG13	Successful verification with readout key	Read
	EF.DG15		
	Transport key file	Successful verification with transport key	Write
	Basic access key file(ENC+MAC)		
	EF.DG1		
	EF.DG2		
	EF.DG13		
	EF.COM		
	EF.SOD		
	EF.DG15	Successful verification with active authentication information access key	Write
	Private key file(active authentication private key)		

6.2.9. FDP_ACF.1b Security attribute based access control (Basic access control)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT.MSA.3 Static attribute initialization

FDP_ACF.1.1b The TSF shall enforce [assignment: *Basic access control SFP*] to objects based on the following: [assignment: *Subject controlled under the indicated SFP [Process on behalf of terminal], object [Files EF.DG1, EF.DG2, EF.DG13, EF.DG15, EF.COM, EF.SOD], and the security attribute [Authentication status of terminal based on mutual authentication]*].

FDP_ACF.1.2b The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *Where the authentication status of terminal has been successfully authenticated, subjects are allowed to read data from objects*].

FDP_ACF.1.3b The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *none*].

FDP_ACF.1.4b The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *Inhibition of access of subjects to the basic access key file and private key file*].

Application Note: This 'access' means file operation by subjects.

Application Note:

Table 6-5 Security attribute based access control (Basic access control)

Subjects	*Objects*	*Authentication status*	*Operations*
Process on behalf of terminal	*EF.DG1*	*Succeful authentication with mutual authentication*	***Read*1***
	EF.DG2		
	EF.DG13		
	EF.DG15		
	EF.COM		
	EF.SOD		
	Basic access key file(ENC+MAC)	*Any authentication with mutual authentication*	***No operation***
	Private key file(active authentication private key)		

**1 Secure messaging is a must.*

6.2.10. FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control or
FDP.IFC.1 Subset information flow control]
FMT.MSA.3 Static attribute initialization

FDP_ITC.1.1 , The TSF shall enforce the [assignment: *Issue processing access control SFP*] when importing user data, controlled under the SFP, from outside the TOE.

Application note: This SFR's target is 'write' operation in Table6-4.

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

FDP_ITC.1.3 The TSF shall enforce the following rules when user data importing controlled under the SFP from outside the TOE: [assignment: *Association between file subject to writing and data as specified by "Access to be permitted" in* Table 3-7 *of the organizational security policy P.Authority*].

6.2.11. FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel or

FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control or
FDP.IFC.1 Subset information flow control]

FDP_UCT.1.1 The TSF shall enforce [assignment: *Basic access control SFP*] to be able to [selection: *transmit, receive*] user data in a manner protected from unauthorized disclosure.

6.2.12. FDP_UIT.1 Data exchange integrity

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control or
FDP.IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel or
FTP_TRP.1 Trusted path]

FDP_UIT.1.1 The TSF shall enforce [assignment: *Basic access control SFP*] to [selection: *transmit, receive*] user data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [selection: *modification, deletion, insertion, replay*] has occurred.

6.2.13. FIA_AFL.1a Authentication failure handling (Active authentication information access key)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1a The TSF shall detect when [selection: *[assignment: 1-15]*] unsuccessful authentication attempts occur related to [assignment: *authentication with the active authentication information access key*].

FIA_AFL.1.2a When the defined number of unsuccessful authentication attempts has been [selection: *met*], the TSF shall [assignment: *permanently stop authentication with the active authentication information access key (fix the authentication status with the active authentication information access key to "No authentication")*].

6.2.14. FIA_AFL.1d Authentication failure handling (Transport key)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1d The TSF shall detect when [selection: *[assignment: 1-15]*] unsuccessful authentication attempts occur related to [assignment: *authentication with the transport key*].

FIA_AFL.1.2d When the defined number of unsuccessful authentication attempts has been [selection: *met*], the TSF shall [assignment: *permanently stop authentication with the transport key (fix the authentication status with the transport key to "No authentication")*].

6.2.15. FIA_AFL.1r Authentication failure handling (Read key)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1r The TSF shall detect when [selection: *[assignment: 1-15]*] unsuccessful authentication attempts occur related to [assignment: *authentication with the readout key*].

FIA_AFL.1.2r When the defined number of unsuccessful authentication attempts has been [selection: *met , surpassed*], the TSF shall [assignment: *permanently stop authentication with the readout key (fix the authentication status with the readout key to "No authentication")*].

6.2.16. FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.17. FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.18. FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [assignment: *multiple authentication mechanisms shown in* Table 6-6] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [assignment: *rules describing how the multiple authentication mechanisms shown in* Table 6-6 *provide authentication*].

Table 6-6: Multiple authentication mechanisms

Authentication mechanism name	Rule applicable to authentication mechanism
Transport key	Verification with transport keys that have been

Authentication mechanism name	Rule applicable to authentication mechanism
	already stored in the TOE
Readout key	Verification with readout keys that have been already stored in the TOE
Active authentication information access key	Verification with active authentication information access keys that have been already stored in the TOE
Mutual authentication	Rules for authentication of terminals according to the mutual authentication procedure defined by ICAO Doc 9303 Part 1

6.2.19. FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf ofthat user.

6.2.20. FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT.SMF.1 Specification of management function

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

6.2.21. FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2.22. FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the role [assignment: *authorized personnel of the passport issuing authorities*].

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

6.2.23. FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No other components.

FPT_EMSEC.1.1 The TOE shall not emit [assignment: electromagnetic emissions] in excess of [assignment: levels which could be measured and analyzed] enabling access to [assignment: none] and [assignment: Active Authentication Private Key].

Application note: STMicrosystems assigns "none" in [assignment: list of types of user data].

FPT_EMSEC.1.2 The TSF shall ensure [assignment: any unauthorized users] are unable to use the following interface [assignment: smart card circuit contacts] to gain access to [assignment: none] and [assignment: Active Authentication Private Key].

