MASKTECH

SECURITY TARGET

COMMON CRITERIA DOCUMENTS | Version 1.1

Xaica-α PLUS ePassport on MTCOS Pro 2.5 with SAC (PACE) and Active Authentication / ST31G480 D01

Certification-ID: BSI-DSZ-CC-1073-V2

Public Version

MaskTech International GmbH | Nordostpark 45 | Nuernberg | www.masktech.com | +49 (0)911 95 51 49-0

Contents

1 ST Introduction

1.1 ST and TOE Reference

Title	Security Target – Xaica-α PLUS ePassport on MTCOS Pro 2.5 with SAC (PACE) and Active Authentication / ST31G480 D01
Version number	1.1
Issue Date	2020-07-17
Author	MaskTech International GmbH
Sponsor	NTT Data Corporation
Developer	MaskTech International GmbH
Registration	BSI-DSZ-CC-1073-V2
CC Reference	3.1 (Revision 5)
Compliant to	Protection Profile for ePassport IC with SAC (PACE) and Active Authentication (JISEC C0499)
Assurance Level	The assurance level for this ST is EAL4 augmented
TOE name	Xaica-α PLUS ePassport on MTCOS Pro 2.5 with SAC (PACE) and Active Authentication / ST31G480 D01
TOE hardware	STMicroelectronics, ST31G480 D01, smartcard IC including cryptographic library Neslib 6.2.1
TOE version	MTCOS Pro 2.5
Key Words	Smart card, IC card, ePassport, Supplemental Access Control (SAC), PACE, Active Authentication

N The notation “Xaica-α” may be substituted by the notation “Xaica-Alpha” to prevent potential coding errors as they may occur if displayed on e.g. a web site. Both notations are equivalent.

1.2 TOE Overview

1.2.1 TOE Types

The TOE is ePassport IC (including necessary software). This ePassport IC is composed of IC chip hardware with the contactless communication interface, and basic software (operating system) and ePassport application program that are installed in the said hardware (hereinafter, the term an “IC chip” shall mean an “ePassport IC”). An external antenna is connected to the IC chip for contactless communication purpose, and the IC chip is embedded in the plastic sheet together with the antenna to constitute a portion of a passport booklet.

1.2.2 TOE description

The TOE addressed by this Security Target is an *ePassport IC* including the necessary software. It comprises of:

- the integrated circuit (IC) ST31G480 D01 by STMicroelectronics,
- the basic software (operating system, OS) MTCOS Pro 2.5 implemented on the IC,
- the ePassport application software,
- the configuration script and
- the associated guidance documentation [AGD].

The IC hardware ST31G480 D01 including the cryptographic library Neslib 6.2.1 provides basic functionality, among others the contactless communication interface, and low-level security features (e.g. random number generator, 3DES-, AES and EC-support). It is certified (ANSSI-CC-2019/12) according to CC EAL5 augmented compliant to the Protection Profile [CC_PP-0084].

MTCOS Pro is a fully interoperable multi-application smart card operating system compliant to [ISO_7816]. It provides the high-level cryptography and the basic functionality for the secure usage of the product.

The ePassport application uses the basic functionality of the OS to provide the specific ePassport functionality. It is developed according to the Logical Data Structure (LDS) compliant to [ICAO_9303].

N The TOE is configured for an antenna capacitance of either 20 pF or 68 pF. The configuration is done during production. This difference is not security-relevant, thus both variants are taken as one single configuration.

The ePassport is viewed as unit of

the physical part of the ePassport in form of the IC sheet/booklet and chip. It presents visual readable data including (but not limited to) personal data of the Passport Holder

1. the biographical data on the biographical data page of the travel document surface,
2. the printed data in the Machine Readable Zone (MRZ) and
3. the printed portrait.

the logical ePassport as data of the Passport Holder stored according to the Logical Data Structure as defined in [ICAO_9303] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the Passport Holder

1. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
2. the digitized portraits (EF.DG2),
3. the other data according to LDS (EF.DG13 to EF.DG15) and
4. the Document Security Object (SOD).

1.2.3 TOE Usage and Main Security Functions

A passport is an identification document issued by each country's government or equivalent public organization, which certifies, for the purpose of international travel, the identity of its holder, generally in a booklet form (passport booklet). The International Civil Aviation Organization (ICAO) of the United Nations has provided the passport booklet guidelines. As for conventional passports, all information necessary as the identification was printed on a paper booklet, and thereby this could cause these passports to be forged for illicit purposes. In order to prevent such forgery, an IC chip containing personal information with digital signature has been incorporated in a passport booklet. Since valid digital signature can be granted only by the official passport issuing authorities, a high level of forgery prevention can be achieved. However, digital signature is not enough to counter forgery of copying personal information with authorized signature to store such information on a different IC chip.

This type of forgery attack can be countered by adding the Active Authentication function to the IC chip and verifying the authenticity of the IC chip with the use of the said function.

The TOE is embedded in a plastic sheet and then interfiled in a passport booklet. At immigration, the immigration official inspects the passport booklet using a passport inspection terminal (hereinafter a "terminal"). Aside from the information printed on the passport booklet in ordinary characters, the same information is encoded, printed on the machine readable zone (MRZ) of the passport booklet, and read by the optical character reader of the terminal. The information is digitized[1] and is stored in the IC chip, i.e., the TOE. These digitalized data are read by the terminal through the contactless communication interface of the TOE. The digitalized data include facial images.

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

The main security functions of the TOE are to protect data stored in the TOE from illicit reading or writing. The operation of the security functions applied to contactless communi-

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

cation with the terminal shall comply with the PACE, and Active Authentication specifications defined by Part 11 of Doc [ICAO_9303].

Attacks on protected data in the TOE include those through the contactless communication interface of the TOE and those attempting to disclose internal confidential information (Active Authentication Private Key) through physical attacks on the TOE.

The TOE provides the main security functions, including:

- PACE function (mutual authentication and Secure Messaging);
- Active Authentication support function (prevention of copying the IC chip);
- Write protection function (protection on writing data after issuing a passport);
- Protection function in transport (protection against attacks during transport before issuing the TOE); and
- Tamper resistance (protection against confidential information leak due to physical attacks).

1.2.4 TOE Life Cycle

The TOE life cycle is described below to clarify the security requirements for the TOE. The TOE life cycle of general IC chips is often described in terms of seven phases in the life cycle. As for the ePassport IC, however, the life cycle is divided into four phases instead of seven.

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) and embedding it together with antenna in the plastic sheet

Phase 3 (Personalization): Production of a passport booklet and writing of personal data

Phase 4 (Operational Use): Use of the TOE by the Passport Holder in operational environment

Phase 1 Phase 1 is a development phase:

STMicroelectronics develops the IC chip hardware, the IC Dedicated Software and the associated guidance documentation.

MaskTech International GmbH develops the basic software (operating system) using the IC guidance documentation, the ePassport application software and the associated guidance documentation.

In phase 1, threats in the operational environment are not considered, but proper development security shall be maintained to protect the confidentiality and integrity of development data. Security related to the TOE in the development phase is evaluated as the development security in assurance requirements. The TOE security functions are still not validly operational in the development phase.

All sites maintain a secure development environment.

The basic software and the application software is securely delivered from MaskTech International GmbH to STMicroelectronics.

Phase 2 Phase 2 is a manufacturing phase.

STMicroelectronics The hardware for the IC chip is manufactured, and operating system and application software for passport are installed in this hardware. A file object necessary for an ePassport is created in the TOE and an IC chip identification serial number is written into the file object. The functional tests of the internal circuit of the IC chip are conducted before the IC chip is sealed (i.e. the Flash Loader is deactivated). After that, only the contactless communication interface becomes available as an external interface.

The manufactured IC is securely delivered from STMicroelectronics to the IC Sheet Manufacturer.

IC Sheet Manufacturer The manufactured IC chip is embedded in the plastic sheet together with the contactless communication antenna. The IC Sheet Manufacturer changes the transport key and writes the readout key and Active Authentication Information Access Key in agreement with the Booklet Manufacturer. Furthermore, he configures the PACE-key, writes the serial number of the sheet into DG13 and writes temporary user data for functional testing. In the following, this process is denoted *personalization (pre-issuance)*.

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

The TOE is issued to the passport issuing authorities[2].

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

Booklet Manufacturer The TOE is interfiled in the ePassport booklet and information necessary for ePassport is written therein. This information includes the personal information of the passport holder (e.g. name, information on birth and so on) and cryptographic key used by the security functions. In the following, this process is denoted *personalization (post-issuance)*.

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

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

[2] In Japan, the Ministry of Foreign Affairs of Japan and the passport manufacturer and regional passport offices under its direction fall under the authorities. The passport manufacturer interfiles a TOE embedded plastic sheet in a passport booklet and configures necessary data other than personal information (e.g. date of birth, facial image data, and data for security related to the said data). Regional passport offices configure passport data related to personal information.

In phase 4, no information stored in the TOE is altered or deleted. The TOE security function protects the information necessary for immigration procedures against illicit reading, unless the information is read by an **Authorized Terminal**. The private key for Active Authentication is only used for the internal processing of the TOE and will never be readout to anywhere other than the TOE. The TOE security functions protect the information assets in the TOE against external unauthorized access.

Note 1: All steps performed by STMicroelectronics in life cycle phases 1 and 2 including the delivery from STMicroelectronics to the IC Sheet Manufacturer are covered by ANSSI-CC-2019/12. The development of the software and associated documentation performed by MaskTech International GmbH in life cycle phase 1 is examined under the ALC assurance of this certification, while the activites of the IC Sheet Manufacturer in life cycle phase 2 and of the Booklet Manufacturer in life cycle phase 3 are examined under the AGD assurance.

Delivery Naming Conventions In this ST the terms **delivery** and **delivered** are used to describe the transport of hardware, software or guidance documentation within the life cycle phases 1 and 2:

- software (basic software, application software and transport key) from MaskTech International GmbH to the IC manufacturer STMicroelectronics
- IC including all software from the STMicroelectronics to the IC Sheet Manufacturer
- configuration script and transport key from MaskTech International GmbH to the IC Sheet Manufacturer
- guidance documentation from MaskTech International GmbH to the IC Sheet Manufacturer

The term **issuance** and **issued** are used to describe the transport of of hardware, software or guidance documentation between the life cycle phases 2 and 3 or phases 3 and 4, respectively:

- IC sheet from the IC Sheet Manufacturer to the Booklet Manufacturer
- key data from the IC Sheet Manufacturer to the Booklet Manufacturer (or *vice versa*, if the Booklet Manufacturer provides the keys)
- guidance documentation from the IC Sheet Manufacturer to the Booklet Manufacturer
- the personalized ePassport from the Booklet Manufacturer to the Passport Holder

2 Conformance Claim

2.1 CC Conformance Claim

CC, to which this ST conforms, are identified. The ST conforms to the following CC V3.1:

- Part 1: Overview and the General Model; April 2017, Version 3.1 Revision 5, CCMB-2017-04-001 [CC_Part1]
- Part 2: Security Functional Components; April 2017, Version 3.1 Revision 5, CCMB-2017-04-002 [CC_Part2]
- Part 3: Security Assurance Components; April 2017, Version 3.1 Revision 5, CCMB-2017-04-003 [CC_Part3]
- Conformance to CC Part 2: CC part 2 extended
- Conformance to CC Part 3: CC part 3 conformant
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; April 2017, Version 3.1 Revision 5 CCMB-2017-04-004 [CC_PartEM]

2.2 PP Claim

This ST complies substantially to 'Protection Profile for ePassport IC with SAC (PACE) and Active Authentication', version 1.00, [CC_PP-C0499] (English translation), which requires strict compliance. For formal reasons no strict conformance to the original Japanese Protection Profile is claimed, because the English translation of [CC_PP-C0499] is not officially certified.

2.3 Package Claim

- In [CC_PP-C0499], the assurance requirement package applicable to the TOE is EAL4 augmented.
- Assurance components augmented are ALC_DVS.2 and AVA_VAN.5.