Application Note: The ST writer shall perform the operation in FPT_EMSEC.1.1 and FPT_EMSEC.1.2. The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. TheIC chip has to provide a smart card contactless interface. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

Application note: The TOE (IC sheet) has only contact-less interface physically.

6.2.24. FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [assignment: the following *list of types of failures in the TSF*].

[*List of types of failures in the TSF*]

- Detection of an abnormal status of the granted check code during EEPROM read-out

- Detection of a recalculation error during the private key calculation
- Detection of an abnormal status of a security sensor of chip hardware
- Detection of self-check test error upon resetting
- Detection of bypass processing not correctly perform

6.2.25. FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up, at the conditions[assignment:* After chip H/W initialization*]*] to demonstrate the correct operation of [selection: *[assignment:* RNG, SF.MemoryManager, SF.DomainSeparation*], the TSF*].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of [selection: *[assignment: Transport Key], TSF data*].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of [selection: *[assignment: parts of TSF]*]

6.2.26. FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist [assignment: *attacks shown in the following list of physical tampering scenarios*] to the [assignment: *hardware of the TOE and firmware and software composing the TSF*] by automatically responding such that the SFRs are always enforced.

[List of physical attack scenarios]

- An attack, which discloses confidential information (active authentication private key) by destructing the outer shell of the TOE and analyzing the behavior of the TOE through physical probing and manipulation to the internal circuit.
- An attack, which discloses confidential information (active authentication private key) by impairing normal TOE operation through the application of environmental stress (e.g. application of temperature, power supply voltage, or clock outside the normal operating range, or application of electromagnetic pulse, or light irradiation) to the TOE in operation and analyzing the behavior of the TOE at that time.
- An attack, which discloses confidential information (active authentication private key) by analyzing the behavior of the TOE through monitoring of electromagnetic waves leaking from the TOE in operation.

Application Note: Security functional requirements used to counter physical attacks all have been summarized in this requirement. Attacks that monitor leakage of electromagnetic waves associated with the operation of the TOE may not involve interference with or damage to the TSF. As means to counter the said attacks, physical means (e.g.

electromagnetic shielding) may be used or logic means (e.g. randomization of power consumption) may be used in combination. However, it is reasonable to include the attacks stated above in the same category as that of other physical attacks in terms of using physical means not through the logical interface of the TOE as tampering means. Therefore, monitoring attacks were made against the physical attack scenarios in this requirement to define requirements to counter such attacks.

6.2.27. FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1	The TSF shall establish the communication channel between itself and another trusted IT product that is logically distinct from other communication channel and provides assured identification of its end point and protection of channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit [selection: *TSF, another trusted IT product*] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [assignment: *reading data from the TOE*].

Application Note: Communication between terminal and TSF shall be performed via the secure messaging channel defined by ICAO Doc 9303 Part 1. After the secure messaging channel is established, only the secure messaging channel is available for the communication path between terminal and TOE.

6.3. Security assurance requirements

The security assurance requirement level is EAL4 augmented with ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2 and ATE_DPT.3.

6.4. Security requirements rationale

6.4.1. Security Objectives and Security Functional Requirements

The relationship between Security Objectives and Security Functional Requirements are shown inTable 6-7.
InTable 6-8, the section numbers where rationale of such relationship is described are also shown.

Table 6-7: Security Functional Requirements and Security Objectives

Security Functional Requirements / Security Objectives	FCS_CKM.1	FCS_CKM.4	FCS_COP.1a	FCS_COP.1m	FCS_COP.1s	FDP_ACC.1a	FDP_ACC.1b	FDP_ACF.1a	FDP_ACF.1b	FDP_ITC.1	FDP_UCT.1	FDP_UIT.1	FIA_AFL.1a	FIA_AFL.1d	FIA_AFL.1r	FIA_UAU.2	FIA_UAU.4	FIA_UAU.5	FIA_UID.2	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_EMSEC.1	FPT_FLS.1	FPT_TST.1	FPT_PHP.3	FTP_ITC.1
O.AA							x		x																		
O.Physical_Attack																							x	x	x	x	
O.Logical_Attack			x			x		x		x																	
O.BAC	x	x		x	x		x		x	x	x	x				x	x	x	x								x
O.Authority						x		x		x						x		x	x	x	x	x					
O.Data_Lock													x	x	x												

Table 6-8: Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
O.AA	FCS_COP.1a FDP_ACC.1a FDP_ACF.1a FDP_ITC.1	Section 6.3.2
O.Physical_Attack	FPT_EMSEC.1 FPT_FLS.1 FPT_TST.1 FPT_PHP.3	Section 6.3.2
O.Logical_Attack	FDP_ACC.1b FDP_ACF.1b	Section 6.3.2
O.BAC	FCS_CKM.1 FCS_CKM.4 FCS_COP.1m FCS_COP.1s FDP_ACC.1b FDP_ACF.1b FDP_ITC.1 FDP_UCT.1 FDP_UIT.1 FIA_UAU.2 FIA_UAU.4 FIA_UAU.5 FIA_UID.2 FTP_ITC.1	Section 6.3.2
O.Authority	FDP_ACC.1a FDP_ACF.1a FDP_ITC.1 FIA_UAU.2 FIA_UAU.5 FIA_UID.2 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1	Section 6.3.2

Security Objectives	Security Functional Requirements	Rationale
O.Data_Lock	FIA_AFL.1a FIA_AFL.1d FIA_AFL.1r	Section 6.3.2

The relationship between Security Objectives and Security Functional Requirements are shown inTable 6-9.