2.4 Conformance Rationales

The ST claims no conformance to other PP and thereby provides no description of conformance rationales.

2.5 PP Additions

The following items have been expanded or added, respectively, to those addressed in [CC_PP-C0499]:

Threat

- T.Physical_Attack (expanded to emphasize the threat of exploitment of information leakage and to include secret cryptographic keys other than the Active Authentication Private key)

Organizational Security Policies

- P.Personalization (added to address the security policy for personalization)

Security Objective

- O.Logical_Attack (expanded to include the protection of all secret cryptographic keys)
- O.Physical_Attack (expanded to include the protection against exploitment of information leakage and to include secret cryptographic keys other than the Active Authentication Private key)
- OE.Personalization (added to address the objective for personalization)

Security Functional Requirement

- FCS_RND.1 (changed with regard to the SFR given in [CC_PP-C0499] in order to provide detailed information; see also chapter 5)
- FPT_EMS.1 (added to address TOE emanation; see also chapter 5)

3 Security Problem Definition

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

The threats, organizational security policies, and assumptions are named using an identifier with the prefix “T.,” “P.,” or “A.,” respectively.

3.1 Users and Assets

The following Users are defined:

User	Description	Related to Subject[1]
IC Sheet Manufacturer	Embedding of the IC to the plastic sheet and applying the antenna (not within the scope of this certification); performing pre-issuance personalization	User Process
Booklet Manufacturer	Including the IC sheet into the passport booklet; performing post-issuance personalization	User Process
Authorized Terminal	Interface for reading the passport in phase 4	Process on behalf of terminal
Passport Holder	Person for whom the passport has been personalized	Process on behalf of terminal

Table 3.1: User definition.

The following assets are defined:

[1] as defined in section 6.1

Asset	Description	Properties to be maintained
User data	Personal data of the passport holder **Related Objects**: Files EF.DG[1, 2, 13], EF.COM	Confidentiality, Integrity, Authenticity
Secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality **Related Objects**: transport key, readout key, Active Authentication Information Access key, password key, Active Authentication private key	Confidentiality, Integrity
Non-secret key material	Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material used by the TOE in order to enforce its security functionality. **Related Objects**: EF.DG[14, 15], EF.SOD	Integrity, Authenticity

Table 3.2: Asset definition and relationship to Objects.

3.2 Threats

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

T.Copy

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

Note 2: If information retrieved from the legitimate TOE is copied into an illicit IC chip, as information stored in the TOE will be copied together with the associated digital signature, forgery protection by means of digital signature verification becomes ineffective. Since the original information can be protected against tampering by means of digital signature, passport forgery may be detected by means of comparative verification of the facial image. However, it is difficult to surely detect forged passport just by comparing the facial image.

T.Logical_Attack

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

Note 3: If an attacker has physical access to a passport booklet, the attacker can visually read personal information printed on the passport booklet and optically read the printed MRZ data. Since the security functions of the TOE cannot prevent such sort of

readings, the information and data stated above is not included in the threat-related assets to be protected by the TOE. In other words, the intended meaning of the threat here is an attack aimed to read confidential information (Active Authentication Private Key) stored in the TOE by having access to the said TOE through the contactless communication interface using data that the attacker has read from the MRZ.

T.Communication_Attack

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

Note 4: As for an attack which interferes with communication between a terminal and a passport booklet, it is considered impossible that the attacker physically accesses the target passport booklet without being noticed by the passport holder and/or an immigration official. An attacker can obtain MRZ data only when the passport booklet is physically accessible. Therefore, the attacker mentioned here is assumed to be unaware of the MRZ data.

T.Physical_Attack

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

Furthermore, an attacker may exploit information leaking from the TOE during its usage in order to disclose confidential user data or/and confidential information (secret cryptographic keys) stored on the TOE or/and exchanged between the TOE and the terminal connected. The information leakage may be inherent in the normal operation or caused by the attacker.

Note 5: An attacker may attempt to read confidential information (secret cryptographic keys) or rewrite information stored in the TOE through physical access to the TOE. Making such a physical attack may impair the security function operated by the TOE program to provide the original functionality thereof, resulting in potential violation of SFR. The example of nondestructive attacks includes measurements on leaked electromagnetic wave associated with the TOE operation and induction of malfunctions in security functions by applying environmental stress (e.g. changes in temperature or clock, or application of high-energy electromagnetic fields) to the TOE in operation. The example of destructive attacks shows those collecting, analyzing, and then disclosing confidential information by probing and manipulating the internal circuit. Test pins and power supply pins left in the TOE may be used to make the said attacks. The TOE that has been subject to a destructive attack may not be reused as an ePassport IC. Even in such case, however, the disclosed private key may be abused to forge TOEs.

Note 6: T.Physical_Attack from [CC_PP-C0499] has been expanded to emphasize the threat emerging from information leaking from the TOE during regular operational usage. Beside the Active Authentication Private key an attacker may disclose other secret cryptographic keys (PACE-key) and confidential user data.

3.3 Organizational Security Policies

This section describes organizational security policies that apply to TOEs and operational environment. In [CC_PP-C0499], the organizational security policies include conformance to the standards provided by ICAO and conditions required by the passport issuing authorities in Japan.

P.PACE

In the operational environment after issuing a TOE embedded passport booklet, the TOE shall allow a terminal to read a certain information from the TOE in accordance with the PACE procedure defined by Part 11 of [ICAO_9303]. This procedure includes mutual authentication and Secure Messaging between the TOE and terminal devices. TOE files to be read are EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, and EF.SOD under the rules stated above. As for any files under the same rules except the files stated above, the handling of such files which are not listed in this ST is not defined.

P.Authority

The TOE under the control of the passport issuing authorities shall allow only authorized users (persons who succeeded in verification of readout key, transport key, or Active Authentication Information Access Key) to have access to the internal data of the TOE, as shown in Table 3.3.

Authentication status[*1]	File subject to access control	Operation permitted	Reference: Data to be operated
Successful verification with readout key	EF.DG13[*2]	Read	IC chip serial number (entered by manufacturer)
Successful verification with transport key	Transport key file	Write	Transport key data (update of old data)
	Password key file		Password key
	EF.DG1	Read or Write	MRZ data
	EF.DG2		Facial image
	EF.DG13[*2]		Management data (Passport number and Booklet management number)
	EF.DG14		PACE v2 Security information Active Authentication hash function information
	EF.COM[*3]		Common data
	EF.SOD		Security data related to Passive Authentication defined by Part 10 of [ICAO_9303].
	EF.CardAccess	Write	PACE v2 Security information
	EF.DG15	Read	Active Authentication Public Key
Successful verification with Active Authentication Information Access Key	EF.DG15	Write	Active Authentication Public Key
	Private key file		Active Authentication Private Key

Table 3.3: Internal data of the TOE access control by passport issuing authorities.

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

[*2] In EF.DG13, an IC chip serial number has been recorded by the manufacturer (IC Sheet Manufacturer), and the management data is appended to the file by the passport issuing authorities (Booklet Manufacturer).

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

Note 7: All files stated in the table above store user data or TSF data. The transport key file stores TSF data, and all other files store user data (cryptographic keys are managed as user data). The TSF data file is not included in files subject to access control stated in Section 6.1 “Security Functional Requirements,” but treated in FMT_MTD.1.

Note 8: Note that the transport key, the readout key and the Active Authentication Information Access key are realized as passwords.

P.Data_Lock

When the TOE detects a failure in authentication with the transport key, readout key or Active Authentication Information Access Key, it will permanently disable authentication related to each key, thereby prohibiting reading or writing the file based on successful authentication thereof. Table 3.3 shows the relationship between the key used for authentication and its corresponding file in the TOE.

P.Prohibit

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

P.Personalization

The passport issuing authority guarantees the correctness of the biographical data, the printed portrait and the digitized portrait and other data of the ePassport with respect to the Passport Holder. The personalization of the ePassport for the Passport Holder is performed by an agent authorized by the passport issuing authority only.

Note 9: This policy has been taken from [CC_PP-0056-V2] and adapted to match the wording conventions of this ST.

3.4 Assumptions

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

A.Administrative_Env

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

A.PKI

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

4 Security Objectives

This chapter describes security objectives for TOEs and its environment for the security problems described in Chapter 3. Section 4.1 describes the security objectives to be addressed by the TOEs, while Section 4.2 describes those to be addressed by its environment. In addition, Section 4.3 describes rationales for the appropriateness of the security objectives for solving the security problems. The security objectives for the TOEs and the security objectives for the operational environment are represented by an identifier with the prefix “O.” or “OE.” respectively.

4.1 Security Objectives for the TOE

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

O.AA

TOEs shall provide a means to verify the authenticity of the IC chip itself that composes the TOE in order to prevent the copy of personal information including the digital signature on an illicit IC chip and the forgery of the passport. This means shall be standardized so as to ensure the global interoperability of ePassport and, for this purpose, shall support the Active Authentication defined by Part 11 of [ICAO_9303].

O.Logical_Attack

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

Note 10: O.Logical_Attack has been expanded to address the protection of all secret cryptographic keys.

O.Physical_Attack

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

Furthermore, he TOE must provide protection against disclosure of confidential user data or/and confidential information (secret cryptographic keys) stored and/or pro-

cessed by the travel document by exploitment of information leakage during regular operational usage.

Note 11: O.Physical_Attack from [CC_PP-C0499] has been expanded to address protection against any disclosure by information leaking from the TOE during regular operational usage.

O.PACE

This security objective applies to the operational environment after issuing the passport booklet. PACE procedure defined by Part 11 of [ICAO_9303], if the terminals require, shall be used to ensure the global interoperability of the ePassport. This procedure shall be used in the mutual authentication and Secure Messaging between the TOE and terminals.

Information the terminal reads from the TOE is stored in the EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, and EF.SOD files among the files contained in the rules stated above. The TOE shall permit only the terminal that has succeeded in mutual authentication to read the files stated above. As for any files under the same rules except the files stated above, the handling of such files which are not listed in this ST is not defined.

O.Authority

The TOE shall limit users who can access the internal TOE data and their operations, in the environment under the control of the passport issuing authorities according to Table 3.3 described in the organizational security policy P. Authority.

O.Data_Lock

The operation of the internal TOE data shall be available only to the authorized user (i.e., authorized personnel under the control of the passport issuing authorities or the terminal after issuing the passport) to prevent illicit reading and writing by any users other than those stated above. As a means for this purpose, if the TOE detects an authentication failure with the readout key, transport key, or Active Authentication Information Access Key, it shall be permanently prohibited to read or to write the internal TOE data permitted according to authentication related to each of the said keys. This security objective shall also apply in the event that the passport issuing authorities disable readout key, transport key, or Active Authentication Information Access Key by causing an authentication failure intentionally before the TOE is issued to the passport holder. The relationship between the readout key, transport key, and Active Authentication Information Access Key and their corresponding internal TOE data is as listed in Table 3.3 of the organizational security policy P.Authority. After the security objective O.Data_Lock is achieved, only the access to TOE stated in the security objective O.PACE is permitted.

4.2 Security Objectives for the Operational Environment

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

OE.Administrative_Env

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

OE.PKI

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

OE.Personalization

The passport issuing authority must ensure that the Booklet Manufacturer acting on his behalf (i) establish the correct identity of the Passport Holder and create the biographical data for the ePassport, (ii) enroll the biometric reference data of the Passport Holder, (iii) write a subset of these data on the physical Passport (optical personalization) and store them in the ePassport (electronic personalization) for the Passport Holder as defined in [ICAO_9303], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the document security object defined in [ICAO_9303].

The IC Sheet Manufacturer and Booklet Manufacturer must ensure the confidentiality and integrity of all data by acting within a secure operational environment. Furthermore, all secret cryptographic keys or passwords to be personalized, respectively, must be of appropriate quality to prevent disclosure by trial and error.