Table 6-9: SFRs and Security Objectives

Security Functional Requirements	Security Objectives
FCS_CKM.1	O.BAC
FCS_CKM.4	O.BAC
FCS_COP.1a	O.AA
FCS_COP.1m	O.BAC
FCS_COP.1s	O.BAC
FDP_ACC.1a	O.AA O.Authority
FDP_ACC.1b	O.BAC O.Logical_At
FDP_ACF.1a	O.AA O.Authority
FDP_ACF.1b	O.BAC O.Logical_At
FDP_ITC.1	O.AA O.BAC O.Authority
FDP_UCT.1	O.BAC
FDP_UIT.1	O.BAC
FIA_AFL.1a	O.Data_Lock
FIA_AFL.1d	O.Data_Lock
FIA_AFL.1r	O.Data_Lock
FIA_UAU.2	O.BAC O.Authority
FIA_UAU.4	O.BAC
FIA_UAU.5	O.BAC O.Authority
FIA_UID.2	O.BAC O.Authority
FMT_MTD.1	O.Authority
FMT_SMF.1	O.Authority

Security Functional Requirements	Security Objectives
FMT_SMR.1	O.Authority
FPT_EMSEC.1	O.Physical_Attack
FPT_FLS.1	O.Physical_Attack
FPT_TST.1	O.Physical_Attack
FPT_PHP.3	O.Physical_Attack
FTP_ITC.1	O.BAC

6.4.2. Objectives

Verifying the effectiveness of the Security requirements against Security Objectives.

O.AA

To achieve the security objective O.AA, it shall address the active authentication procedure defined by ICAO Doc 9303 Part 1. This active authentication is an act for a terminal to authenticate the IC chip of the TOE, and the TOE itself needs not to provide any authentication mechanism. The TOE is authenticated by properly addressing the authentication procedure. To address requirements for the authentication procedure from the terminal, the TOE incorporates the public key and private key pair and performs cryptographic operation using the private key defined by FCS_COP.1a. The public key and private key pair is imported to the TOE by FDP_ITC.1. Access control associated with FDP_ITC.1 is defined by FDP_ACC.1a and FDP_ACF.1a. The security objective O.AA is thoroughly achieved by the said SFRs.

O.Logical_Attack

Confidential information (active authentication private key) subject to protection is stored in the private key file of the TOE. FDP_ACC.1b and FDP_ACF.1b deny reading of data from the private key file by the user process on behalf of the terminal. The security objective O.Logical_Attack is thoroughly achieved by the said SFRs.

O.Physical_Attack

Attack scenarios trying to disclose the active authentication private key that is confidential information by a physical means are stated in the list of physical attack scenarios shown in the FPT_PHP.3 section. The TSF automatically resists the attacks according to FPT_PHP.3 to protect against the disclosure of the confidential information.

TSF resists EMA/DEMA according to FPT_EMSEC.1. SPA/DPA is the attack which discloses confidential information by analyzing of electromagnetic waves leaking from the TOE

FPT_TST.1 contributes to the correct execution of TSF code by running self tests to demonstrate the correct operation of TSF and providing authorized users with the capability to verify the integrity of TSF data and executable code.

TSF preserves a secure state according to FPT_FLS.1 when failures occur in the TOE.

These means protects against the disclosure of the confidential information.
With that, the security objective O.Physical_Attack is thoroughly achieved.

O.BAC

FIA_UID.2 and FIA_UAU.2 provides the TOE service for the user (equivalent to a terminal) that has succeeded in identification and authentication. User authentication requires the mutual authentication procedure with the basic access control defined by ICAO, which is defined by FIA_UAU.5. This mutual authentication procedure requires new authentication data based on random numbers for each authentication, which is defined by FIA_UAU.4. Likewise, secure messaging required by the basic access control is defined by FDP_UCT.1 and the requirements for the protection of transmitted and received data by FDP_UIT.1 and cryptographic communication channels by FTP_ITC.1. Further, with regard to cryptographic processing required for the basic access control procedure, FCS_COP.1m defines cryptographic operations necessary for the mutual authentication procedure and FCS_COP.1s defines cryptographic operations for secure messaging. With regard to the cryptographic keys used for secure messaging, FDP_ITC.1 defines the import of basic access keys, FCS_CKM.1 defines the generation of session keys, and FCS_CKM.4 defines the destruction of these keys. In order for only permitted personnel to read given information from the TOE, rules governing access control with FDP_ACC.1b and FDP_ACF.1b are defined. The security objective O.BAC is thoroughly achieved by the said SFRs.

O.Authority

For TOE processing by the passport issuing authorities, the identification and authentication requirements FIA_UID.2 and FIA_UAU.2 are applied, in order to grant the processing authority only to the duly authorized user. For user authentication mechanisms, FIA_UAU.5 defines the use of the transport key, readout key, or active authentication information access key. The rules governing access control with FDP_ACC.1a and FDP_ACF.1a are applied to the user that has succeeded in authentication by verification with the said key and access to the internal TOE information defined by O.Authority is granted to that user. The user operation includes writing of the authentication key (transport key), cryptographic keys (active authentication public key and private key pair, and basic access key for secure messaging), and other user data in the TOE. Correspondence between object and security attributes for writing is defined by FDP_ITC.1. O.Authority includes updating (rewriting) of the transport keys by the authorized personnel of the passport issuing authorities and is defined by FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1. The security objective O.Authority is thoroughly achieved by the said SFRs.

O.Data_Lock

When the active authentication information access key, transport key, or readout key causes a failure in authentication, the security objective of permanently inhibiting authentication corresponding to the relevant key is thoroughly achieved by the three SFRs FIA_AFL.1a, FIA_AFL.1d, and FIA.AFL.1r.

6.4.3. SFRs dependencies

Table 6-10 shows the dependency provided in CC which is to be supported by the Security Functional Requirements as well as the dependencies supported or not supported by the TOE. The indication "-" in the table means no

dependency.

For those requirements whose dependency is not supported, the rationales of the exclusion of such dependency are described below.

Table 6-10: SFRs dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1s FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1a	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 (1)
FCS_COP.1m	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 (1)
FCS_COP.1s	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 FCS_CKM.4
FDP_ACC.1a	FDP_ACF.1	FDP_ACF.1a
FDP_ACC.1b	FDP_ACF.1	FDP_ACF.1b
FDP_ACF.1a	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1a (2)
FDP_ACF.1b	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1b (2)
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1a (2)
FDP_UCT.1	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	FTP_ITC.1 FDP_ACC.1b
FDP_UIT.1	[FTP_ITC.1 or FTP_TRP.1]	FTP_ITC.1 FDP_ACC.1b

Requirements	CC Dependencies	Satisfied Dependencies
	[FDP_ACC.1 or FDP_IFC.1]	
FIA_AFL.1a	FIA_UAU.1	FIA_UAU.2
FIA_AFL.1d	FIA_UAU.1	FIA_UAU.2
FIA_AFL.1r	FIA_UAU.1	FIA_UAU.2
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.4	–	–
FIA_UAU.5	–	–
FIA_UID.2	–	–
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	–	–
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_EMSEC.1	–	–
FPT_FLS.1	–	–
FPT_TST.1	–	–
FPT_PHP.3	–	–
FTP_ITC.1	–	–

Rationale for the exclusion of dependencies

(1) Since the modification and destruction of cryptographic keys are inhibited, the destruction requirement FCS_CKM.4 does not apply to.

(2) Objects are generated by default configuration, but not generated in the operational environment of the TOE. Therefore, FMT_MSA.3 related to file generation does not apply to.

6.4.4. SARs dependencies

Table 6-11 shows the dependency provided in CC which is to be supported by the Security Assurance Requirements as well as the dependencies supported or not supported by the TOE. The indication "–" in the table means no dependency.

Table 6-11: SARs dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.5, ADV_TDS.4
ADV_FSP.5	(ADV_IMP.1) and (ADV_TDS.1)	ADV_IMP.1, ADV_TDS.4
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.4, ALC_TAT.1
ADV_INT.2	(ADV_IMP.1) and (ADV_TDS.1) and (ALC_TAT.1)	ADV_IMP.1, ADV_TDS.4, ALC_TAT.2
ADV_TDS.4	(ADV_FSP.4)	ADV_FSP.5

Requirements	CC Dependencies	Satisfied Dependencies
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.5
AGD_PRE.1	No dependencies	–
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4, ALC_DVS.2, ALC_LCD.1
ALC_CMS.5	No dependencies	–
ALC_DEL.1	No dependencies	–
ALC_DVS.2	No dependencies	–
ALC_LCD.1	No dependencies	–
ALC_TAT.2	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No dependencies	–
ASE_INT.1	No dependencies	–
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No dependencies	–
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.5, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.5, ATE_FUN.1
ATE_DPT.3	(ADV_ARC.1) and (ADV_TDS.4) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.4, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.5, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.3	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.5, ADV_IMP.1, ADV_TDS.4, AGD_OPE.1, AGD_PRE.1, ATE_DPT.3

6.4.5. Rationale for the Security Assurance Requirements

To use the IC chip as the TOE, leading-edge technologies are required for SFRs and design methods for realizing the SFRs, the TOE must have resistance against the sophisticated attack.In order to provides defence of property level against the sophisticated attack, stringency of the top level for commercial product is required.As a result, EAL4 is required in [PP-AA], which is selected for this ST.

The security property of this TOE is focused on the difficulty in forging the TOE (IC chip) by adopting the active authentication function.

This ST is augmented with assurance requirements included in pacage of EAL5 except the vulnerability assessment and ALC_DVS.2 required in [PP-AA] .
In these assurance requirements, ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_DVS.2, ALC_TAT.2 and ATE_DPT.3 are components of a higher level than EAL4 claimed by this ST.

But AVA_VAN.5 is selected as assurance requirements of vulnerability assessment in [AA-PP], AVA_VAN.3 is selected in this ST.

ADV_FSP.5 has dependencies with ADV_IMP.1 and ADV_TDS.1.
ADV_INT.2 has dependencies with ADV_IMP.1, ADV_TDS.1 and ALC_TAT.1.
ADV_TDS.4 has dependencies with ADV_FSP.4.
ALC_TAT.2 has dependencies with ADV_IMP.1.
ATE_DPT.3 has dependencies with ADV_ARC.1, ADV_TDS.4 and ATE_FUN.1.
All these dependencies are satisfied by EAL4. ALC_DVS.2 and ALC_CMS.5 have no dependencies.

7. TOE summary specification

In this chapter, the security functions of TOE are provided.

7.1. Security Functions and Security Functional Requirements

This section presents the compliance to the security functional requirements by describing the TOE security function summary specifications. The Table 7-1 shows the relationship between the security functional requirements and the security functions.

Table 7-1: Security Functions and Security Functional Requirements

Security Functions / Security Functional Requirements	7.1.1 SF.Init	7.1.2 SF.Crypt	7.1.3 SF.SecureMessaging	7.1.4 SF.KeyManager	7.1.5 SF.MemoryManager	7.1.6 SF.DomainSeparation	7.1.7 SF.Authentication	7.1.8 SF.AccessControl	7.1.9 SF.Supervisor	7.1.10 SF.PhysicalTamper
FCS_CKM.1		*		*						
FCS_CKM.4		*	S	*						
FCS_COP.1a		*								
FCS_COP.1m		*					S			
FCS_COP.1s		*	*							
FDP_ACC.1a						S		*		
FDP_ACC.1b		S				S		*		
FDP_ACF.1a						S	S	*		
FDP_ACF.1b		S				S	S	*		
FDP_ITC.1							*	*		
FDP_UCT.1			*							
FDP_UIT.1			*							
FIA_AFL.1a				S			*			
FIA_AFL.1d				S			*			
FIA_AFL.1r				S			*			
FIA_UAU.2						S	*	S		
FIA_UAU.4							*			
FIA_UAU.5							*			
FIA_UID.2							*			
FMT_MTD.1						S	S	*		
FMT_SMF.1						S	S	*		
FMT_SMR.1						S	*			
FPT_EMSEC.1		*								*
FPT_FLS.1		S								*
FPT_TST.1	*									*
FPT_PHP.3	*	*				S			*	*
FTP_ITC.1			*							

'*' … primary SFR , 'S' … supportive SFR

The summary specification of TOE security functions (TSF) is described below.