Note 12: This policy has been taken from [CC_PP-0056-V2] and adapted to match the wording conventions of this ST and to emphasize the secure operational environment and the usage of secure values for secret cryptographic keys.

4.3 Security Objectives Rationales

This chapter describes rationales for the effectiveness of the security objectives stated above for individual parameters of the security problem definition. Section 4.3.1 describes that each of the security objective can be traced back to any of the security problems, while Section 4.3.2 describes that any of the security problems is effectively addressed by the corresponding security objective.

4.3.1 Correspondence between Security Problem Definition and Security Objectives

Table 4.1 shows the correspondence between the security problem definition and the security objectives. As shown in the table, all security objectives can be traced back to one (or more) item(s) in the security problem definition.

Security problem definition / Security objective	O.AA	O.Logical_Attack	O.Physical_Attack	O.PACE	O.Authority	O.Data_Lock	OE.Administrative_Env	OE.PKI	OE.Personalization
T.Copy	x								x
T.Logical_Attack		x							
T.Communication_Attack				x					
T.Physical_Attack			x						
P.PACE				x					
P.Authority					x				
P.Data_Lock						x			
P.Prohibit						x			
P.Personalization					x				x
A.Administrative_Env							x		
A.PKI								x	

Table 4.1: Correspondence between security problem definition and security objectives

4.3.2 Security Objectives Rationale

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

T.Copy

If an attacker copies the personal information (with digital signature) read from the TOE to the IC chip having the same functionality as that of the TOE, the forged passport cannot be detected through the verification of digital signature. To prevent this attack, the security objective for the TOE: O.AA and the security objective for the environment: OE.Personalization address embedding of data that enable verifying the authenticity of the IC chip itself in the TOE. This enables the TOE to detect illicit IC chips and prevent the forgery of passports, thus removing the threat of T.Copy.

Note 13: The TOE provides the precondition for the terminal to effectively verify integrity and authenticity of the data received from the TOE.

T.Logical_Attack

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

T.Communication_Attack

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

T.Physical_Attack

The security objective for the TOE: O.Physical_Attack makes it possible to counter an attack to disclose confidential information (secret cryptographic keys) in the TOE or tamper security-related information not via the contactless communication interface of the TOE but physical means. Regarding the physical means, both nondestructive attacks and destructive attacks are considered, and countermeasures shall be implemented so that the TOE can counter known attacks against the IC chip. Thus the threat can be diminished to an adequate level for the practical use.

Note 14: In addition to T.Physical_Attack and O.Physical_Attack from [CC_PP-C0499] the threat of exploitment of information leakage during regular operational usage and the protection against this threat has been addressed.

P.PACE

The security objective for the TOE: O.PACE allows only the authorized personnel (terminal) to read the internal TOE data through a secure communication path by applying PACE procedure defined by Part 11 of [ICAO_9303]. O.PACE includes all contents of P.PACE, thus the organizational security policy P.PACE is properly implemented.

P.Authority

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

P.Data_Lock

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

P.Prohibit

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

P.Personalization

The organizational security policy P.Personalization addresses the (i) the enrollment of the logical travel document by the Booklet Manufacturer as described in the security objective for the TOE environment OE.Personalization, and (ii) the access control for the user data and TSF data as described by the security objective O.Authority.

A.Administrative_Env

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

A.PKI

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

5 Extended Components Definition

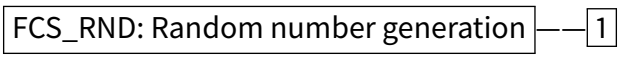
The extended component **FCS_RND** (Random number generation) as defined in [CC_PP-0084] (FCS_RNG) is used (replacing the extended component **FCS_RND** defined in [CC_PP-C0499]). In addition this ST uses the extended component **FPT_EMS** (TOE emanation), which is defined in [CC_PP-0068-V2].

5.1 FCS_RND: Random number generation

Family Behavior

This family defines quality requirements for the generation of random numbers which are intended to be use for cryptographic purposes.

Component leveling



FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management:	FCS_RND.1 There are no management activities foreseen.
Audit:	FCS_RND.1 There are no actions defined to be auditable.
FCS_RND.1	Random number generation
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RND.1.1	The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].
FCS_RND.1.2	The TSF shall provide [selection: *bits, octets of bits, numbers* [*assignment: format of the numbers*]] that meet [assignment: *a defined quality metric*].

5.2 FPT_EMS: TOE emanation

The family FPT_EMS (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 secret data stored in and used by the TOE 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 being not directly addressed by any other component of CC part 2 [CC_Part2].

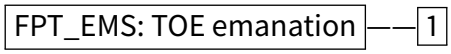
The family 'TOE Emanation (FPT_EMS)' is specified as follows:

FPT_EMS: TOE emanation

Family Behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling



FPT_EMS.1	TOE emanation has two constituents:
FPT_EMS.1.1	Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
FPT_EMS.1.2	Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.
Management:	FPT_EMS.1 There are no management activities foreseen.
Audit:	FPT_EMS.1 There are no actions defined to be auditable.

FPT_EMS.1	**TOE Emanation**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.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_EMS.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

6.1 Security Functional Requirements

Table 6.1 shows the list of the security functional requirements (SFRs) defined by the PP.

Chapter No.	Identifier name	
6.1.1	FCS_CKM.1p	Cryptographic key generation (PACE, session keys)
6.1.2	FCS_CKM.1e	Cryptographic key generation (PACE, ephemeral key pairs)
6.1.3	FCS_CKM.4	Cryptographic key destruction
6.1.4	FCS_COP.1a	Cryptographic operation (Active Authentication, signature generation)
6.1.5	FCS_COP.1h	Cryptographic operation (Active Authentication, hash functions)
6.1.6	FCS_COP.1n	Cryptographic operation (Nonce encryption)
6.1.7	FCS_COP.1e	Cryptographic operation (Key agreement)
6.1.8	FCS_COP.1hp	Cryptographic operation (PACE, hash functions)
6.1.9	FCS_COP.1mp	Cryptographic operation (PACE, mutual authentication)
6.1.10	FCS_COP.1sp	Cryptographic operation (PACE, Secure Messaging)
6.1.11	FCS_RND.1	Random number generation
6.1.12	FDP_ACC.1a	Subset access control (Issuance procedure)
6.1.13	FDP_ACC.1p	Subset access control (PACE)
6.1.14	FDP_ACF.1a	Security attribute based access control (Issuance procedure)
6.1.15	FDP_ACF.1p	Security attribute based access control (PACE)
6.1.16	FDP_ITC.1	Import of user data without security attributes
6.1.17	FDP_UCT.1p	Basic data exchange confidentiality (PACE)
6.1.18	FDP_UIT.1p	Data exchange integrity (PACE)
6.1.19	FIA_AFL.1a	Authentication failure handling (Active Authentication Information Access Key)

6.1.20	FIA_AFL.1d	Authentication failure handling (Transport key)
6.1.21	FIA_AFL.1r	Authentication failure handling (Readout key)
6.1.22	FIA_UAU.1	Timing of authentication
6.1.23	FIA_UAU.4	Single-use authentication mechanism
6.1.24	FIA_UAU.5	Multiple authentication mechanisms
6.1.25	FIA_UID.1	Timing of identification
6.1.26	FMT_MTD.1	Management of TSF data
6.1.27	FMT_SMF.1	Specification of management functions
6.1.28	FMT_SMR.1	Security roles
6.1.29	FPT_EMS.1	TOE Emanation
6.1.30	FPT_PHP.3	Resistance to physical attack
6.1.31	FTP_ITC.1	Inter-TSF trusted channel

Table 6.1: List of SFRs.

SFR is defined by performing as-needed operation on the security functional component defined by CC Part 2. The operation is denoted for each SFR by the following method:

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

The following section describes SFRs defined by [CC_PP-C0499].

6.1.1 FCS_ CKM.1p Cryptographic key generation (PACE, session keys)

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1p	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *session key generation algorithm in PACE specified by Part 11 of [ICAO_9303] and [BSI_TR-03111]*] and specified cryptographic key sizes [assignment: *128 bits and 256 bits*] that meet the following: [assignment: *Standards for session key generation in PACE specified by Part 11 of [ICAO_9303] and [BSI_TR-03111]*].

Note 15: Session key generation (PACE) is specified in Part 11 of [ICAO_9303], sec. 9.7.3 and [BSI_TR-03111], sec. 4.3.3.2.

6.1.2 FCS_CKM.1e Cryptographic key generation (PACE, ephemeral key pairs)

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1e	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *Elliptic Curve Key Pair Generation*] and specified cryptographic key sizes [assignment: *256 bits and 384 bits*] that meet the following: [assignment: *Standards for the key pair generation specified by [BSI_TR-03111]*].

Note 16: Cryptographic key generation for PACE (ephemeral key pairs) is specified in [BSI_TR-03111], sec. 4.1.3. The domain parameters NIST P-256 and NIST P-384 are used.

6.1.3 FCS_CKM.4 Cryptographic key destruction

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

Note 17: The TOE shall destroy cryptographic keys on volatile memory by overwriting the key data with random data.

6.1.4 FCS_COP.1a Cryptographic operation (Active Authentication, signature generation)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1a	The TSF shall perform [assignment: *generation of digital signature for Active Authentication data*] in accordance with a specified cryptographic algorithm [assignment: *ECDSA*] and cryptographic key sizes [assignment: *256 bits and 384 bits*] that meet the following: [assignment: the Digital Signature Standards specified by [BSI_TR-03111], [ICAO_9303], [ICAO_SAC]and [BSI_TR-03110-1]].

Note 18: Only the combination of 256 bits and SHA-256 or that of 384 bits and SHA-384 is permitted as the key sizes for this requirement and the hash algorithm of FCS_COP.1h.

Note 19: ECDSA signature generation is specified in [BSI_TR-03111], sec. 4.2.1 in conformance with [ANSI_X9.62], sec. 7. The domain parameters NIST P-256 and NIST P-384 are used.

6.1.5 FCS_COP.1h Cryptographic operation (Active Authentication, hash functions)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1h	The TSF shall perform [assignment: *generation of data for Active Authentication*] in accordance with a specified cryptographic algorithm [assignment: *SHA-256 and SHA-384*] and cryptographic key sizes [assignment: *none*] that meet the following: [assignment: *the Digital Signature Standards specified by [BSI_TR-03111]*].

Note 20: Cryptographic hash functions are specified in [BSI_TR-03111], sec. 4.1.2 and

[FIPS_180-4], sec. 6.2 (SHA-256) and sec. 6.5 (SHA-384).

6.1.6 FCS_COP.1n Cryptographic operation (Nonce encryption)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1n	The TSF shall perform [assignment: *nonce encryption*] in accordance with a specified cryptographic algorithm [assignment: *AES-CBC*] and cryptographic key sizes [assignment: *128 bits and 256 bits*] that meet the following: [assignment: *Standards for the PACE procedure specified by Part 11 of [ICAO_9303]*].

Note 21: Nonce encryption is specified in Part 11 of [ICAO_9303], sec. 4.4.3.3 according to [ISO_10116], sec. 7 (CBC mode).

6.1.7 FCS_COP.1e Cryptographic operation (Key agreement)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1e	The TSF shall perform [assignment: *key agreement*] in accordance with a specified cryptographic algorithm [assignment: *ECDH*] and cryptographic key sizes [assignment: *256 bits and 384 bits*] that meet the following: [assignment: *Standards for the PACE procedure specified by Part 11 of [ICAO_9303]*].

Note 22: Key agreement is specified in Part 11 of [ICAO_9303] and [BSI_TR-03111], sec. 4.3.2.1. The domain parameters NIST P-256 and NIST P-384 are used.

6.1.8 FCS_COP.1hp Cryptographic operation (PACE, hash functions)

Hierarchical to:	No other components.

Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1hp	The TSF shall perform [assignment: *generation of session keys for PACE*] in accordance with a specified cryptographic algorithm [assignment: *SHA-1 and SHA-256*] and cryptographic key sizes [assignment: *none*] that meet the following: [assignment: *Standards for session key generation in PACE specified by Part 11 of [ICAO_9303]*].

Note 23: Cryptographic hash functions are specified in Part 11 of [ICAO_9303], sec. 9.7.1.2, [BSI_TR-03111], sec. 4.1.2 and [FIPS_180-4], sec. 6.1 (SHA-1) and sec. 6.2 (SHA-256).

6.1.9 FCS_COP.1mp Cryptographic operation (PACE, mutual authentication)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1mp	The TSF shall perform [assignment: *authentication token generation and verification*] in accordance with a specified cryptographic algorithm [assignment: *AES-CMAC*] and cryptographic key sizes [assignment: *128 bits and 256 bits*] that meet the following: [assignment: *Standards for mutual authentication included in PACE specified by Part 11 of [ICAO_9303]*].

Note 24: PACE (mutual authentication) specified in Part 11 of [ICAO_9303], sec. 4.4; AES is specified in [FIPS_197], sec. 7, CMAC is specified on [NIST_SP800-38B], sec. 6.

6.1.10 FCS_COP.1sp Cryptographic operation (PACE, Secure Messaging)

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

FCS_COP.1.1sp	The TSF shall perform [assignment: *cryptographic operation shown in Table 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 PACE specified by [ICAO_9303]*].

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

Table 6.2: Cryptographic mechanisms in Secure Messaging (PACE).

Note 25: PACE (Secure Messaging) is specified in Part 11 of [ICAO_9303], sec. 9.8; AES is specified in [FIPS_197], CBC mode is specified in [ISO_10116], sec. 7, CMAC is specified on [NIST_SP800-38B], sec. 6.

Note 26: Whether Secure Messaging is applied or not depends on the type of commands. Therefore, data encryption and message authentication codes are not necessarily applied to all commands and responses.

6.1.11 FCS_RND.1 Random number generation

Hierarchical to:	–
Dependencies:	–

FCS_RND.1.1	The TSF shall provide a [selection: ~~*physical, non-physical true, deterministic,*~~ *hybrid physical*, ~~*hybrid deterministic*~~] random number generator that implements: [assignment *(PTG.3.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.* *(PTG.3.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG [selection: prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source~~, generates the internal random numbers with a post-processing algorithm of class DRG.3 as long as its internal state entropy guarantees the claimed output entropy~~].* *(PTG.3.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 post-processing algorithm have been finished successfully or when a defect has been detected.* *(PTG.3.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.* *(PTG.3.5) The online test procedure checks the raw random number sequence. It is triggered [selection: ~~externally, at regular intervals,~~ continuously~~, upon specified internal events~~]. The online test is suitable for detecting nontolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.* *(PTG.3.6) The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-processing algorithm shall not exceed its input data rate.*]
FCS_RND.1.2	The TSF shall provide [selection: ~~*bits,*~~ *octets of bits*, ~~*numbers [assignment: format of the numbers]*~~] that meet: [assignment *(PTG.3.7) Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A*[1] *[assignment: none].* *(PTG.3.8) The internal random numbers shall [selection: use PTRNG of class PTG.2 as random source for the postprocessing~~, have [assignment: work factor], require [assignment: guess work~~]].*

Note 27: This SFR has been changed according to [CC_PP-0084] (FCS_RNG.1) to specify the requirements given in [BSI_AIS31v3] for PTG.3.

[1] See [KiSch-RNG] Section 2.4.4.

6.1.12 FDP_ACC.1a Subset access control (Issuance procedure)

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1a	The TSF shall enforce the [assignment: *Issuance procedure access control SFP*] on [assignment: *Subject [User process], Objects [Files shown in Table 3.3 of Organizational security policy P.Authority] and List of operations among subjects and objects addressed by SFP [Data Input/Output operation to/from object]*].

6.1.13 FDP_ACC.1p Subset access control (PACE)

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1p	The TSF shall enforce the [assignment: *PACE SFP*] on [assignment: *Subject [Process on behalf of terminal], Objects [Files EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, EF.SOD, password key file, transport key file, and private key file] and list of operations among subjects and objects addressed by SFP [Reading data from object]*].

Note 28: PACE SFP is the access control policy applied after succeeding in mutual authentication based on PACE.

6.1.14 FDP_ACF.1a Security attribute based access control (Issuance procedure)

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1a	The TSF shall enforce the [assignment: *Issuance procedure access control SFP*] to objects based on the following: [assignment: *Subject controlled under the indicated SFP [User process], objects [Files shown in Table 3.3 of the organizational security policy P.Authority], and, the SFP-relevant security attributes [Authentication status shown in Table 3.3 of the organizational security policy P.Authority]* according to each].

FDP_ACF.1.2a	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *When the authentication status shown in Table 3.3 of the organizational security policy P.Authority is met, an operation to the file associated with the said authentication status is allowed*].
FDP_ACF.1.3a	The TSF shall explicitly 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: *Access to files that are not listed in Table 3.3 of the organizational security policy P.Authority is prohibited.*].

6.1.15 FDP_ACF.1p Security attribute based access control (PACE)

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

6.1.16 FDP_ITC.1 Import of user data without security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialization
FDP_ITC.1.1	The TSF shall enforce the [assignment: *Issuance procedure access control SFP*] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *none*].

6.1.17 FDP_UCT.1p Basic data exchange confidentiality (PACE)

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

6.1.18 FDP_UIT.1p Data exchange integrity (PACE)

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

6.1.19 FIA_AFL.1a Authentication failure handling (Active Authentication Information Access Key)

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1a	The TSF shall detect when [selection: *[assignment: 3], ~~an administrator configurable positive integer within [assignment: range of acceptable values]~~*] unsuccessful authentication attempts occur related to [assignment: *authentication with the Active Authentication Information Access Key*].
FIA_AFL.1.2a	When the defined number of unsuccessful authentication attempts has been [selection: *met, ~~surpassed~~*], the TSF shall [assignment: *permanently stop authentication with the Active Authentication Information Access Key (fix the authentication status with the Active Authentication Information Access Key to "Not authenticated yet")*].

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

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1d	The TSF shall detect when [selection: *[assignment: 3], ~~an administrator configurable positive integer within [assignment: range of acceptable values]~~*] unsuccessful authentication attempts occur related to [assignment: *authentication with the transport key*].
FIA_AFL.1.2d	When the defined number of unsuccessful authentication attempts has been [selection: *met, ~~surpassed~~*], the TSF shall [assignment: *permanently stop authentication with the transport key (fix the authentication status with the transport key to "Not authenticated yet")*].

6.1.21 FIA_AFL.1r Authentication failure handling (Readout key)

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

FIA_AFL.1.1r	The TSF shall detect when [selection: *[assignment: 3]*, ~~*an administrator configurable positive integer within [assignment: range of acceptable values]*~~] unsuccessful authentication attempts occur related to [assignment: *authentication with the readout key*].
FIA_AFL.1.2r	When the defined number of unsuccessful authentication attempts has been [selection: *met,* ~~*surpassed*~~], the TSF shall [assignment: *permanently stop authentication with the readout key (fix the authentication status with the readout key to "Not authenticated yet")*].

6.1.22 FIA_UAU.1 Timing of authentication

Hierarchical to:	No other components
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1	The TSF shall allow [assignment: *readout of EF.CardAccess and EF.ATR/INFO*], on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.23 FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to [assignment: *mutual authentication mechanism with the PACE procedure*].

6.1.24 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1	The TSF shall provide [assignment: *multiple authentication mechanisms shown in Table 6.3*] 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 6.3 provide authentication*].

Authentication mechanism name	Rule applicable to authentication mechanism
Transport key	Rule of authenticating the authorized personnel of the passport issuing authorities by verifying transport key that have been already stored in the TOE
Readout key	Rule of authenticating the authorized personnel of the passport issuing authorities by verification with readout key that have been already stored in the TOE
Active Authentication Information Access Key	Rule of authenticating the authorized personnel of the passport issuing authorities by verification with Active Authentication Information Access Key that have been already stored in the TOE
Mutual authentication	Rule of authenticating terminals according to the mutual authentication procedure in PACE defined by [ICAO_9303]

Table 6.3: Multiple authentication mechanisms

6.1.25 FIA_UID.1 Timing of identification

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow [assignment: *readout of EF.CardAccess and EF.ATR/INFO*], on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.26 FMT_MTD.1 Management of TSF data

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
FMT_MTD.1.1	The TSF shall restrict the ability to [selection: ~~*change_default, query,* modify, *delete, clear, [assignment: other operations]*~~] the [assignment: *transport key*] to [assignment: *the authorized personnel of the passport issuing authorities*].

Note 29: This requirement has to do with the configuration of transport key used to transport the TOE from the passport booklet manufacturer to a regional passport office in Phase 3. In this requirement, the authorized personnel who are allowed to manage TSF data are the staff of the passport manufacturer. The staff has no chance to rewrite the transport key

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

6.1.27 FMT_SMF.1 Specification of management functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [assignment: *modification of transport key*].

6.1.28 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles [assignment: *authorized personnel of the passport issuing authorities*].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.1.29 FPT_EMS.1 TOE Emanation

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit [assignment: *information about IC power consumption and command execution time*] in excess of [assignment: *non-useful information*] enabling access to [assignment: 1. *PACE session keys*, 2. *the PACE ephemeral private key*] and [assignment: 3. *Transport key*, 4. *Readout key*, 5. *Active Authentication Information Access key*, 6. *Active Authentication Private key*].

FPT_EMS.1.2	The TSF shall ensure [assignment: *any users*] are unable to use the following interface [assignment: *smart card circuit contacts*] to gain access to [assignment: 1. *PACE session keys*, 2. *the PACE ephemeral private key*] and [assignment: 3. *Transport key*, 4. *Readout key*, 5. *Active Authentication Information Access key*, 6. *Active Authentication Private key*].

Note 30: SFR FPT_EMS.1 is taken in addition to the SFRs from [CC_PP-C0499] (see also chapter 5); the SFR applies to life cycle phase 4.

6.1.30 FPT_PHP.3 Resistance to physical attack

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF shall resist [assignment: *attacks defined by the CC Supporting Documents related to Smartcards*] to the [assignment: *hardware of the TOE and software composing the TSF*] by responding automatically such that the SFRs are always enforced.

Note 31: The supporting documents that are the latest version at the time of the evaluation for the TOE are applied. The document at the time of [CC_PP-C0499] issuance is the [JIL_AP].

6.1.31 FTP_ITC.1 Inter-TSF trusted channel

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

FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [assignment: *reading data from the TOE*].

Note 32: Communication between terminal and TSF shall be performed via the Secure Messaging channel defined by [ICAO_9303]. After the Secure Messaging channel is established, only the Secure Messaging channel is to be available for the communication path between terminal and TOE.

6.2 Security Assurance Requirements

Security assurance requirements applicable to this TOE are defined by assurance components shown in Table 6.4. These components are all included in CC Part 3. Components except ALC_DVS.2 and AVA_VAN.5 are included in the EAL4 assurance package. ALC_DVS.2 is a high-level component of ALC_DVS.1 and AVA_VAN.5 is a high-level component of AVA_VAN.3. [CC_PP-C0499] applies no operation to all components shown in Table 6.4.

Assurance class	Assurance component
Security target evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Development	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3
Guidance documents	AGD_OPE.1
	AGD_PRE.1
Life-cycle support	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.1
Tests	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability assessment	AVA_VAN.5

Table 6.4: Assurance components

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

This chapter describes rationales for that the defined SFRs properly achieve the security objectives for the TOE. Section 6.3.1.1 describes that each of the SFRs can be traced back to any of the security objectives for the TOE, while Section 6.3.1.2 describes that each of the security objectives for the TOE is properly met by the corresponding effective SFR.