7.1.1. SF.Init

The function of SF.Init performs the initialization upon occurrence of the reset interrupt. The initialization process ensures the correct initialization of the TOE's functionalities.

7.1.2. SF.Crypt

With this function, the following cryptographic functions are achieved. Enhanced DES accelerator (EDES) and NESCRYPT accelerator which are cryptographic coprocessors of ST23YR80 are used for encryption (EDES is for Triple-DES (2 key) , and NESCRYPT is for RSA). These coprocessors are controlled using the cryptographic library from STMcroelectronics (ST23 open source cryptographic library is for Triple-DES (2 key), and NesLib is for RSA).

(a) Symmetric-key Cryptography

- Triple-DES (2 key) : Enhanced DES accelerator (ST23 open source cryptographic library)
  : CBC mode Single-DES 8bytes
  : CBC mode Triple-DES 16bytes

(b) Public-key Cryptography

- RSA :NESCRYPT accelerator (NesLib)
  :RSA1792bit CRT supports digital signature conplying with [ISO/IEC9796-2]

(c) Hash Operation

- SHA-1/256 :SHA-1/256 complies with [FIPS180-2]

The random number generation is implemented by this function too. The TRNG complies with AIS 31 class P2 [AIS31], and generates 1byte random numbers per 64CPU Clock.

7.1.3. SF.SecureMessaging

The purpose of the function SF.SecureMessaging is the protection of Command APDUs or Response APDUs exchanged between the Smart Card and an external device. Session key distributed By 'MUTUAL_AUTHENTICATE' command is used for the encryption and adding message identifier.Encryption and authentication are the two functions SF.SecureMessaging has. While the encryption is to ensure secrecy by encrypting a command or data part of a response, the authentication guarantees authenticity of the APDU and its sender by adding message identifier (CCS) to APDU.

7.1.4. SF.KeyManager

The function of SF.KeyManager is for managing a key data for encryption.

It involves:

- Key-format check, and dispatch of a key to a relevant encryption function;
- Read-out of the number of key authentication attempts remaining;

- Loading the key; and
- Managing the session key

7.1.5. SF.MemoryManager

The function of SF.MemoryManager ensures the confidentiality regarding the operations including Read, Create and Update from RAM or EEPROM. It also ensures the integrity in the Read operation from these memories.

7.1.6. SF.DomainSeparation

The function of SF.DomainSeparation divides the memory into multiple segments by using the MPU function which is provided by the Security IC, granting an attribute to each of them. The attribute of the segment is evaluated for access control at the time of the access to the memory. The access control is also implemented by the software firewall, by which the objects other than the selected one are deactivated.

The function implements the following countermeasures against the vulnerabilities and prevents the malfunction of the Security IC as well as the mutual interference between the applications. The countermeasures are:

- Unauthorized data read-out: Data read-out from the field other than the communication buffer during communication;
- Buffer Overflow: Buffer overflow caused by sending the data bigger than the communication buffer;
- Stack Overflow: Data destruction and alteration caused by the wrongful data stacking; and
- Forbidding the direct access from application to TOE asset

7.1.7. SF.Authentication

The function of SF.Authentication implements external authentication in order to confirm if a card user is authorized to use card functions. The external authentication is implemented by the card through verifying internally the authentication data sent from the external devices.

It involves:

- PIN verification;
- Signature verification;
- Update of the number of key authentication attempts remaining;and
- BAC verification.

7.1.8. SF.AccessControl

The function of SF.AccessControl checks if a card user has a right required for executing a specific command based on the result of external authentication and life cycle information.

7.1.9. SF.Supervisor

The function of SF.Supervisor manages starting address and ending address of each segment (ROM/RAM/EEPROM) and the privilege to be given in an integrated fashion in order to ensure the correct functioning of the MPU functions implemented in the Security IC. It also controls the access based on the given privilege.

7.1.10. SF.PhysicalTamper

The function of SF.PhysicalTamper is achived by security IC, by a physical means, averts attacks trying to disclose confidential information.

Application note: Description of this function is described in IC chip's ST[STSTM].

8. Compatibility Statement

In this chapter, compatibility statements are described.

8.1. Compatibility regarding the separation between platform TSF and composite TSF

In the Table 8-1, platform SFRs used in the composite ST is provided. The platform-TSFs can be subdivided into the relevant platform-TSFs used in the ST and others. This means that IP_SFR = { FMT_LIM.1, FMT_LIM.2, FAU_SAS.1, FRU_FLT.2, FDP_IFC.1, FMT_MSA.3, FMT_MSA.1, FDP_ACC.2, FDP_ACF.1, FDP_ITT.1, FPT.ITT.1 } and RP_SFR = { FPT_PHP.3, FCS_COP.1,FPT_FLS.1, FCS_RNG.1 }. In other words, Platform-SFR = IP_SFR U RP_SFR.