6.3.1.1 Tracing between Security Objectives and Security Functional Requirements

Table 6.5 shows the SFRs corresponding to the security objectives for the TOE. This table provides the rationales for the traceability of all SFRs to at least one security objective for the TOE.

SFR	**Security objective for the TOE** O.Logical_Attack	O.Physical_Attack	O.AA	O.PACE	O.Authority	O.Data_Lock
FCS_CKM.1p				x		
FCS_CKM.1e				x		
FCS_CKM.4			x	x		
FCS_COP.1a			x			
FCS_COP.1h			x			
FCS_COP.1n				x		
FCS_COP.1e				x		
FCS_COP.1hp				x		
FCS_COP.1mp				x		
FCS_COP.1sp				x		
FCS_RND.1				x		
FDP_ACC.1a			x		x	
FDP_ACC.1p	x			x		
FDP_ACF.1a			x		x	
FDP_ACF.1p	x			x		
FDP_ITC.1			x	x	x	
FDP_UCT.1p				x		

SFR	Security objective for the TOE	O.Logical_Attack	O.Physical_Attack	O.AA	O.PACE	O.Authority	O.Data_Lock
FDP_UIT.1p					x		
FIA_AFL.1a							x
FIA_AFL.1d							x
FIA_AFL.1r							x
FIA_UAU.1					x	x	
FIA_UAU.4					x		
FIA_UAU.5					x	x	
FIA_UID.1					x	x	
FMT_MTD.1						x	
FMT_SMF.1						x	
FMT_SMR.1						x	
FPT_EMS.1			x				
FPT_PHP.3			x				
FTP_ITC.1					x		

Table 6.5: Tracing between security objectives for the TOE and SFRs

6.3.1.2 Justification for the tracing

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

O.AA To achieve the security objective O.AA, it shall address the Active Authentication procedure defined by Part 11 of [ICAO_9303]. This Active Authentication is a process for a terminal to authenticate the IC chip of the TOE, and the TOE itself is not required to provide any authentication mechanism. The TOE is authenticated by properly responding the authentication procedure. To meet requirements for the authentication procedure from the terminal, the TOE incorporates the public key and private key pair, performs cryptographic operation using the private key defined by FCS_COP.1a, and hashing operation defined by FCS_COP.1h. The public key and private key pair 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. Destruction of the private key on RAM is defined by FCS_CKM.4. The security objective O.AA is sufficiently achieved by the said SFRs.

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

O.Physical_Attack Attack scenarios trying to disclose secret cryptographic keys that are confidential information, and to tamper security-related information within the TOE, by physical means are stated in the list of attacks shown in the FPT_PHP.3 section. The TSF automatically resists the attacks according to FPT_PHP.3 to protect against the disclosure of the confidential information. Protection against disclosure of confidential user- or/and TSF-data stored on / processed by the TOE by information leakage is, furthermore, achieved by FPT_EMS.1. With that, the security objective O.Physical_Attack is sufficiently achieved.

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

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

and FMT_SMR.1. The security objective O.Authority is sufficiently achieved by the said SFRs.

O.Data_Lock In the event of an authentication failure with the transport key, readout key or Active Authentication Information Access Key, authentication corresponding to the relevant key is permanently prohibited, and as the result, the security objective of permanently prohibiting readout and write of the internal data of the TOE is sufficiently achieved by the three SFRs: FIA_AFL.1a, FIA_AFL.1d, and FIA_AFL.1r.

6.3.1.3 Dependencies for Security Functional Requirements

Table 6.6 shows dependencies and support for the dependencies defined for SFRs. In the table, the Dependencies column describes dependencies defined for SFRs, and the Support for the Dependencies column describes by what SFRs the defined dependencies are satisfied or rationales indicating the justification for non-satisfied dependencies.

SFR	Dependencies	Support of the Dependencies
FCS_CKM.1p	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1sp, FCS_COP.1mp, and FCS_CKM.4 support to satisfy the dependencies.
FCS_CKM.1e	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1e and FCS_CKM.4 support to satisfy the dependencies.
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1, FCS_CKM.1e, and FCS_CKM.1p support to satisfy the dependency. FDP_ITC.1 supports keys only on volatile memory.
FCS_COP.1a	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 supports. FCS_CKM.4 supports keys on volatile memory. Since the modification and destruction of keys on nonvolatile memory are prohibited, FCS_CKM.4 does not apply to.
FCS_COP.1h	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Since keys do not exist, any requirements do not apply to.
FCS_COP.1n	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 supports. FCS.CKM.4 supports on keys on volatile memory. Since the modification and destruction of keys on nonvolatile memory are prohibited, FCS_CKM.4 does not apply to.
FCS_COP.1e	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1e and FCS_CKM.4 support to satisfy the dependencies.
FCS_COP.1hp	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Since keys do not exist, any requirements do not apply to.

SFR	Dependencies	Support of the Dependencies
FCS_COP.1mp	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1p and FCS_CKM.4 support to satisfy the dependencies.
FCS_COP.1sp	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1p and FCS_CKM.4 support to satisfy the dependencies.
FCS_RND.1	No dependencies	N/A
FDP_ACC.1a	FDP_ACF.1	FDP_ACF.1a supports to satisfy the dependency.
FDP_ACC.1p	FDP_ACF.1	FDP_ACF.1p supports to satisfy the dependency.
FDP_ACF.1a	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1a supports. Objects are created at initial configuration, but not created in the operational environment of the TOE. Therefore, FMT_MSA.3 related to file creation does not apply to.
FDP_ACF.1p	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1p supports. Objects are created at initial configuration, but not created in the operational environment of the TOE. Therefore, FMT_MSA.3 related to file creation does not apply to.
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1a supports. Objects are created at initial configuration, but not created in the operational environment of the TOE. Therefore, FMT_MSA.3 related to file creation does not apply to.
FDP_UCT.1p	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	FTP_ITC.1 and FDP_ACC.1p support to satisfy the dependencies.
FDP_UIT.1p	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	FTP_ITC.1 and FDP_ACC.1p support to satisfy the dependencies.
FIA_AFL.1a	FIA_UAU.1	FIA_UAU.1 supports to satisfy the dependency.
FIA_AFL.1d	FIA_UAU.1	FIA_UAU.1 supports to satisfy the dependency.
FIA_AFL.1r	FIA_UAU.1	FIA_UAU.1 supports to satisfy the dependency.
FIA_UAU.1	FIA_UID.1	FIA_UID.1 supports to satisfy the dependency.
FIA_UAU.4	No dependencies	N/A
FIA_UAU.5	No dependencies	N/A
FIA_UID.1	No dependencies	N/A
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1 support to satisfy the dependencies.
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.1 supports to satisfy the dependency.

SFR	Dependencies	Support of the Dependencies
FPT_EMS.1	No dependencies	N/A
FPT_PHP.3	No dependencies	N/A
FTP_ITC.1	No dependencies	N/A

Table 6.6: Dependencies for SFRs

6.3.2 Security Assurance Requirements Rationale

The security functionality of the TOE is featured by difficulty of TOE (IC chip) forgeries realized by adoption of the Active Authentication function and strengthening Secure Messaging with PACE. The security characteristics of the Active Authentication function are achieved by protecting the internal confidential information (private key) in the TOE. And, the security characteristics of the strengthened Secure Messaging functionality are achieved by the use of the session key which possesses sufficient entropy. Reading out the information kept secret in an IC chip requires advanced means of physical attacks, and it costs a certain amount of facilities and takes some time to decipher the strengthened Secure Messaging.

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

When using the IC chip as the TOE, state of the art technologies are required for SFRs and design methods to realize such SFRs. However, there are no significant variations in the security functionality of product, and points to be checked for the vulnerability assessment are also well-defined. Consequently, EAL4, which is the top level for commercial product is adopted as the development and manufacturing assurance requirements except development security and vulnerability assessment.

Note that ALC_DVS.2 does not have dependencies on other components, and the dependencies defined in AVA_VAN.5 are identical to those in AVA_VAN.3 (EAL4). Therefore, being identical to the EAL4 assurance package in terms of dependencies, dependencies among the security assurance components shown in Table 6.4 are all satisfied.

7 TOE Summary Specification

This chapter describes the TOE security functions and the assurance measures covering the requirements of the previous chapter.

7.1 TOE Security Functions

This chapter gives the overview description of the different TOE Security Functions composing the TSF.

7.1.1 TOE Security Functions from Hardware (IC) and Cryptographic Library

7.1.1.1 F.IC_CL: Security Functions of the Hardware (IC) and Cryptographic Library

This Security Function covers the security functions of the hardware (IC) as well as of the cryptographic library. According to the Certification Report the Security Target of the hardware [ST_ST31G480] defines the following Security Services:

- Physical tampering protection. (**STSS_PTP**)
- Initialization of the hardware platform and attributes. (**STSS_IPA**)
- Secure management of the lifecycle. (**STSS_MLC**)
- Logical integrity of the product. (**STSS_LI**)
- Memory firewalls. (**STSS_MF**)
- Management of security violations. (**STSS_MSV**)
- Unobservability of sensitive data. (**STSS_USD**)
- Loading and management of the Flash memory. (**STSS_LMF**)
- Support for symmetric key cryptography. (**STSS_CS**)
- Support for asymmetric key cryptography. (**STSS_CS**)
- Support for random number generation. (**STSS_CS**)
- The optional service of a cryptographic library NesLib 6.2.1 offering DES, AES, RSA, SHA, ECC, and DRGB implementation as well as the secure generation of prime numbers and RSA keys. (**STSS_CS**)

The acronyms in parenthesis (**STSS_..** meaning **ST S**ecurity **S**ervice) were added for easier referencing and are used in the following text of this ST. In addition to the services in the

list above the hardware supports AES and DES/3DES which are also referenced via **STSS_CS** (Cryptographic Support).

7.1.2 TOE Security Functions from Basic Software – Operating System

7.1.2.1 F.Access_Control

This TSF regulates all access by external entities to operations of the TOE which are only executed after this TSF allowed access.

1. Access to objects is controlled based on subjects, objects (any file) and security attributes
2. No access control policy allows reading of any key
3. Any access not explicitly allowed is denied
4. Access Control in **phase 2** (manufacturing): Configuration and initialization of the TOE, configuring of Access Control policy only by the *Manufacturer* or on behalf of him; doing key management by the *Manufacturer* or on behalf of him or by the *IC Sheet Manufacturer* or on behalf of him(see F.Management)
5. Access Control in **phase 3** (personalization): Personalization including the writing of user and dedicated TSF data and reading of initialization data only by the *Booklet Manufacturer* identified with the correct authentication key (see F.Management)
6. Access Control in **phase 4** (operational use): Reading of user data only by an *Authorized Terminal* after a successful PACE authentication and using Secure Messaging

7.1.2.2 F.Identification_Authentication

This function provides identification/authentication of the user roles

- IC Sheet Manufacturer
- Booklet Manufacturer
- Authorized terminal

by the methods:

1. In phase 2 (manufacturing):
   - PIN verification (transport key) that is blocked after three failed authentications. The PIN is stored on the card in a SHA-256 hash representation.
2. In phase 3 (personalization):
   - PIN verification (transport key, readout key, Active Authentication information access key) that is blocked after three failed authentications. The PINs are stored on the card in a SHA-256 hash representation.
3. In phase 4 (operational use):
   - PACE authentication method [BSI_TR-03110-1] with following properties:
     - It uses an MRZ.
     - The cryptographic method for confidentiality is AES/CBC provided by F.Crypto.

  - The cryptographic method for authenticity is CMAC provided by F.Crypto.
  - On error (wrong MAC, wrong challenge) the user role is not identified/authenticated.
  - On success the session keys are created and stored for Secure Messaging.
  - Keys and data in transient memory are overwritten after usage.
- Secure Messaging (PACE) with following properties:
  - The cryptographic method for confidentiality is AES/CBC provided by F.Crypto.
  - The cryptographic method for authenticity is CMAC provided by F.Crypto.
  - In a Secure Messaging protected command the method for confidentiality and the method for authenticity must be present.
  - The initialization vector is an encrypted Send Sequence Counter (SSC) for AES encryption and CMAC.
  - A session key is used.
  - On any command that is not protected correctly with the session keys these are overwritten according to FIPS 140-2 [FIPS_140-2] (or better) and a new PACE authentication is required.
  - Keys and data in transient memory are overwritten after usage.

4. Active Authentication with following properties:
   - According to [ICAO_9303] using ECDSA from F.IC_CL.

7.1.2.3 F.Management

In phase 2 the *Manufacturer* applies the basic software and application software to the chip. The application software includes the configuration and the file layout, which determines the security attributes.

The *IC Sheet Manufacturer* performs the following steps:

- Writing of the (new) transport key, the readout key and the Active Authentication information access key.

In phase 3 the *Booklet Manufacturer* performs the following steps:

- Formatting of all data to be stored in the TOE.
- Writing of all the required data to the appropriate files.
- Changing the TOE into the end-usage mode for phase 4 where reading of the initialization data is prevented.

7.1.2.4 F.Crypto

This function provides a high level interface to

- AES (supplied by F.IC_CL)
- CMAC
- ECC (supplied by F.IC_CL)
- SHA-1 (supplied by F.IC_CL)
- SHA-256 (supplied by F.IC_CL)

- SHA-384 (supplied by F.IC_CL)
- RNG (PTG.3, supplied by F.IC_CL)

7.1.2.5 F.Verification

TOE internal functions ensures correct operation.

7.2 Assurance Measures

The assurance measures fulfilling the requirements of EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 are given in table 7.1.

Measure	Measure
ADV_ARC.1	Security architecture description
ADV_FSP.4	Complete functional specification
ADV_IMP.1	Implementation representation of the TSF
ADV_TDS.3	Basic modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.4	Production support, acceptance procedures, automation
ALC_CMS.4	Problem tracking CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.2	Sufficiency of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: basic design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.5	Advanced methodical vulnerability analysis

Table 7.1: Assurance Measures.

7.3 TOE Summary Specification Rationale

Table 7.2 shows the coverage of the SFRs by TSFs.

SFR	TSFs
FCS_CKM.1p	F.IC_CL
FCS_CKM.1e	F.IC_CL
FCS_CKM.4	F.Identification_Authentication
FCS_COP.1a	F.IC_CL
FCS_COP.1h	F.IC_CL, F.Crypto
FCS_COP.1n	IC_CL, F.Crypto
FCS_COP.1e	F.IC_CL
FCS_COP.1hp	F.IC_CL, F.Crypto
FCS_COP.1mp	F.IC_CL, F.Crypto
FCS_COP.1sp	F.IC_CL, F.Crypto
FCS_RND.1	F.IC_CL, F.Crypto
FDP_ACC.1a	F.Access_Control
FDP_ACC.1p	F.Access_Control
FDP_ACF.1a	F.Access_Control
FDP_ACF.1p	F.Access_Control
FDP_ITC.1	F.Access_Control, F.Identification_Authentication
FDP_UCT.1p	F.Access_Control
FDP_UIT.1p	F.Access_Control
FIA_AFL.1a	F.Identification_Authentication
FIA_AFL.1d	F.Identification_Authentication
FIA_AFL.1r	F.Identification_Authentication
FIA_UAU.1	F.Access_Control
FIA_UAU.4	F.Identification_Authentication
FIA_UAU.5	F.Access_Control, F.Identification_Authentication
FIA_UID.1	F.Access_Control
FMT_MTD.1	F.Access_Control, F.Management
FMT_SMF.1	F.Management
FMT_SMR.1	F.Identification_Authentication
FPT_EMS.1	F.IC_CL
FPT_PHP.3	F.IC_CL
FTP_ITC.1	F.Access_Control, F.Identification_Authentication

Table 7.2: Coverage of SFRs for the TOE by TSFs.

The SFR **FCS_CKM.1p** requires session key generation algorithm in PACE, which is supplied by **F.IC_CL (STSS_CS(AES))**.

The SFR **FCS_CKM.1e** requires the ECDH algorithm. This is provided by the cryptographic library function **F.IC_CL (STSS_CS(ECC))**.

The SFR **FCS_CKM.4** requires the destroying of cryptographic keys. This is done in **F.Identification_Authentication**.

The SFR **FCS_COP.1a** requires ECDSA. **F.IC_CL (STSS_CS(ECC))** provides the functions.

The SFR **FCS_COP.1h** requires SHA-256 and SHA-384. **F.IC_CL (STSS_CS(SHA))** and **F.Crypto** provide these hash algorithms.

The SFR **FCS_COP.1n** requires AES, which is supplied by **F.IC_CL (STSS_CS(AES))** and **F.Crypto**.

The SFR **FCS_COP.1e** requires the ECDH algorithm for key agreement with key size 256 bits and 384 bits. This is provided by the cryptographic library function **F.IC_CL (STSS_CS(ECC))**.

The SFR **FCS_COP.1hp** requires SHA-1 and SHA-256. **F.IC_CL (STSS_CS(SHA))** and **F.Crypto** provide these hash algorithms.

The SFR **FCS_COP.1mp** requires AES in CMAC mode. This is provided in **F.IC_CL (STSS_CS(AES))** and **F.Crypto**.

The SFR **FCS_COP.1sp** requires AES in CBC mode and cryptographic key size 128 bits and 256 bits to perform Secure Messaging – encryption and decryption and AES in CMAC mode and cryptographic key size 128 bits and 256 bits to perform Secure Messaging – Message Authentication Code. This is provided in **F.IC_CL (STSS_CS(AES))** and **F.Crypto**.

The SFR **FCS_RND.1** requires the generation of random numbers which is provided by **F.IC_CL (STSS_CS)** and **F.Crypto**.

The SFR **FDP_ACC.1a** requires the enforcement of the issuance procedure access control policy to the user process for data input/output operation to/from the files as listed in Table 3.3. This is done by **F.Access_Control**.

The SFR **FDP_ACC.1p** requires the enforcement of the PACE policy to the process on behalf of terminal for reading data from the files Files EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, EF.SOD, basic access key file, password key file, transport key file, and private key file. This is done by **F.Access_Control**.

The SFR **FDP_ACF.1a** requires the enforcement of the issuance procedure access control policy to the user process, the files as listed in Table 3.3 and the authentication status as listed in Table 3.3. This is done by **F.Access_Control**.

The SFR **FDP_ACF.1p** requires the enforcement of the PACE policy on the process on behalf of terminal for reading data from the files EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, EF.SOD, basic access key file, password key file, transport key file, and private key file and the authentication status of terminal based on mutual authentication. This is done by **F.Access_Control**.

The SFR **FDP_ITC.1** requires the enforcement of the issuance procedure access control policy when importing user data from outside of the TOE. This is done by **F.Identification _Authentication** and **F.Access_Control**.

The SFR **FDP_UCT.1p** requires the enforcement of PACE policy to transmit/receive user data in a manner protected from unauthorized disclosure. This is done by **F.Access_Control**.

The SFR **FDP_UIT.1p** requires the enforcement of PACE policy to transmit/receive user data in a manner protected from modification, deletion, insertion and replay errors. This is done by **F.Access_Control**.

The SFR **FIA_AFL.1a** requires the detection of an unsuccessful authentication attempt authentication with the Active Authentication Information Access key and permanently stop authentication with the Active Authentication Information Access key. **F.Identification_Authentication** detects unsuccessful authentication attempts.

The SFR **FIA_AFL.1d** requires the detection of an unsuccessful authentication attempt authentication with the transport key and permanently stop authentication with the transport key. **F.Identification_Authentication** detects unsuccessful authentication attempts.

The SFR **FIA_AFL.1r** requires the detection of an unsuccessful authentication attempt authentication with the readout key and permanently stop authentication with the readout key. **F.Identification_Authentication** detects unsuccessful authentication attempts.

The SFR **FIA_UAU.1** requires the timing of authentication. The readout of EF.CardAccess and EF.ATR/INFO shall be allowed on behalf of the user to be performed before the user is authenticated. This is done by **F.Access_Control**.

The SFR **FIA_UAU.4** requires prevention of authentication data reuse related to mutual authentication mechanism with the PACE procedure. This is done by **F.Identification_Authentication**.

The SFR **FIA_UAU.5** requires multiple authentication mechanisms as shown in Table 6.3 and the authentication of any user's claimed identity. This is done by **F.Access_Control** and **F.Identification_Authentication**.

The SFR **FIA_UID.1** requires the timing of identification. The readout of EF.CardAccess and EF.ATR/INFO on behalf of the user to be performed before the user is identified. This is done by **F.Access_Control**.

The SFR **FMT_MTD.1** requires the management of TSF data. The ability to modify the transport key shall be restricted to the authorized personnel of the passport issuing authorities. This is done by **F.Access_Control** and **F.Management**.

The SFR **FMT_SMF.1** requires the specification of management functions. The modification of the transport key shall be possible. This is done by **F.Management**.

The SFR **FMT_SMR.1** requires the maintenance of the role authorized personnel of the passport issuing authorities. The roles are managed by **F.Identification_Authentication**.

The SFR **FPT_EMS.1** requires limiting of emanations. This is provided by F.IC_CL (STSS_USD).

The SFR **FPT_PHP.3** requires the enforcement to resistance to physical attacks. This is provided by **F.IC_CL (STSS_MLC, STSS_USD, STSS_PTP, STSS_LI)**.

The SFR **FTP_ITC.1** requires the usage of a trusted channel. This is done by **F.Access_Control** and **F.Identification_Authentication**.

7.4 Statement of Compatibility

This is a statement of compatibility between this Composite Security Target and the Security Target of ST31G480 D01[ST_ST31G480].

Note 33: The optional technology *MIFARE DESFire EV1* and *MIFARE Plus X* are not used by the TOE, the corresponding hardware security services are not relevant for the composite Security Target. Also the security problems, objectives and requirements concerning these technologies are not relevant for the composite ST.

7.4.1 Relevance of Hardware TSFs

Table 7.3 shows the relevance of the hardware security functions for the composite Security Target.

HW-TSFs[1]	Description	Relevant	Not relevant
STSS_PTP	Physical tampering protection	x	
STSS_IPA	Initialization of the hardware platform and attributes	x	
STSS_MLC	Secure management of the lifecycle	x	
STSS_LI	Logical integrity of the product	x	
STSS_MF	Memory firewalls		x
STSS_MSV	Management of security violations	x	
STSS_USD	Unobservability of sensitive data	x	
STSS_LMF	Loading and management of the Flash memory		x
STSS_CS (3DES)	Cryptographic Support		x
STSS_CS (AES)	Cryptographic Support	x	
STSS_CS (RSA)	Cryptographic Support		x
STSS_CS (ECC)	Cryptographic Support	x	
STSS_CS (SHA)	Cryptographic Support	x	
STSS_CS (TRNG)	Cryptographic Support	x	

Table 7.3: Relevance of Hardware TSFs for Composite ST

[1] See definition in 7.1.1.1

7.4.2 Compatibility: TOE Security Environment

7.4.2.1 Assumptions

The following list shows that the assumptions of the hardware are either not relevant for this Security Target or are covered by appropriate security objectives. The assumptions for the TOE are not relevant for the hardware ST.

- Assumptions of the TOE
  - A.Administrative_Env: no conflict
  - A.PKI: no conflict
- Assumptions of the hardware
  - A.Process-Sec-IC (Protection during Packaging, Finishing and Personalization): no conflict
  - A.Resp-Appl (Treatment of User Data): covered by security objective O.Logical_Attack of the TOE ST

7.4.2.2 Threats

The threats of the TOE and the hardware can be mapped (see Table 7.4) or are not relevant. They show no conflicts between each other.