Table 8-1: Relevant Platform-SFRs and Composite-SFRs

Platform -SFRs / Composite -SFRs	FRU_FLT.2	FPT_FLS.1	FMT_LIM.1	FMT_LIM.2	FAU_SAS.1	FPT_PHP.3	FDP_ITT.1	FPT_ITT.1	FDP_IFC.1	FCS_RNG.1	FCS_COP.1	FDP_ACC.2	FDP_ACF.1	FMT_MSA.3	FMT_MSA.1	Security Functionality
FCS_CKM.1										*						Cryptographic operation by ST23 open source cryptographic library
FCS_CKM.4																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer
FCS_COP.1a											*					Cryptographic operation by ST23 open source cryptographic library
FCS_COP.1m											*					Cryptographic operation by ST23 open source cryptographic library and NesLib
FCS_COP.1s											*					Cryptographic operation by ST23 open source cryptographic library and NesLib
FDP_ACC.1a																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer
FDP_ACC.1b																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer

Platform -SFRs / Composite -SFRs	FRU_FLT.2	FPT_FLS.1	FMT_LIM.1	FMT_LIM.2	FAU_SAS.1	FPT_PHP.3	FDP_ITT.1	FPT_ITT.1	FDP_IFC.1	FCS_RNG.1	FCS_COP.1	FDP_ACC.2	FDP_ACF.1	FMT_MSA.3	FMT_MSA.1	Security Functionality
FDP_ACF.1a																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer
FDP_ACF.1b																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer
FDP_ITC.1																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer
FDP_UCT.1																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer
FDP_UIT.1																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer
FIA_AFL.1a																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer
FIA_AFL.1d																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer
FIA_AFL.1r																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer
FIA_UAU.2																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer
FIA_UAU.4																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer

Platform -SFRs / Composite -SFRs	FRU_FLT.2	FPT_FLS.1	FMT_LIM.1	FMT_LIM.2	FAU_SAS.1	FPT_PHP.3	FDP_ITT.1	FPT_ITT.1	FDP_IFC.1	FCS_RNG.1	FCS_COP.1	FDP_ACC.2	FDP_ACF.1	FMT_MSA.3	FMT_MSA.1	Security Functionality
FIA_UAU.5																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer
FIA_UID.2																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer
FMT_MTD.1																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer
FMT_SMF.1																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer
FMT_SMR.1																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer
FPT_EMSEC.1						*					*					Implementing the EMA/DEMA countermeasures using the Platform-SFRs
FPT_FLS.1		*														Maintaining the secure status against the security compromise detected by the Platform-SFRs
FPT_TST.1		*				*										Implementing the secure initialization using the Platform-SFRs
FPT_PHP.3		*				*										Implementing the countermeasure for physical attack using the Platform-SFRs
FTP_ITC.1																Platform-SFRs are not used as this functionality is implemented in the AP layer or OS layer

8.2. Compatibility of Threats, OSPs, Assumptions and Objectives

In the Table8-2, compatibility of Threats, OSPs, Assumptions and Objectives with IC Security Target are shown.

Table 8-2: Composition with IC Security Target

IC Elements	Relevant	Consistent in Composite ST with	Justification
BSI.T.Leak-Inherent Inherent Information Leakage	Yes	T.Physical_Attack	This threat is considered as EMA attacks. Threat of T.Physical_Attack considered various physical attack including EMA, Malfunction, Probing, Manipulation.
BSI.T.Phys-Probing Physical Probing	Yes	T.Physical_Attack	This threat is considered as Probing attacks. Threat of T.Physical_Attack considered various physical attack including EMA, Malfunction, Probing, Manipulation.
BSI.T.Malfunction Malfunction due to Environmental Stress	Yes	T.Physical_Attack	This threat is considered as Malfunction attacks. Threat of T.Physical_Attack considered various physical attack including EMA, Malfunction, Probing, Manipulation.
BSI.T.Phys-Manipulation Physical Manipulation	Yes	T.Physical_Attack	This threat is considered as Manipulation attacks. Threat of T.Physical_Attack considered various physical attack including EMA, Malfunction, Probing, Manipulation.
BSI.T.Leak-Forced Forced Information Leakage	Yes	T.Physical_Attack	This threat is considered as EMA attacks. Threat of T.Physical_Attack considered various physical attack including EMA, Malfunction, Probing, Manipulation.
BSI.T.Abuse-Func Abuse of Functionality	Yes	T.Physical_Attack	This threat is considered as Abuse of Functionality. Threat of T.Physical_Attack considered various physical attack including EMA, Malfunction, Probing, Manipulation.

IC Elements	Relevant	Consistent in Composite ST with	Justification
BSI.T.RND Deficiency of Random Numbers	Yes	T.Physical_Attack	This threat is considered as entropy of random number reduced by any attacks. Threat of T.Physical_Attack considered various physical attack including EMA, Malfunction, Probing, Manipulation.
AUG4.T.Mem-Access Memory Access Violation	Yes	T.Physical_Attack	This threat is considered as abuse memory access by manipulation etc. Threat of T.Physical_Attack considered various physical attack including EMA, Malfunction, Probing, Manipulation.
BSI.P.Process-TOE Protection during TOE Development and Production	No	n/a	This OSP requires to identify IC. This OSP does not interfere with the composite ST ones.
AUG1.P.Add Functions Additional Specific Security Functionality (Cipher Scheme Support)	No	n/a	This OSP requires to provide functionality of DES and T-DES. This OSP does not interfere with the composite ST ones.
BSI.A.Process-Sec-IC Protection during Packaging, Finishing and Personalisation	Yes	A.Administrative_Env	This Assumption ensure security of the delivery and storage of the TOE and related data. There is no descrepancies with composite ST ones.
BSI.A.Plat-Appl Usage of Hardware Platform	No	n/a	This Assumption ensure appropriate usage of Hardware Platform in development process. This Assumptions does not interfere with the composite ST ones.
BSI.A.Resp-Appl Treatment of User Data	No	n/a	This Assumption ensure appropriate treatment of User data in development process. This Assumptions does not interfere with the composite ST ones.