- Threats of the TOE
  - T.Copy: no conflict
  - T.Logical_Attack: matches T.Abuse-Func of the hardware ST
  - T.Communication_Attack: no conflict
  - T.Physical_Attack: matches T.Phys-Manipulation, T.Phys-Probing, T.Malfunction, T.Mem-Access, T.Leak-Inherent and T.Leak-Forced of the hardware ST
- Threats of the hardware
  - T.Phys-Manipulation (Physical Manipulation): matches T.Physical_Attack of the TOE ST
  - T.Phys-Probing (Physical Probing): matches T.Physical_Attack of the TOE ST
  - T.Malfunction (Malfunction due to Environmental Stress): matches T.Physical_Attack of the TOE ST
  - T.Leak-Inherent (Inherent Information Leakage): matches T.Physical_Attack of the TOE ST
  - T.Leak-Forced (Forced Information Leakage): matches T.Physical_Attack of the TOE ST
  - T.Abuse-Func (Abuse of Functionality): matches T.Logical_Attack of the TOE ST
  - T.RND (Deficiency of Random Numbers): basic threat concerning especially the PACE functionality of the TOE; no conflict
  - T.Mem-Access (Memory Access Violation): matches T.Physical_Attack of the TOE ST

Hardware threats	TOE threats	T.Logical_Attack	T.Physical_Attack
T.Phys-Manipulation			x
T.Phys-Probing			x
T.Malfunction			x
T.Leak-Inherent			x
T.Leak-Forced			x
T.Abuse-Func		x	
T.Mem-Access			x

Table 7.4: Mapping of hardware to TOE threats (only threats that can be mapped directly are shown)

7.4.2.3 Organizational Security Policies

The organizational security policies of the TOE and the hardware have no conflicts between each other. They are shown in the following list.

- Organizational Security Policies of the TOE
  - P.PACE: not applicable
  - P.Authority: not applicable
  - P.Data_Lock: not applicable
  - P.Prohibit: not applicable
  - P.Personalization: not applicable
- Organizational Security Policies of the hardware
  - P.Process-TOE (Identification during TOE Development and Production): not applicable
  - P.Add-Functions (Additional Specific Security Functionality): not applicable
  - P.Lim_Block_Loader (Limiting and Blocking the Loader Functionality): not applicable
  - P.Controlled-ES-Loading (Controlled loading of the Security IC Embedded Software): not applicable
  - P.Resp-Appl (Treatment of user data): not applicable

7.4.2.4 Security Objectives

- Security objectives for the TOE
  - O.AA: no conflicts
  - O.Logical_Attack: matches O.Add-Functions of the hardware ST

  - O.Physical_Attack: matches O.Phys-Manipulation, O.Phys-Probing, O.Malfunction, O.Abuse-Func, O.Mem-Access, O.Leak-Inherent and O.Leak-Forced of the hardware ST
  - O.PACE: no conflicts
  - O.Authority: matches O.Identification of the hardware ST
  - O.Data_Lock: no conflicts
- Security Objectives for the hardware
  - O.Phys-Manipulation (Protection against Physical Manipulation): covered by O.Physical_Attack of the TOE ST
  - O.Phys-Probing (Protection against Physical Probing): covered by O.Physical_Attack of the TOE ST
  - O.Malfunction (Protection against Malfunctions): covered by O.Physical_Attack of the TOE ST
  - O.Leak-Inherent (Protection against Inherent Information Leakage): covered by O.Physical_Attack of the TOE ST
  - O.Leak-Forced (Protection against Forced Information Leakage): covered by O.Physical_Attack of the TOE ST
  - O.Abuse-Func (Protection against Abuse of Functionality): covered by O.Physical_Attack of the TOE ST
  - O.Identification (TOE Identification): covered by O.Authority of the TOE ST
  - O.RND (Random Numbers): basic objective for the security of the TOE; no conflicts with any security objective of the TOE
  - O.Cap_Avail_Loader (Capability and availability of the Loader): no conflicts
  - O.Add-Functions (Additional specific security functionality): covered by O.Logical_Attack of the TOE ST
  - O.Mem-Access (Area based Memory Access Control): covered by O.Physical_Attack of the TOE ST
  - O.Controlled-ES-Loading (Controlled loading of the Security IC Embedded Software): no conflicts
  - OE.Lim_Block_Loader (Limitation of capability and blocking the Loader): no conflicts
  - OE.Resp-Appl (Treatment of User Data): no conflicts
  - OE.Process-Sec-IC (Protection during Packaging, Finishing and Personalization): no conflicts

Hardware objectives	TOE objectives	O.Logical_Attack	O.Physical_Attack	O.Authority
O.Phys-Manipulation			x	
O.Phys-Probing			x	
O.Malfunction			x	
O.Leak-Inherent			x	
O.Leak-Forced			x	
O.Abuse-Func			x	
O.Identification				x
O.Add-Functions		x		
O.Mem-Access			x	

Table 7.5: Mapping of hardware to TOE security objectives including those of the environment (only those that can be mapped directly are shown)

7.4.2.5 Security Requirements

None of the SFRs show any conflicts between each other.

- Relevant Security Requirements of the TOE
  - FCS_CKM.1p (Cryptographic key generation (PACE, session keys)): no conflicts
  - FCS_CKM.1e (Cryptographic key generation (PACE, ephemeral key pairs)): no conflicts
  - FCS_CKM.4 (Cryptographic key destruction): no conflicts
  - FCS_COP.1a (Cryptographic operation (Active Authentication, signature generation)): matches FCS_COP.1/ECC of the hardware ST
  - FCS_COP.1h (Cryptographic operation (Active Authentication, hash functions)): matches FCS_COP.1/SHA of the hardware ST
  - FCS_COP.1n (Cryptographic operation (Nonce encryption)): matches FCS_COP.1/AES of the hardware ST
  - FCS_COP.1e (Cryptographic operation (Key agreement)): matches FCS_COP.1/ECC of the hardware ST
  - FCS_COP.1hp (Cryptographic operation (PACE, hash functions)): matches FCS_COP.1/SHA of the hardware ST
  - FCS_COP.1mp (Cryptographic operation (PACE, mutual authentication)): matches FCS_COP.1/AES of the hardware ST
  - FCS_COP.1sp (Cryptographic operation (PACE, Secure Messaging)): matches FCS_COP.1/AES of the hardware ST
  - FCS_RND.1 (Random number generation): matches FCS_RNG.1 of the hardware ST
  - FDP_ACC.1a (Subset access control (Issuance procedure)): no conflicts
  - FDP_ACC.1p (Subset access control (PACE)): no conflicts

  - FDP_ACF.1a (Security attribute based access control (Issuance procedure)): no conflicts
  - FDP_ACF.1p (Security attribute based access control (PACE)): no conflicts
  - FDP_ITC.1 (Import of user data without security attributes): no conflicts
  - FDP_UCT.1p (Basic data exchange confidentiality (PACE)): no conflicts
  - FDP_UIT.1p (Data exchange integrity (PACE)): no conflicts
  - FIA_AFL.1a (Authentication failure handling (Active Authentication Information Access Key)): no conflicts
  - FIA_AFL.1d (Authentication failure handling (Transport key)): no conflicts
  - FIA_AFL.1r (Authentication failure handling (Readout key)): no conflicts
  - FIA_UAU.1 (Timing of authentication): no conflicts
  - FIA_UAU.4 (Single-use authentication mechanism): no conflicts
  - FIA_UAU.5 (Multiple authentication mechanisms): no conflicts
  - FIA_UID.1 (Timing of identification): no conflicts
  - FMT_MTD.1 (Management of TSF data): no conflicts
  - FMT_SMF.1 (Specification of management functions): no conflicts
  - FMT_SMR.1 (Security roles): no conflicts
  - FPT_EMS.1 (TOE emanation): Matches FDP_ITT.1, FDP_IFC.1 and FPT_ITT.1 of the hardware ST
  - FPT_PHP.3 (Resistance to physical attack): matches FPT_PHP.3 of the hardware ST
  - FTP_ITC.1 (Inter-TSF trusted channel): no conflicts

- Security Requirements of the hardware (SFRs that cannot be mapped directly to SFRs of the TOE, but are used implicitly, are underlined)
  - FRU_FLT.2 (Limited fault tolerance): used implicitly, no conflicts to the TOE SFRs
  - FPT_FLS.1 (Failure with preservation of secure state): used implicitly, no conflicts to the TOE SFRs
  - FMT_LIM.1/Test (Limited capabilities - Test): used implicitly, no conflicts to the TOE SFRs
  - FMT_LIM.2/Test (Limited capabilities - Test): used implicitly, no conflicts to the TOE SFRs
  - FMT_LIM.1/Loader (Limited capabilities - Loader): not applicable
  - FMT_LIM.2/Loader (Limited availability - Loader): not applicable
  - FAU_SAS.1 (Audit storage): used implicitly, no conflicts to the TOE SFRs
  - FDP_SDC.1 (Stored data confidentiality): no conflicts to the TOE SFRs
  - FDP_SDI.2 (Stored data integrity monitoring and action): no conflicts to the TOE SFRs
  - FPT_PHP.3 (Resistance to physical attack): matches FPT_PHP.3 of the TOE ST
  - FDP_ITT.1 (Basic internal transfer protection): matches FPT_EMS.1 of the TOE ST
  - FPT_ITT.1 (Basic internal TSF data transfer protection): matches FPT_EMS.1 of the TOE ST
  - FDP_IFC.1 (Subset information flow control): matches FPT_EMS.1 of the TOE ST
  - FCS_RNG.1 (Random number generation): matches FCS_RND.1 of the TOE ST
  - FCS_COP.1/TDES (Cryptographic operation (EDES)): not relevant
  - FCS_COP.1/AES (Cryptographic operation (AES)): matches FCS_COP.1n, FCS_COP.1mp and FCS_COP.1sp of the TOE ST

- FCS_COP.1/RSA (Cryptographic operation (RSA)): not relevant
- FCS_COP.1/ECC (Cryptographic operation (ECC)): matches FCS_COP.1a and FCS_COP.1e of the TOE ST
- FCS_COP.1/SHA (Cryptographic operation (SHA)): matches FCS_COP.1h and FCS_COP.1hp of the TOE ST
- FCS_CKM.1/Prime generation (Cryptographic key generation (Prime generation)): not relevant
- FCS_CKM.1/RSA key generation (Cryptographic key generation (RSA key generation)): not relevant
- FDP_ACC.2/Memories (Complete access control): used implicitly, no conflicts to the TOE SFRs
- FDP_ACF.1/Memories (Security attribute based access control): used implicitly, no conflicts to the TOE SFRs
- FMT_MSA.1/Memories (Management of security attributes): used implicitly, no conflicts to the TOE SFRs
- FMT_MSA.3/Memories (Static attribute initialization): used implicitly, no conflicts to the TOE SFRs
- FMT_SMF.1/Memories (Specification of Management Functions): used implicitly, no conflicts to the TOE SFRs
- FDP_ITC.1/Loader (Import of user data without security attributes - Loader): not applicable
- FDP_ACC.1/Loader (Subset access control - Loader): not applicable
- FDP_ACF.1/Loader (Security attribute based access control - Loader): not applicable
- FMT_MSA.1/Loader (Management of security attribute - Loader): not applicable
- FMT_MSA.3/Loader (Static attribute initialization - Loader): not applicable
- FMT_SMR.1/Loader (Security roles - Loader): not applicable
- FIA_UID.1/Loader (Timing of identification - Loader): not applicable
- FMT_SMF.1/Loader (Specification of management functions - Loader): not applicable

Hardware SFRs / **TOE SFRs**	FCS_COP.1a	FCS_COP.1h	FCS_COP.1n	FCS_COP.1e	FCS_COP.1hp	FCS_COP.1mp	FCS_COP.1sp	FCS_RND.1	FPT_EMS.1	FPT_PHP.3
FPT_PHP.3										x
FDP_ITT.1									x	
FPT_ITT.1									x	
FDP_IFC.1									x	
FCS_RNG.1								x		
FCS_COP.1/AES			x			x	x			
FCS_COP.1/ECC	x			x						
FCS_COP.1/SHA		x			x					

Table 7.6: Mapping of hardware to TOE SFRs (only SFRs that can be mapped directly are shown).