IC Elements	Relevant	Consistent in Composite ST with	Justification
AUG1.A.Key-Function Usage of key-dependent functions	No	n/a	This Assumption requires that key-dependent functions are implemented in a way which protects against EMA attack. This Assumptions does not interfere with the composite ST ones.
BSI.O.Leak-Inherent Protection against Inherent Information Leakage	Yes	O.Physical_Attack	This Objective requires to protect against EMA attack. Software is designed to be protected against Leakage. This Objective is realized by the hardware support.
BSI.O.Phys-Probing Protection against Physical Probing	Yes	O.Physical_Attack	This Objective requires to protect against Probing attack. This Objective is realized by the IC.
BSI.O.Malfunction Protection against Malfunctions	Yes	O.Physical_Attack	This Objective requires to protect against Malfunction attack. Software is designed to be protected against Malfunction. This Objective is realized by the hardware support.
BSI.O.Phys-Manipulation Protection against Physical Manipulation	Yes	O.Physical_Attack	This Objective requires to protect against Manipulation attack. Software is designed to be protected against Manipulation. This Objective is realized by the hardware support.
BSI.O.Leak-Forced Protection against Forced Information Leakage	Yes	O.Physical_Attack	This Objective requires to protect against EMA attack. Software is designed to be protected against Leakage. This Objective is realized by the hardware support.

IC Elements	Relevant	Consistent in Composite ST with	Justification
BSI.O.Abuse-Func Protection against Abuse of Functionality	Yes	O.Physical_Attack	This Objective requires to protect against abuse of functionality attack. Software is designed to be protected against manipulation or bypass. This Objective is realized by the hardware support.
BSI.O.Identification TOE Identification	No	n/a	This Objective requires to identify TOE. There is no descrepancies with composite ST ones.
BSI.O.RND Random Numbers	Yes	O.Physical_Attack	This Objective requires to protect against entropy of random number reduced by any attacks. This objective is realized by the IC.
AUG1.O.Add-Functions Additional Specific Security Functionality	Yes	O.BAC	This Objective requires to provide functionality of DES and T-DES. These functionalities are implemented by using Neslib. This Objective is realized by the hardware support.
AUG4.O.Mem Access Dynamic Area based Memory Access Control	Yes	O.Physical_Attack	This objcective requires to define dynamic memory segmentation and protection and enforce the defined access rules. This objective is realized by the IC.
BSI.OE.Plat-Appl Usage of Hardware Platform with AUG1.Clarification & AUG4.Clarification	No	n/a	This Objective ensures appropriate usage of Hardware Platform in development process. This Objective does not interfere with the composite ST ones.
BSI.OE.Resp-Appl Treatment of User Data with AUG1.Clarification & AUG4.Clarification	No	n/a	This Objective ensures appropriate treatment of user data in development process. This Objective does not interfere with the composite ST ones.

IC Elements	Relevant	Consistent in Composite ST with	Justification
BSI.OE.Process-Sec-IC Protection during composite product manufacturing	Yes	OE.Administrative_Env	This Objective ensures security of the delivery and storage of the TOE and related data. There is no descrepancies with composite ST ones.

9. References

In this chapter, terms used in this ST and references are listed

9.1. Terms

Table 9-1: Terms

Terms	Definition
ADV	Development class
AGD	Guidance Documents class
ALC	Life-Cycle Support class
API	Application Programming Interface
ATE	Tests class
AVA	Vulnerability Assessment class
CC	Common Criteria
CCS	Cryptographic Checksum Message Authentication Code (MAC) provided in secure messaging for message Authentication
CM	Card Manager
Strict conformance	hierarchical relationship between a PP and an ST where all the requirements in the PP also exist in the ST
DF	Dedicated File
DPA	Differential Power Analysis A very strong power analysis attack based on a statistical method to classify traces of power consumed during several algorithm runs.
EAL	Evaluation Assurance Level
EF	Elementary File
EMA	ElectroMagnetic Analysis Electromagnetic Analysis (EMA) attacks measure electromagnetic emissions from an IC during its operation and inferences to the data processed knowing such magnetic emissions is related to the logical value or the content of the processing.
fault injection	Fault injection is the attack dealing with the insertion or simulation of faults during the operation of Smart Card in order to infer the cryptographic key. Sometimes, such insertion of faults could affect destructive damage.
IAP	Initialize AP.Initializing the smart card.
IEF	Internal EF
invasive attacks	Invasive attacks start with the removal of the chip package. The direct access to the chip allows chip research or chip operation to steal private key.
JAP-DF	DF named “JAP-DF”.
JCD-AP	The application named “JCD-AP”. “JCD-AP” has its own life cycle.
MF	Master File
MPU	Memory Protection Unit The memory protection function provided by ST23YR80
perturbation attacks	Perturbation attacks change the normal behavior of an IC under the condition outside specification (voltage, frequency, temperature etc.) in order to create an exploitable error in the operation of a TOE.
physical manipulation	A kind of attack which destroys or manipulates the specific circuit (e.g. sensor circuit) on an IC chip.
PP	Protection Profile A document used as part of the certification process according to the Common

Terms	Definition
	Criteria (CC). A security requirement specification for security. The security description described in it is independent from implementation and satisfies user's requirements.
probing	An invasive attack to read signals (information) by establish electrical contact with on-chip bus lines without damaging them using micro-prober etc
RNG	Random Number Generator
SFR	Security Functional Requirement
SPA	Simple Powering Analysis Simple power analysis is a form of side channel attack in which the attacker studies the power consumption of a cryptographic hardware device in order to extract cryptographic keys and other secret information from the device.
ST	Security Target
TOE	Target of Evaluation
TRNG	True Random Number Generator
TSF	TOE Security Functionality
TSF data	The data generated by TOE or those generated in connection with TOE, which may affect the behaviors of TOE.
WEF	Working Elementary File
Integer data	The data whose integrity must be fully protected
Object	The passively acting entity which receives or stores information and is the object of the operations by a subject.
Card AP	The processing definitions and information required for using card application services.
Confidential data	The data which needs to be kept confidential
Subject	The actively acting entity which performs operation on the Object.
Brute Force Attack	Brute Force Attack A strategy used to break the encryption of data which involves traversing the search space of possible keys until the correct key is found.
User Data	The data generated by a user or those generated in connection with a user, which may affect the behaviors of TSF.
Lifecycle	Concept that presents the cyclical nature from birth, development, maturity and deterioration, of families, organizations etc. For Smart Card, it can mean the life cycle from manufacturing to disposal (card life cycle), the life cycle from the generation of applications to their deletion of multi-purpose card (AP life cycle) and a file life cycle.
ICAO	International Civil Aviation Organization
ePassport	A ePassport is a passport with IC chip to prevent forgery.
passport	A passport is an identification document, issued by government or public organization, which certifies, for the purpose of international travel, the identity of its holder, generally in a booklet(passport-booklet form)
Immigration official	At immigration, the immigration official inspects the passport booklet using a passport inspection terminal.
MRTD	Machine readable travel document
Active Authentication	Security mechanism, by which means the public key and private key pair based on the public key encryption system is stored and the private key is kept secret in the IC chip that is a part of the TOE. The public key is delivered to an external device trying to authenticate the TOE and the TOE is authenticated through cryptographic calculation by the challenge response system using the private key, which has been kept a secret in the TOE. The active authentication procedure has been standardized by ICAO.
Application note	Optional informative part of the PP containing additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created

Terms	Definition
	by the issuing State or Organization
Basic Access Control	Security mechanism defined in [7] by which means the MTRD's chip proves and the inspection system protect their communication by means of secure messaging with Basic Access Keys (see there).
Inspection terminal	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is a integrated circuit.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means.
Eavesdropper	A threat agent with low attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait.
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
Inspection	The act of a State examining an MRTD presented to it by a traveller (the MRTD holder) and verifying its authenticity. [9]
Integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer).
Issuing state	The Country issuing the MRTD.
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods.
Application software	ePassport application software
holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
ePassport IC Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.
Passive authentication	Security mechanism, by which the digital signature of the passport issuing authority is put on personal information data stored in the TOE, and the authenticity of data read from the TOE is verified by using the PKI system with assured interoperability both on the passport issuing and receiving sides. The passive authentication procedure has been standardized by ICAO.
Personalization	The process by which the portrait, signature and biographical data are applied to the document.
Personalization Agent	The agent acting on the behalf of the issuing State or organisation to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.
Pre-personalization	Any data that is injected into the non-volatile memory of the TOE by the MRTD

Terms	Definition
Data	Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Keys.
Receiving State	The Country to which the MRTD holder is applying for entry.
reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
secure messaging	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1).
User data	Data created by and for the user, that does not affect the operation of the TSF (CC part 1).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template.

9.2. Reference Materials

Table 9-2: Reference Materials

Identifier	Document Name
[CC1]	Common Criteria for Information Technology Security Evaluation Version 3.1, Part 1: Introduction and general model Revision 3 (CCMB-2009-07-001)
[CC2]	Common Criteria for Information Technology Security Evaluation Version 3.1, Part 2: Introduction and general model Revision 3 (CCMB-2009-07-002)
[CC3]	Common Criteria for Information Technology Security Evaluation Version 3.1, Part 3: Introduction and general model Revision 3 (CCMB-2009-07-003)
[CEM]	Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 3 (CCMB-2009-07-004)
[PP-ESforSSD]	Protection Profile Embedded Software for Smart Secure Devices Basic and Extended Configurations, Version 1.0, 27th November 2009
[PP-AA]	Protection Profile for Passport Booklet IC with Active Authentication,Version 1.00 February 15, 2010
[CRYPTO]	MécaniSMes cryptographiques. Règles et recommendations concernant le choix et le dimensionnement deSMécaniSMes cryptographiques. Version 1.11, 24 October 2008, ANSSI.
[STSTM]	ST23YR80A Security Target – Public Version, SMD_ST23YR80_ST_09_001 Rev1.00, February 2009, STMicroelectronics.
[ICAO Doc]	ICAO Doc9303 Machine Readable Travel Documents Part1 Machine Readable Passports Sixth Edition Volume1and 2 SUPPLEMENT to Doc9303-Part1-Sixth Edition Release7
[CCDB1]	Composite product evaluation for Smart Cards and similar devices, September 2007, Version 1.0 Revision 1 (CCDB-2007-09-001)
[CCDB2]	Application of Attack Potential to Smartcards, March 2009, Version 2.7 Revision 1 (CCDB-2009-03-001)
[AIS31]	Functionality classes and evaluation methology for physical random number generators, reference :AIS31 version 1, 25/09/2001, BSI
[FIPS140-2]	Federal Information Processing Standards Publication 140-2 Security Requirements for Cyptographic Modules, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2001 May 25 – standard for a Security Level 3 cryptographic module(statistical test upon demand)
[FIPS180-2]	Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD (+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1
[ISO9796-2]	ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002
[ISO14443]	ISO/IEC 14443-3(2001) Identification cards — Contactless integrated circuit(s) cards — Proximity Cards — Part 3: Initialization and anti-collision ISO/IEC 14443-4(2001) Identification cards — Contactless integrated circuit(s) cards — Proximity cards —Part 4: Transmission protocol