7.4.2.6 Assurance Requirements

The level of assurance of the

- TOE is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.
- Hardware is EAL5 augmented with ADV_IMP.2, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ASE_TSS.2 and AVA_VAN.5.

This shows that the Assurance Requirements of the TOE is matched or exceeded by the Assurance Requirements of the hardware. There are no conflicts.

7.4.3 Conclusion

Overall no contradictions between the Security Targets of the TOE and the hardware can be found.

8 Glossary

8.1 CC Related

PP	Protection Profile
CC	Common Criteria; the same contents of the CC are also established as ISO/IEC 15408 Standards.
ST	Security Target
TOE	Target of Evaluation

8.2 ePassport Related

ICAO	International Civil Aviation Organization
SAC	Supplemental Access Control: This is written in 1.1.3 Supplemental Access Control of [ICAO_SAC] as follows. This Technical Report specifies PACE v2 as an access control mechanism that is supplemental to Basic Access Control. PACE MAY be implemented in addition to Basic Access Control, i.e. • States MUST NOT implement PACE without implementing Basic Access Control if global interoperability is required. • Inspection Systems SHOULD implement and use PACE if provided by the MRTD chip.
Passport manufacturer	An organization, which manufactures passport booklets and configures basic data (e.g. management data such as passport number, and Active Authentication Public Key and private key pair) to the TOE.
Passport office	An organization, which configures the passport booklet including the TOE with the personal information of the passport holder, and issues the passport. The passport offices are set up in various regions and serve as a counter to deliver the passport to the passport holder.

Active Authentication	Security mechanism, by which means the public key and private key pair based on the public key cryptography 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 transmitted 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.
Passive Authentication	Security mechanism, by which the digital signature of the passport issuing authority is applied to 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.
Readout key	A key which is used at issuing a passport, and is embedded in the TOE at the manufacturing stage. Refer to Table 3.3 for operations which are permitted by successful verification.
Transport key	Same as above.
Active Authentication Information Access Key	Same as above.
MRZ data	Data which are printed on a surface of ePassport and readable with terminals.
Password key file	A file storing the key, which is derived from MRZ data, used for encryption of Nonce at the PACE procedure.
PACE v2 security information	Information used for PACE v2 such as cryptographic algorithms and domain parameters.

Bibliography

[AGD] User Guidance – Xaica-α PLUS ePassport, MaskTech International GmbH, Version 1.1, 2020-07-17.

[ANSI_X9.62] ANSI X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), Inc. Accredited Standards Committee X9, 2005-11-16.

[BSI_AIS31v3] AIS 31, Version 3, Anwendungshinweise und Interpretationen zum Schema – Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, BSI, 2013-05-15.

[BSI_TR-03110-1] TR-03110-1, Technical Guideline TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, BSI, Version 2.20, 2015-02-26.

[BSI_TR-03110-3] TR-03110-3, Technical Guideline 03110: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3 – Common Specifications, BSI, Version 2.21, 2016-12-21.

[BSI_TR-03111] TR-03111, Technical Guideline TR-03111: Elliptic Curve Cryptography, BSI, Version 2.1, 2018-06-01.

[BSI_TR-03116-2] TR-03116-2, Technische Richtlinie – Kryptographische Verfahren für Projekte der Bundesregierung - Teil 2 – Hoheitliche Ausweisdokumente, BSI, Stand 2018, 2018-04-12.

[CC_Part1] CCMB-2017-04-001, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Common Criteria Maintenance Board, 2017-04.

[CC_Part2] CCMB-2017-04-002, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Common Criteria Maintenance Board, 2017-04.

[CC_Part3] CCMB-2017-04-003, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Common Criteria Maintenance Board, 2017-04.

[CC_PartEM] CCMB-2017-04-004, Version 3.1, Revision 5, Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Common Criteria Maintenance Board, Version 3.1, Revision 5, 2017-04.

[CC_PP-0056-V2] BSI-CC-PP-0056-V2-2012, Common Criteria Protection Profile / Machine Readable Travel Document with 'ICAO Application', Extended Access Control with PACE, BSI, Version 1.3.2, 2012-12-05.

[CC_PP-0068-V2] BSI-CC-PP-0068-V2-2011, Common Criteria Protection Profile / Machine Readable Travel Document using Standard Inspection Procedure with PACE (ePass_PACE PP), BSI, Version 1.0, 2011-11-02.

[CC_PP-0084] BSI-CC-PP-0084-2014, Security IC Platform Protection Profile with Augmentation Packages, BSI, Version 1.0, 2014-01-13.

[CC_PP-C0499] JISEC C0499, version 1.00, Protection Profile for ePassport IC with SAC (PACE) and Active Authentication, JBMIA, 2016-03-08.

[FIPS_140-2] FIPS PUB 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, 2001-05.

[FIPS_180-4] FIPS PUB 180-4, Secure Hash Standard, National Institute of Standards and Technology, 2012-03.

[FIPS_197] FIPS PUB 197, ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology, 2001-11-26.

[ICAO_9303] ICAO Doc 9303, Machine Readable Travel Documents, ICAO, 2015.

[ICAO_SAC] TR-SAC, Supplemental Access Control for Machine Readable Travel Documents, ICAO, Version 1.1, 2014-04-15.

[ISO_10116] ISO/IEC 10116:2006, Information technology – Security techniques – Modes of operation for an n-bit block cipher, ISO/IEC, 2006-02-01.

[ISO_7816] ISO/IEC 7816:2008, Information technology – Identification cards – Integrated circuit cards – Multipart Standard, ISO/IEC, 2008.

[JIL_AP] Joint Interpretation Library, Application of Attack Potential to Smartcards, Joint Interpretation Working Group, Version 3.0, 2019-04.

[KiSch-RNG] Version 2.0, A proposal for: Functionality classes for random number generators, W. Killmann and W. Schindler, 2011-09-18.

[NIST_SP800-38B] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology, 2005-05.

[NIST_SP800-90a-R1] NIST Special Publication 800-90A Rev. 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standards and Technology, 2015-06.

[ST_ST31G480] STMicroelectronics, ST31G480 D01 including optional cryptographic library NESLIB, and optional technologies MIFARE® DESFire® EV1 and MIFARE Plus® X – Security Target for composition, ANSSI-CC-2019/12, 2019-03-05.

9 Revision History

Version	Date	Author	Changes
1.0	2020-04-09	Gudrun Schürer	First public version
1.1	2020-07-17	Gudrun Schürer	Revised cryptographic overview in appendix A

10 Contact

MaskTech GmbH – **Headquarters**

Nordostpark 45	Phone	+49 911 955149 0
D-90411 Nuernberg	Fax	+49 911 955149 7
Germany	Email	support@masktech.de

MaskTech GmbH – **Support**

Bahnhofstr. 13	Phone	+49 831 5121077 1
D-87435 Kempten	Fax	+49 831 5121077 5
Germany	Email	support@masktech.de

NTT DATA CORPORATION – **Sponsor**

Toyosu Center Building ANNEX	–	
3-9 Toyosu 3 Chome	Homepage	www.nttdata.com
Koto-ku Tokyo		
Japan		

A Overview Cryptographic Algorithms

The following cryptographic algorithms are used by the TOE to enforce its security policy:

	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments ST-Reference
1	Authenticated Key Agreement	PACEv2 (Generic Mapping), PACE (key agreement, authentication), Elliptic Curve Diffie-Hellman, Nonce Encryption, Authentication Token	[BSI_TR-03110-1], [BSI_TR-03110-3], [ICAO_SAC], [ICAO_9303], [BSI_TR-03111] sec. 4.3.2.1, [FIPS_197] (AES), [NIST_SP800-38B], sec. 6 (CMAC) also cf. line 5 and 8	|MRZ| = 160, |Nonce| = 128, NIST: 256, 384, Session keys: AES: 128, 256,	[BSI_TR-03110-1] [BSI_TR-03110-3], [ICAO_SAC], [ICAO_9303]	FCS_COP.1e, FCS_COP.1mp, FIA_UAU.1, FIA_UAU.5
2	Authentication	Active Authentication ECDSA signature generation (using NIST P-256/SHA-256 and NIST P-384/SHA-384)	[BSI_TR-03111], sec. 4.2.1, [ANSI_X9.62], sec. 7, [FIPS_180-4], sec. 6, also cf. line 11	NIST: 256, 384	[ICAO_9303], [ICAO_SAC], [BSI_TR-03110-1]	FCS_COP.1a
3	Integrity	Secure Messaging, AES/CMAC	[BSI_TR-03110-1], [BSI_TR-03110-3], [ICAO_SAC], [ICAO_9303], [FIPS_197] (AES), [NIST_SP800-38B], sec. 6 (CMAC)	128, 256	[BSI_TR-03110-1], [BSI_TR-03110-3], [ICAO_SAC], [ICAO_9303]	FCS_COP.1sp, FDP_UIT.1p
4	Key Generation	PACE (ephemeral key pairs), Elliptic Curve Diffie-Hellman (using NIST P-256 and NIST P-384)	[BSI_TR-03111], sec. 4.1.3	256, 384	[BSI_TR-03111]	FCS_CKM.1e
5	Key Derivation	Cryptographic key generation (PACE, session keys)	[BSI_TR-03110-1], [BSI_TR-03110-3], [ICAO_SAC], [ICAO_9303] part 11, sec. 9.7.3, [FIPS_180-4] sec. 6, [BSI_TR-03111] sec. 4.3.3.2,	AES: 128, 256	[BSI_TR-03110-1], [BSI_TR-03110-3], [ICAO_SAC], [ICAO_9303]	FCS_CKM.1p
6	Confidentiality	Secure Messaging, AES in CBC mode	[BSI_TR-03110-1], [BSI_TR-03110-3], [ICAO_SAC], [ICAO_9303], part 11, sec. 9.8, [FIPS_197], (AES), [ISO_10116], sec. 7 (CBC)	128, 256	[BSI_TR-03110-1], [BSI_TR-03110-3], [ICAO_SAC], [ICAO_9303]	FCS_COP.1sp, FDP_UCT.1p

	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments ST-Reference
7	Trusted Channel	Secure Messaging in ENC/MAC (PACE)	[BSI_TR-03110-1], [BSI_TR-03110-3], [ICAO_SAC] (PACE), [ICAO_9303] additionally cf. lines 3 and 6 (PACE)	-	[BSI_TR-03110-1], [BSI_TR-03110-3], [ICAO_SAC], [ICAO_9303]	FTP_ITC.1
8	Nonce encryption	AES in CBC mode	[ICAO_9303], sec. 4.4.3.3, [ISO_10116], sec. 7 (CBC)	-	[BSI_TR-03110-3] [ICAO_9303]	FCS_COP.1n
9	Cryptographic Primitive	PTG.3 Random number generator (PTG.2 and cryptographic post-processing)	[BSI_AIS31v3], [NIST_SP800-90a-R1], sec. 10.2, 10.3.2	-	[BSI_TR-03116-2]	FCS_RND.1
10	Hash for key derivation (Cryptographic Primitive)	SHA-[1, 256]	[BSI_TR-03110-1], [BSI_TR-03110-3], [ICAO_9303], [ICAO_SAC], [FIPS_180-4], sec. 6	-	[BSI_TR-03110-1], [BSI_TR-03110-3], [ICAO_9303], [ICAO_SAC]	FCS_COP.1hp
11	Hash for signature generation (Cryptographic Primitive)	SHA-[256, 384]	[BSI_TR-03110-1], [ICAO_9303], [ICAO_SAC], [FIPS_180-4], sec. 6	-	[BSI_TR-03110-1], [BSI_TR-03110-3], [ICAO_9303], [BSI_TR-03111]	FCS_COP.1h

Table A.1: Overview Cryptographic Algorithms